S. HRG. 112–130

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: GOVERNMENT PERSPECTIVES ON PROTECTING PRIVACY IN THE DIGITAL AGE

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 6, 2011

Serial No. J–112–14

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

70–856 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	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: GOVERNMENT PERSPECTIVES ON PROTECTING PRIVACY IN THE DIGITAL AGE

WEDNESDAY, APRIL 6, 2011

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

The Committee met, pursuant to notice, at 10:08 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, and Grassley.

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

Chairman LEAHY. Good morning. Today the Committee will hold a timely and I think important hearing on the Federal Government's use of the Electronic Communications Privacy Act, or ECPA, as we know it. It is one of the Nation's premier digital privacy laws. ECPA has been a bridge between what are, of course, legitimate law enforcement needs but also the equally legitimate privacy rights of Americans. When the Committee held its first hearing on ECPA reform last September, I said that while there is general agreement that ECPA has become outdated by vast technological advances and changing law enforcement missions since the law's initial enactment, the question of how best to update this law has no simple answer. We know it has to be updated. The difficult part is exactly how do we do it.

Congress is considering many different approaches to ECPA reform, but I think there should be a few core principles to guide our work. Meaningful ECPA reform must carefully balance privacy rights, public safety, and security. Reforms must also encourage American innovation, and they have got to instill confidence in American consumers, law enforcement, and the business community. All these principles we should agree on. It is how best to do it.

For many years, ECPA has provided vital tools to law enforcement to investigate crime and to keep us safe. At the same time, the law has been crucial to safeguarding Americans' digital privacy rights. I know. I was one of the ones who helped write this bill. With the explosion, though, of cloud computing, social networking sites, and other new technologies, determining how best to bring

this privacy law into the Digital Age is going to be one of Congress' greatest challenges.

While still a useful tool for our Government today, ECPA is a law that is hampered by conflicting standards that cause confusion for law enforcement, the business community, and American consumers alike. For example, just to put it right down in the concrete, 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. And on that, it is a much different era than when I was first in law enforcement where, if police had legitimate rights and legitimate—reasons, rather, to get into a phone conversation, they would have their warrant, and they basically went and clipped on to some wires in one particular area. That is not the situation today, and, of course, it becomes even more aggravated in national security matters.

So we are having this hearing so we can examine how these and other shortcomings impact the Government's ability to fight crime and protect national security. We will also examine the Government's views about various proposals being considered by Congress to update this privacy law.

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, but also the views of the Department of Justice, which relies upon ECPA to carry out its vital law enforcement and national security duties. So I am glad both are here, and I will yield to my good friend from Iowa, the Ranking Member of this Committee, Senator Grassley.

STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Thank you, Chairman Leahy. This hearing provides us an opportunity to hear the Government's view on the need to reform this law.

At our 2010 hearing the Departments of Justice and Commerce both testified about the need for our laws to keep pace with technological developments. Both witnesses agreed that technology has changed significantly since the law was passed in 1986, but neither witness offered proposals. The hearing focused largely upon changes sought by private sector businesses and interest groups that have formed a coalition to reform the law.

We in Congress need to work to ensure that our laws are up to date and do not negatively impact business innovation. We also need to address legitimate privacy concerns.

We need to hear from the law enforcement community to ensure that we do not limit their ability to obtain information necessary to catch criminals and terrorists who use electronic communications. This statute, just like the PATRIOT Act, has specific meanings and definitions, and any amendment requires careful consideration to ensure that we do not create loopholes that make it harder for law enforcement to do their job.

Today we have an opportunity to follow up with both of those departments. No legislative proposal has been put forward by the administration. Instead, the witnesses, it seems to me, will point out areas where changes could be made to bring clarity to the law.

I hope the Department of Justice changes what they view will be brought forward and what they feel will harm investigations. I also want to hear what Commerce has to say about changes that they feel are necessary to ensure that we remain competitive and how reforming our privacy laws could enhance business.

That said, there is clearly a tension between the two points, and that was how we arrived at the current law, a carefully crafted compromise. The 1986 statute struck a balance then between privacy and law enforcement. Replicating that balance will be the key to any possibility of being successful on proposed legislation.

I will put the rest of my statement in the record.

[The prepared statement of Senator Grassley appears as a submission for the record.]

Chairman LEAHY. Thank you very much.

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

Mr. Kerry, we will put your full statement in the record, but please go ahead, and then we will hear from Mr. Baker, and then we will go to questions.

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

Mr. KERRY. Mr. Chairman, thank you and good morning. Mr. Chairman, Ranking Member Grassley, and members of the Committee, I am pleased to be joining you again to discuss updating the Electronic Communications Privacy Act of 1986.

I am here today to say that the administration fully understands and supports the Committee's rationale for reexamining this statute, and I am here to offer to you two recommendations.

The first is that there should be a principled relationship between the legal protections and the procedures that apply to law enforcement access to electronic information and the legal protections and procedures for comparable materials in the physical world. What those protections and procedures should be should be determined by reference to a number of factors, including the privacy expectations of the parties involved, who has access to or control of the information, and the reasonable needs of law enforcement and national security.

The second is that the legal protection afforded to electronic content should not turn simply on factors that are disconnected from reasonable privacy interests of ordinary citizens.

As the Chairman and as other members of the Committee observed when we were here last September, one may question whether the Stored Communications Act's 180-day rule, the notion that privacy protection accorded to an electronic message could change 180 days after it is sent, should continue. If Congress wants to revisit this issue, the appropriate level of privacy protection once again should turn on an assessment of other factors, including the expectation of privacy of the parties to the communication, the mode of communication used in connection with the content, and who controls it, and, again, of course, the interests of law enforcement and national security.

Since we were here in September, the Department of Commerce has been at work on a commercial data privacy framework to meet the needs of the 21st century information economy. When we were here in September, we told you that even though we had not asked about ECPA, a number of industry players came to us and volunteered concerns about the statute.

Last December, we published a green paper that is included with my written testimony, which included the recommendation that, in light of changes in technology and changes in market condition, the administration should review ECPA with a view to assessing privacy protections in cloud computing and location-based services. That is a process which we are conducting. It is under with the Department of Justice and other administration colleagues.

In response to the green paper, we have received further comments from industry and from consumer groups. All of these endorsed updating ECPA. So I would be happy to provide the Committee with a summary of those comments and what they had to say about the impact of ECPA in light of new technologies, the uncertainties and emerging gaps in privacy protection.

There is another reason why this ongoing examination of ECPA is timely, which I discussed in my written testimony, and that is court decisions in recent years that have injected uncertainty on the standards and the privacy protections in emerging technologies.

So, Mr. Chairman, as you and members of the Committee proceed with what you have said is a difficult, challenging process of striking a new balance, we stand ready to work with you, and now I stand ready to respond to your questions.

Thank you.

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

Chairman LEAHY. Thank you, Mr. Kerry.

I may note that in 37 years—I do not even want to think about how many thousands of hearings I have either attended or presided over. I think this is the first time I have had somebody give their testimony from an electronic pad, and so I——

Mr. KERRY. I am an early adopter, Mr. Chairman. We try to stay on top of technology.

Chairman LEAHY. I have seen that, and I appreciate that very much. I do not use my old Selectric typewriter as much as I used to.

[Laughter.]

Chairman LEAHY. That is a joke. I actually found one in a closet at home the other day. I do not whether to give it to the Smithsonian.

Our next witness, James Baker, is the Associate Deputy Attorney General at the U.S. Department of Justice. He has worked extensively on all aspects of national security policy and investigations. He has been an official at the U.S. Department of Justice for nearly two decades, well respected by this Committee and by me for his work. He has provided the United States intelligence community legal and policy advice for many years. In 2006, he received the George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest award for counterterrorism achievements.

I am well aware of the background of that award, and it was justly and honorably deserved.

Mr. Baker also taught at Harvard Law School, served as resident fellow at Harvard University's Institute of Policy.

Mr. Baker, please go ahead, sir.

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

Mr. BAKER. Good morning, Mr. Chairman, Ranking Member Grassley, and members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice here today regarding ECPA, and here with my colleague, Mr. Kerry, from the Department of Commerce.

As you know, ECPA, which includes the Stored Communications Act and the pen register statute, is part of a set of laws that controls the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. These laws serve two functions, as folks have mentioned today. They are critical tools for law enforcement, national security, and cyber security activities, and they are essential for protecting the privacy interests of all Americans.

ECPA has never been more important than it is now. Because many criminals, terrorists, and spies use telephones or the Internet, electronic evidence obtained pursuant to ECPA is now critical in prosecuting cases involving a wide range of crimes, including terrorism, espionage, and violent crimes.

ECPA has three key components that regulate the disclosure of certain communications and related data. The first prohibits unlawful access to stored communications; The second regulates voluntary disclosures by network service providers of customer communications and records, both to Government and to non-governmental entities; and the third regulates Government access to stored communications and provides procedures for law enforcement officers to follow to compel disclosure of stored communications and related data. ECPA, as you know, was originally enacted in 1986, but it has been amended repeatedly since then, especially with substantial revisions in 1994 and in 2001.

Mr. Chairman, the Department of Justice is charged with the responsibility of enforcing the laws, safeguarding the constitutional rights of Americans, and protecting the national security of the

United States. As such, we welcome these hearings on this very important topic. We appreciate the concerns that some in Congress, the courts, and the public have expressed about ECPA, and we know that some believe that ECPA has not kept pace with technological changes or the way that people today communicate and store records, notwithstanding the fact that ECPA has been amended several times, as I just mentioned. We respect those concerns, and we appreciate the opportunity to discuss them here today. We also applaud your efforts to undertake a renewed examination of whether the current statutory scheme appropriately accommodates such concerns and adequately protects privacy while at the same time fostering innovation and economic development. It is legitimate to have a discussion about our present conceptions of privacy, about judicially supervised tools the Government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both. For example, we appreciate that there are concerns regarding ECPA's treatment of stored communications—in particular, the rule that the Government may use lawful process short of a warrant to obtain the content of e-mails that are stored for more than 180 days. And we are ready and willing to engage in a robust discussion of these matters to ensure that the law continues to provide appropriate protections for the privacy and civil liberties of Americans as technology develops.

As we engage in that discussion, as several have referenced this morning, what we must not do—either intentionally or unintentionally—is unnecessarily hinder the Government's ability to effectively and efficiently enforce the criminal law and protect national security. The Government's ability to access, review, analyze, and act promptly upon the communications of criminals that we lawfully acquire, as well as data pertaining to such communications, is vital to our mission to protect the public from terrorists, spies, organized criminals, kidnappers, and other malicious actors. At the Department of Justice, we are prepared to consider reasonable proposals to update the statute—and indeed, as set forth in my written statement for the record, we have a few of our own to suggest—provided that they do not compromise our ability to protect the public from the real threats that we face.

In closing, Mr. Chairman, it is important to note that ECPA protects privacy in another way as well. By authorizing law enforcement officers to obtain evidence from communication providers, ECPA enables the Government to investigate and prosecute hackers, identity thieves, and other online criminals. Pursuant to ECPA, the Government obtains evidence critical to our ability to prosecute these privacy-related crimes.

Mr. Chairman and members of the Committee, ECPA is an important topic, and I look forward to taking your questions here today, and I would ask that my written statement be submitted as part of the record.

Chairman LEAHY. It will be made part of the record.

Mr. BAKER. Thank you, Mr. Chairman.

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

Chairman LEAHY. I was struck when you said you are willing to consider proposals we might have, and, of course, the fact is if we do not have proposals as we go forward, then we stay with the law the way it is, and I do not think anybody would find that best. So it is a case where this is not just let us consider what Congress thinks. The fact is either Congress acts or you are stuck with the old law.

Mr. Kerry, I was pleased to learn the Commerce Department and the Justice Department are working together to consider potential updates to ECPA, so we would welcome any feedback. Can you give us a short summary of the progress of this partnership to date? Then I am going to ask the same question of Mr. Baker.

Mr. KERRY. Well, we have been in active discussions really through the year to try to deal with proposals to update and restrike the balance. The written testimony that you have from each of us is a reflection of some of the direction that that has taken. We are certainly prepared to put our shoulders to the wheel with the Committee. I think the process of you, Senator, and the Committee holding our feet to the fire and developing this testimony has helped to advance the discussions, and I think we are in a position to move forward in a concrete way.

Chairman LEAHY. Well, I would like to see the administration recommendations because, as I said, sometimes I find that inertia sometimes gets the greatest bipartisan support on the Hill, but I would like to see us move forward.

So, Mr. Baker, I would ask you the same question: How is this work with Commerce going?

Mr. BAKER. Yes, Senator, I agree with Mr. Kerry completely. We have been working on a whole range of issues related to surveillance, privacy, innovation, all of these issues. We have made, I think, substantial progress. I think the two statements together indicate that we have worked through a lot of issues. We actually got some concrete areas at least that we agree that we should focus on that are reflected in the statement. So I think that is significant progress.

We have certainly been working at the Department of Justice on language that supports the proposals that we have put forward, or at least raised. We have not finished that work yet, even within the Department and with the interagency, so we have got some additional work to do in that regard. But we have made significant progress, Senator.

Chairman LEAHY. For an incentive, I think there is a willingness of Republicans and Democrats to work together on this because when I talk about the inertia, I do not find many people who want to just stick with the law the way it is. It is outdated from both a national security point of view, but from a privacy point of view, and we worked very, very hard on the first law to get that balance, realizing that technology changes and a lot of the things that we could consider at the time we wrote the law, that those of us who worked on it knew technology might change, but none of us could predict where and to what extent. Nobody knew about the cloud at that time, for example.

Now, let me ask you a couple of specifics. Last year, the Court of Appeals for the Third Circuit held the Government could be re-

quired to obtain a search warrant before it could access an individual's cell phone location data. Under ECPA the Government can obtain cell phone location data by several different methods, including seeking a court order, but the statute does not specify whether the Government must always establish probable cause to get this order, as would be the case with a search warrant.

What is the Department's view about the legal standard that should apply in order for the Government to access cell phone location information?

Mr. BAKER. Senator, just to clarify, when we speak about cell phone location information, there is a variety of different types that are potentially available. So there is the very precise GPS type of information that might be available that more pinpoints accuracy.

Chairman LEAHY. That is right.

Mr. BAKER. And then you have cell site location information, which it is increasingly more accurate in terms of determining where a cell phone is, but it still is not as precise as——

Chairman LEAHY. It just says that cell phone is next to this—that cell phone is within the area of this cell tower, but it could be——

Mr. BAKER. There is a range of——

Chairman LEAHY. Yes.

Mr. BAKER. Depending upon where you are, in a rural, suburban, or urban area, it depends. So it is key to understand that there are different technologies that exist with respect to cell phone location information.

The Department's policy now is that if we want the GPS Information, we have to go get a warrant in order to obtain that. For the cell site location information, the less precise information, we have to still go get a court order, a variety of orders depending upon whether it is historical or prospective, but in any event, you still have to go to court and get an order, albeit under a lower standard than you have for a warrant.

Chairman LEAHY. Would it help to have some clarification specifically in this area?

Mr. BAKER. Well, we think that based on the Third Circuit case that—and we have suggested that it is definitely an area that is worth examining.

Chairman LEAHY. Well, let me ask you that, because we also have the D.C. Circuit. They vacated the life sentence of an individual who had been convicted, I believe it was in drugs, but he was—they had installed a global positioning device on his car to track him in connection, and they vacated it.

Now, I understand the Department is considering appealing this case. Am I correct? Or are you aware of that?

Mr. BAKER. I do not think we have—I would have to check on that.

It is being reviewed by the Department right now, Senator.

Chairman LEAHY. What is the legal standard to apply if you want to obtain information by using or installing a global positioning device? And does that change whether it is historical, as you had referred to earlier, or realtime?

Mr. BAKER. So just to make sure I understand, the device you are talking about is a device that is attached to a vehicle——

Chairman LEAHY. That is right.

Mr. BAKER [continuing]. As opposed to a communications device. So it is a little bit different in that sense.

Chairman LEAHY. A GPS device.

Mr. BAKER. It is a GPS, but it is not a cell phone, it is not a personal——

Chairman LEAHY. That is right. You are not talking——

Mr. BAKER. Correct.

Chairman LEAHY. It is simply a locator.

Mr. BAKER. So there have been a lot of rulings on these kinds of cases over the years, and I think, unfortunately, the answer depends on the facts of the case. And so it depends where you are when you install the device, and it depends what the device is attached to and where it goes. In circumstances in which it would go into an area that is protected by the Fourth Amendment, then you would have to get a warrant to continue to monitor the signals from that device. But to the extent that the device is attached in an unprotected area, in terms of the Fourth America, and then travels in areas that are not protected by the Fourth Amendment, then currently you would not need a warrant to obtain that information.

Chairman LEAHY. Thank you. And does it make a difference if it is historical information or realtime?

Mr. BAKER. I guess it would depend. I am thinking about the beeper. I mean, I guess if you had the beeper recording for a period of time and then downloaded the information, that would be historical. But I think the same rules that I just discussed would apply in that context since it is not a communication device.

Chairman LEAHY. Whether you put it on their garage or whether you put it on the——

Mr. BAKER. On the public street or something, where the car goes and so on, yes, all those factors are relevant to the analysis.

Chairman LEAHY. Thank you.

Senator Grassley.

Senator GRASSLEY. I am going to start with Mr. Baker. This coalition that is promoting these changes wants to increase the standards to obtain non-content information through the—just a minute. I am on the wrong question. Just a minute.

The coalition, a group of businesses and interest groups, as we know, supports a probable cause standard for obtaining all electronic communications regardless of its age, the location or storage facilities, or the provider's access to information. Do you support raising the legal standard for obtaining all electronic communications to a probable cause determination?

Mr. BAKER. Senator, I think that is the kind of concern that we have that I expressed in my statement, that we have to make sure—that the kinds of information we are talking about, especially when you come to non-content information, is critical for our ability to conduct investigations. And if we were to raise the standard with respect to some electronic communications, even content, it is going to have an impact on law enforcement investigations. We have to be mindful of that. We have to be thoughtful about that. And so whatever proposals come forward, we have to look at that in that light.

Senator GRASSLEY. Well, I think you just told me, and if you did not say this, say I interpreted you wrong. But my next question dealt with the probable cause determination, the effect on law enforcement. And you just told me it would be more difficult.

Mr. BAKER. It would be more difficult.

Senator GRASSLEY. Could this significant change also unduly burden the agencies and prosecutors and the courts?

Mr. BAKER. It would impact our—let me just stick with the location information that Senator Leahy was asking about. We use that information as sort of the basic building blocks of investigations. So an IP address, a cell phone piece of information, where you were when you placed a particular call, these are the kinds of information that we use to locate people, suspects, and also to investigate links between suspects. So we use it as sort of the basic building blocks, and we also use that kind of information to build our way toward obtaining probable cause. And so we need to be able to obtain a certain amount of information to work our way to the more intrusive types of techniques that we have available.

Senator GRASSLEY. Okay. It takes longer to prepare a 2703(d) order application than a subpoena, and it takes longer to prepare a search warrant application than a 2703(d) order application. If you would agree with those two statements, is it fair to say that raising the standard will slow down a criminal investigation?

Mr. BAKER. I think it would have an impact along those lines, Senator, yes. It would consume more resources and require us to engage in more process. I think there is no doubt about that.

Senator GRASSLEY. And since time is a critical factor during a lot of criminal investigations and speed is essential, if Congress slows down the process, then this could have real-life consequences, you know, particularly where human life is involved?

Mr. BAKER. Absolutely, Senator. As I said, whatever we do in this area, we need to get the balance right. We need to make sure that we achieve all the objectives that we want to achieve.

Senator GRASSLEY. Let me focus on the court for just a minute, and I referred to that just a couple questions ago. If all electronic communications, with emphasis upon "all," required a search warrant, the courts would experience additional burdens as well, and these increased burdens on the court system would naturally increase the delays when investigating time-sensitive threats to human life. Would that be right?

Mr. BAKER. Senator, I expect there would be some additional burden on the court. I have worked with judges for many years, and they are always ready to take on whatever the Government brings to them. So I am not sure that they would say that it would burden them that much, but I think it is additional requirements that we would have to meet and have to go to a court to achieve.

Senator GRASSLEY. This coalition supports increasing the standard to obtain non-content information through pen register or trap-and-trace orders. They are pushing for a standard to be at least as strong as that required under an electronic communication 2703(d) order. They are further pushing for this increased standard to apply to e-mail addresses, instant messages, texts, Internet protocols, addresses of Internet sites.

Currently does the legal process and authority for obtaining pen register information work well?

Mr. BAKER. For obtaining pen register information? I think our perspective would be that it does work well actually currently.

Senator GRASSLEY. And are you aware of any problems in using it?

Mr. BAKER. Using the pen registers?

Senator GRASSLEY. Yes.

Mr. BAKER. I think the answer is we are generally satisfied with the way the statute is now. There was a particular amendment in 2001 that was extremely helpful, so I think—with respect to all these, if I just may add, we are working through all these issues. I think everybody agrees that these are the significant issues to focus on. We do not have a cleared position from the administration yet on these proposals, but I think we have identified the concerns that we have.

Senator GRASSLEY. If I could just have three short questions here.

Chairman LEAHY. Go ahead.

Senator GRASSLEY. Then that will finish this point.

Do you think the legal standard to obtain information through pen register or trap-and-trace orders would be increased to a probable cause or 2703 standard?

Mr. BAKER. I am sorry, Senator. Do I think it would be——

Senator GRASSLEY. The legal standard to obtain information should be increased.

Mr. BAKER. Oh, again, this is an area—the pen registers and these kinds of things are the basic building blocks for our investigations, so any changes to those would have to be reviewed very carefully. Any changes to that standard would have to be reviewed very carefully.

Senator GRASSLEY. Well, then, I will skip a question and go to my last one. Would not a change like this increase burdens on investigators, prosecutors, and the courts?

Mr. BAKER. Yes.

Senator GRASSLEY. Okay. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

I will yield to Senator Whitehouse and then in a few minutes turn the gavel over to him.

Senator WHITEHOUSE. Thank you, Chairman, and thank you, gentlemen, both for being here. I appreciate your work on this issue.

I am going to be here until the end of the hearing because I will be taking over the gavel, so I am just going to ask a sort of brief set of overview questions now that are kind of in the nature of framing what the topics should be that we should be prepared to address as we go forward. And I assume that you are working on them as well.

One obviously is how location information should be treated. As a general proposition, I do not know that there is an established privacy right cognizable under the Fourth Amendment regarding your location. If the police want to put a tail on somebody, they do not get a warrant for that or take any action, and they can follow to the best of their ability and figure out where somebody is. When

you move up to pen register and trap-and-trace, there is a more complicated standard. And when you go to a full-blown Fourth Amendment search warrant requirement and you are involved in content, there is a much higher standard. And as I understand it, we should be sorting out where the location information, which is now newly available really in ways that it was not when ECPA was written, where it falls into that array of possibilities. Correct?

Mr. KERRY. Yes.

Senator WHITEHOUSE. So that is one. Okay. We should review the question—as a general proposition, you both agree that warrants are ordinarily required to access content of a communication. Correct?

Mr. BAKER. Not always.

Senator WHITEHOUSE. Ordinarily.

Mr. BAKER. Ordinarily. But—I am sorry. It depends. Not always. So we can talk about that.

Senator WHITEHOUSE. But the 180-day rule under ECPA specifically allows access to content if it is more than 180 days old without a warrant——

Mr. BAKER. Correct.

Senator WHITEHOUSE. We should review that determination given the change in technology and practice that has taken place. Correct?

Mr. BAKER. We agree that is definitely an area that people want to talk about, and we are happy to engage in that discussion.

Senator WHITEHOUSE. The next issue is private sector disclosures, and they come in two ways. One is private sector disclosures to other private sector commercial operators and whether we should put some restrictions on that so that, for instance, your ISP is not selling your location to McDonald's so that every time you are within 100 feet of a McDonald's you are getting a message saying, "Don't you feel like a hamburger." And at the same time, on the other side, there is the concern that the ISPs now have considerable access and considerable situational awareness about the cyber threat and what is happening out there, and ECPA restricts their ability to warn Government about those activities so that Government can be prepared to take national security protection action. And both of those are things we should be examining, correct?

Mr. KERRY. That is correct, Senator, yes. Those are actively at work in interagency processes within the administration.

Senator WHITEHOUSE. It seems to me that as we move more into the cyber realm, there are searches and then there are searches. And the Constitution concerns itself with searches in which somebody gains awareness of your personal papers and communications. That strikes me as the fundamental protection of the Fourth Amendment. Where you have a mechanism that potentially no human actually is aware of that scans the flow of data that goes through cyber space and simply alerts when it determines that a virus or a malware or some kind of threat is attached to that content, it is conceivable in that circumstance that no person actually locates that, although technically is remains a search because an agent has deployed this technology and has actually scanned the packet of content. Is that a distinction that is worth beginning to

pursue? That seems to be a novelty nowadays. You know, in the old days, if somebody went through your papers, it was an agent and they were looking at it, and your privacy was really implicated in a very significant way when another person was looking at your papers. If all that is happening is that the content of your e-mail stream is being scanned for known malware and viruses and that is causing a safety action to be taken to protect the Internet, that is a slightly different piece of—it is a slightly different privacy interest involved there, isn't it?

Mr. BAKER. Senator, these are exactly the right kinds of questions to ask and areas to think about. I have seen some folks analogize what I think you are talking about to a situation like a dog sniffing luggage at the airport for either explosives or for narcotics or something like that, and they go along the line and, you know, sniff what is there, and then they alert only on the thing that has contraband in it. So it is a different regime. It depends on the context. Airports are different than a lot of other things. But in any event——

Senator WHITEHOUSE. Conceivably, there is even less of a privacy interest in this because what happens when the dog alerts is that your suitcase gets opened and people plow through it, and a human knows what you have in your suitcase, and that affects the privacy interest; whereas, it is not unusual that what happens to a digital alert is that simply the message is rerouted and nobody actually ever gets awareness of the content.

Mr. BAKER. Well, that is one way you could do it, certainly, but I think there would be an interest in looking at that communication and trying to analyze it from a cyber security perspective to have a better idea where it came from, what its purpose is, and what its destination is.

Senator WHITEHOUSE. All right. My time has expired, and I just to figure out who was here first.

Senator Franken was here first.

Senator FRANKEN. Thank you, Mr. Chairman, and thank you, gentlemen, for your testimony.

ECPA gives citizens privacy protections with respect to law enforcement, but ECPA also says when an ISP can share our information with other businesses or the general public, and I am worried that these privacy protections are just far too weak.

Here is an example. If I make a phone call from my smart phone and my phone company learns of my location, they cannot go out and sell that information or give it to anybody unless they have my express consent. But I use the same smart phone to do a Google search, under certain court decisions that same phone company would likely be free to give my location information to any business or person that it wants to. The difference is that my phone call is covered by the Telecommunications Act, and my Internet search is covered by ECPA.

Mr. BAKER. and Mr. Kerry, are you aware of this discrepancy? And what do you think of it?

Mr. KERRY. I am aware of the discrepancy, and that, in fact, is the case. I mentioned the effort that we have undertaken to address privacy policy in the commercial data context. Indeed, a cou-

ple of weeks ago, the administration announced support for baseline privacy regulation in the online area.

The issue of what usage, what resale, what communication with third parties can be made of the kind of location information that you described, among many other kinds of information that people generate as they go online, is one of the issues that needs to be addressed as part of baseline privacy protection.

Senator FRANKEN. And as part of rewriting this bill?

Mr. KERRY. I am not sure that that necessarily fits under changing ECPA. There are aspects of it that need to be addressed under ECPA, as Mr. Baker said in response to earlier questions. Trying to establish some certainty on Government access to geo-location data and other location data is certainly an appropriate subject for consideration.

Senator FRANKEN. Well, this specific issue with location is part of a broader problem in ECPA, and you note in your testimony, Mr. Baker, that ECPA allows ISPs to disclose customer records to pretty much anyone they want as long as it is not the Government. That includes information on whom you e-mail, when you e-mail, and to some extent the websites that you visit. This is totally out of line with the Cable Act and Communications Act, which require cable and phone companies to get your consent before making these disclosures to third parties.

Mr. BAKER., I applaud the Department's position that this part of ECPA may be insufficiently protective of customer privacy. Would you agree that in this respect ECPA's consumer privacy protections represent a lower standard than the kind of protections our law provides to cable and phone service customers?

Mr. BAKER. I think it is lower with respect to the providers that ECPA applies to when compared to the regulations under the Communication Act and the Cable Act, those kinds of things that apply to different companies or at least companies wearing different hats at different times. And as you said, yes, it is one provision of ECPA that allows this more robust sharing of consumer data—not communications, not the content, but the data.

Senator FRANKEN. So it is a lower standard.

Mr. BAKER. It is a lower—well, it permits it. It permits the sharing without more to anybody who is not a governmental entity. And if I could just note that a foreign government falls within that category. In other words, it prohibits disclosures to the U.S. Government or a State government. It does not prohibit disclosures to a foreign government. So we are——

Senator FRANKEN. Thank you for that distinction.

Mr. Kerry, Minnesota is home to a lot of so-called cloud computing businesses. These are businesses that allow other businesses or individuals to store their e-mails, documents, and photos remotely instead of on their computers. I recently heard from one company in Minnesota, N Stratus. They said they are losing business because they cannot definitively tell their prospective clients when and how the Government will access their information. Because of this uncertainty, people are not deciding to put their documents on the cloud. They are choosing to keep their documents on their own computers and servers.

Mr. Kerry, I am sure you have heard of many companies that are in this situation. How can we amend ECPA to help businesses like N Stratus?

Mr. KERRY. Senator Franken, I certainly have heard that from a great many companies. I spoke yesterday at a gathering of technology and software general counsels. There was a lot of interest in this issue. We have seen in the development of e-commerce that, you know, people's willingness to trust vendors with credit card information was a critical threshold to get across. You see the same thing with cloud computing.

Harris research, market research by computing companies, indicates a very large number of both businesses and consumers are concerned about their privacy and their security in putting information into the cloud-–80 percent in the Harris survey.

One of the reasons that we have engaged in the privacy and security discussion at the Department of Commerce is because trust is such a critical component of the digital economy, and cloud providers need to be able to assure their customers that what they provide to them in the cloud is as trustworthy as physical records or other ways of storing digital information, and that, you know, they have no competitive disadvantage with other business models. That is the clear message that we have gotten from a great many companies in this area.

Senator FRANKEN. Thank you.

Senator WHITEHOUSE. Senator Coons.

Senator COONS. Thank you, Senator Whitehouse. And I must say, as I read the background of the briefing in the materials in preparation for today's hearing, I initially thought I must be mistaken that the murkiness of the legal field—it was the last memo I read before falling asleep last night. I thought it was my error. It is a truly unclear and unresolved legal landscape in the balance between Fourth Amendment interests and privacy rights between the law enforcement and the commercial. We have here a statute that has truly been exceeded by developments in technology over the last decade and more. And I am concerned about the uncertainty for law enforcement, for companies, for individuals in their privacy rights, and the interests of law enforcement.

One comment, if I might, in opening and follow-up to what Senator Grassley said. The only concern for law enforcement, I think, is not just speed. It is also efficacy. The county police department over which I had responsibility before this, we could kick down doors, arrest people, haul them out, but if it was not done in a way that was legally sound, if the evidence was not gathered in a legally sound way, then lots of the investigation and the prosecution ultimately would be wasted. And the uncertainty of the legal standards under which you are proceeding with investigations and prosecutions here I think puts law enforcement equally at risk as the possibility of raising the standards in a way that would slow down law enforcement. Law enforcement needs to be both swift and certain and done in a way that protects the privacy rights that makes America a unique place.

I would like to follow up on some of the questions Senator Franken was asking about the tensions between consumer interests and privacy rights.

Mr. Kerry, how do the U.S. protections for stored communications, data, and documents, particularly those stored in the cloud—we were talking about the tension between paper records, internal records, and those that are electronic but offsite. How does this compare with protections abroad? What is the status of the EU Data Privacy Directive? And how do our protections compare around the world given that many companies now are truly global in terms of the communications and the documents?

Mr. KERRY. Thank you, Senator Coons. As a general matter, certainly as it is perceived, the European protections under the European Data Privacy Directive are more extensive, certainly more prescriptive than those under the United States regime. Part of that is because there is no comprehensive protection in the United States; so we have some very strong sectoral regimes, we have strong common law, FTC protections, but there are gaps.

So part of our effort is to fill those gaps. That is a major reason for the administration's endorsement of baseline privacy protection. It is a key ingredient in cloud computing and data, the free flow of data as an instrument of trade and of economic growth. We have seen over the past years, the past couple of years, that the digital sector, the information economy, is leading the way out of the recession. It is a key component of our economic growth, so we need to take steps internationally to align our privacy law with consumer expectations. That is the effort on the data privacy front. I think it is an appropriate effort under ECPA.

Senator COONS. Thank you, Mr. Kerry.

Mr. BAKER. Your written testimony argued current protections for communications stored longer than 180 days makes sense because analogous paper records can be accessed with just a subpoena. Are stored e-mail communications really analogous to records accessible with a subpoena? And how do you make that analogy?

Mr. BAKER. I guess we make the analogy based upon where you are storing them, with whom, for how long, and so on. So in the paper world, if you store your records with someone else, depending upon a lot of facts and circumstances, so we can go into that if you want, but we can go and we can use a grand jury subpoena, for example, go to that third party, deliver the subpoena, and demand the records. Even somebody's personal records that they maintain in their own house, we can go with a grand jury subpoena and ask for those records. There may be some other issues there in terms of them producing them, but the basic idea is we can subpoena records when they are in the hands of either yourself or third parties if we do not want to use a warrant.

Senator COONS. And at what point does the standard rise to requiring a warrant?

Mr. BAKER. Well, if we are going to intrude on a protected privacy interest, so if we want to go—if we do not think you are going to produce the documents from your house, we want to go in your house and take them, we get a warrant that authorizes us to do that. If we thought that a third party even would pose a threat or might destroy the records, something like that, we would go and get a warrant and take them from the third party.

Senator COONS. And given the dramatic developments in the last decade in terms of the capacity for storage for e-mail—I think none of us 20 years ago had years of stored e-mail just sitting out there somewhere—how do you measure emerging privacy standards and how do we strike an appropriate balance in the law enforcement context?

Mr. BAKER. Well, I think for us our obligation on that last part is to come up and explain to you what we think the proposed changes would have on our ability to do our jobs. I think that is what we need to do.

I think it is difficult and I think courts are struggling with actually understanding what people's personal subjective expectations of privacy are because in some circumstances people want to share a lot of data with others in the world. But the question under the Fourth Amendment is not only what do they subjectively think, but what objectively is a reasonable expectation of privacy. And that is what I think Congress is going to struggle with over the next period of time to understand that and try to deduce that.

I think it is hard to understand, though. I think it is hard to actually figure out what people's reasonable conceptions of privacy are today.

Senator COONS. And I do think——

Senator WHITEHOUSE. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

I want to focus on the area of potential legislation that you have identified as No. 6 in your testimony, Mr. Baker, restricting disclosures of personal information by service providers, that is, the commercial disclosure of information, sharing, exchanging, selling information, where I think a lot of consumers are most directly impacted. We can debate in this Committee hearing the standards that ought to apply to disclosure by service providers to the Government, but as we have seen in the security breach that occurred, reported just recently occurred sometime in the past with Epsilon, literally millions of consumers are now going to be at risk of phishing, potential identity theft as a result of the breach of security concerning Epsilon that has received information from some of the major retailers around the country. And both as to content and non-content information, I think there is a significant privacy interest at stake here, as you very correctly identified in your testimony. And, in fact, I have asked the Attorney General of the United States to begin an investigation. I sent him a letter yesterday concerning the Epsilon breach, and I would like to emphasize to you now how concerning I believe this breach is. I have asked for this investigation literally within the last 24 hours, so I am not going to ask you for a response here on behalf of the Department. But I believe that it is extraordinarily important for the Department of Justice to indicate its interest in this area.

I would like to ask in my question to you whether you believe that there is a need for more explicit restrictions. You say there are none now in the legislation concerning disclosure, sharing, exchange of this kind of information, whether you believe this is an appropriate topic for us to legislate on in reforming ECPA.

Mr. BAKER. Thank you, Senator. Obviously, as the statement reflects, we certainly think it is an area—we agree—I mean, the

VerDate Nov 24 2008 12:36 Nov 22, 2011 Jkt 070856 PO 00000 Frm 00021 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70856.TXT SJUD1 PsN: CMORC

Commerce Department agrees that this is an area that we should look at. How you exactly change the rules, if at all, is another matter, but it is an area that a number of people have raised, and so it seems to be a legitimate area of inquiry.

Obviously, if people want to share information voluntarily for whatever purpose, they are free to do so. That is clear. And I do not think anybody is talking about trying to restrict people's ability to voluntarily share information to take advantage of all these amazing technologies that are out there for a whole range of different purposes. But the question is: To what extent should the companies be able to share that information consistent with their obligations to their customers? And should law enforcement be in a different position with respect to such data than private sector entities are? Maybe they should be. Maybe they should not be. But at least the key thing is to understand that.

One quick final point. With a lot of this data, as Mr. Kerry said, people are very concerned about their privacy. We understand it. And as you reference, they are also concerned about their security, the security of all this data that is out there. And the more data you share and the more data third parties have, the more data, you know, that is subject to the kinds of cybersecurity threats that Senator Whitehouse was referencing.

Senator BLUMENTHAL. Well, let me ask you very directly. If there were a requirement, for example, carrying out the policy that you have just articulated so well that people ought to be given the choice whether to share data or not, that Best Buy or L.L. Bean should be required to get a consumer's consent before they share that information, law enforcement would be impacted in absolutely no way.

Mr. BAKER. Well, I think if they agree to it—and I believe that in many circumstances they do agree to it. When you accept the terms of service, when you click "I agree" after you read or at least see these long statements that are out there, that is a legally binding contract, and so——

Senator BLUMENTHAL. Well, sometimes they do and sometimes they do not. But my question to you really is separate and apart from what the means of consent might be. It is whether law enforcement would have an interest or would be impacted—in other words, to put it more directly, I would posit the theory that the law enforcement of and the protection and security of the United States of America would not be impacted if L.L. Bean or Best Buy would be required to have a great big box requiring consumer consent before they share or sell this information, because it would not impact the standard that you would need to go to a service provider and seek the same information. You are in two separate realms of legal accountability.

Mr. BAKER. I see what you are saying, Senator. Yes, I think that is right. Obviously, we do investigate the kinds of crimes that you are talking about, so we have an interest in what is being shared and what information is out there and what information we have to investigate the unlawful disclosure of. But I think you are right. It at least puts us in no worse a position, but in terms of looking at privacy and understanding what the rules of the road are with respect to privacy, it is at least a legitimate area of inquiry.

Senator BLUMENTHAL. Thank you.

Senator WHITEHOUSE. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

Thank you to both of you for joining us today to talk about this important topic. As a former prosecutor, I see both sides: the fundamental right to privacy, but also the way criminals can try to take advantage of our respect for that privacy by claiming communications are protected and by making it very hard to get at things. So that is the way I look at this and have had some interesting times in my past jobs trying to get information.

I wanted to talk about, first of all, cloud computing. It was raised by two other Senators, and I have been working in the last 6 months on a bill with Senator Hatch that we are going to put out shortly, and I wondered if you could talk, Mr. Kerry, about how Commerce is looking at that as you look at this bill and how you are going to work cloud computing into ECPA as you move ahead.

Mr. KERRY. Thank you, Senator. We will be interested to work with you on that bill.

The Obama administration has made cloud computing a priority, and it is part of the technological initiatives that Federal agencies have been directed under a Cloud First Initiative to move toward cloud computing. It provides important economic advantages of scalability, of efficiency, which, as the digital economy leads the way to economic growth, is an important driver of innovation, of economic growth, of our ability to compete in the world and to outcompete and outinnovate the rest of the world. So that is an important driver here.

I spoke earlier—I do not recall whether you were here at the time—about the concern among cloud computing companies about leveling the playing field, about enabling them to provide the same assurance of trust in both privacy and security that their competitors have, both, you know, in the United States and around the world. So aligning the law to consumer privacy expectations is an important step toward that.

Senator KLOBUCHAR. Very good.

Mr. BAKER. What is the current law for data stored in the cloud under the Privacy Act? And does the Justice Department have any proposals for updating as it relates to that data?

Mr. BAKER. Well, the law—it depends on a lot of different facts and circumstances. In particular, it depends upon whether the information is in transmission still or whether the transmission has been completed and it has been received by the intended recipient of the communication if you are talking about communications data in the cloud. Obviously, you can store non-communications data in the cloud as well—business records and other things that corporations, for example, might want to store with a third party, or individuals—photos, things of this nature.

So I think the answer is it depends upon the kind of communication that you are talking about, and I think different rules would apply depending upon the amount of time that it has been stored there, whether it is in transmission or not, things of this nature. So it is a relatively complicated area.

Also, there is a key distinction in the law between content and non-content, as we have been talking about, so if the Government

wants non-content information, one set of rules applies. And if we want content information, a different set applies.

Senator KLOBUCHAR. Okay. In your testimony you explained the difference between cell site location, cell phone tower information, and GPS location information, and you mentioned that some courts seem to confuse the two. Your testimony states that since cell site information is much less precise than GPS information, the burden for law enforcement should be lower to obtain it.

It seems to me that the appropriate burden on law enforcement depends heavily on the precision of the information. I was hoping you could clarify just how precise the cell site information is. I have had some experiences with this before when I was a prosecutor, and I know that it gives a location within a cell tower's area and can often be as precise as giving location within a cell sector. But how precise is it in real-world terms?

Mr. BAKER. So my understanding is that—again, we are talking about a cell site, so one tower, and then that is divided up into sectors. And so if the company has the information and it is available, it can identify it with respect to the particular sector. As I mentioned earlier, it depends upon whether you are in a rural area, a suburban area, or certain urban areas. And the ranges that I have seen have been from 5 miles, so it "pinpoints" you within 5 miles of where you are, to 1 to 2 miles as you get into a more heavily populated area, to up to 100 yards. So that is the lowest amount that I have seen, 100 yards.

A key thing also that I would suggest the Committee should think about is not only the precision but also the issue with respect to the voluntariness of the sharing of that information. So generally speaking, it is information that when you move around or when you have a communication, when you move around through certain sectors and certain areas, or when you have a communication, when you initiate a communication, that is when this data is obtained. And so at least in our minds, it does bear similarities to the type of pen register information that you collect when you are at your home in your private residence and you decide to make a phone call and you reveal something about where you are at that date and time.

Senator KLOBUCHAR. Okay. Thank you very much.

Senator WHITEHOUSE. Before we conclude, I see Senator Blumenthal is still here. Would you like to do a second round?

Senator BLUMENTHAL. I would, Mr. Chairman. I wonder if you would like——

Senator WHITEHOUSE. No, why don't you proceed? I have to be here anyway, so I will wrap up.

Senator BLUMENTHAL. Thank you, Mr. Chairman. And thank you again for your testimony.

I would like to pursue some of the areas that we began discussing relating to the consent provisions and the need and advisability perhaps of restrictions. In your testimony, Mr. Baker, you say there are no explicit restrictions on a provider disclosing non-content information. Are there any restrictions, in your view?

Mr. BAKER. Well, one thing that comes to mind is the kinds of documents that we were talking about earlier, so you could have

a contractual limitation that the provider agrees to when you agree to engage in that service. So that is one off the top of my head.

Senator BLUMENTHAL. I am sorry. When I asked the question, I should have said that your testimony says that ECPA contains no explicit restrictions, and I assume from your answer that that kind of contractual provision is not in ECPA.

Mr. BAKER. That is correct. That is correct. As we discussed earlier, I think with Senator Franken, there are other parts of law that restrict other entities from disclosing certain types of data that is comparable at least, so there are other parts of law that affect that. But when we are talking about ECPA, there is no explicit limitation.

Senator BLUMENTHAL. And in your view, are those protections sufficient right now? Or should we consider it as part of this process? I know that you have suggested it may be appropriate, but given the administration's interest in privacy for consumers, would that be an appropriate area?

Mr. BAKER. Let me just first correct what I said. When I say there is no limitations, that is on the non-content information, so just to be clear about that.

The administration does not have a position yet on the exact answer to this question, but we can see that it is a legitimate question to ask. And so that is what we—you hear this all the time, but we are happy to work with you to try to figure out what the answer is here and whether additional protections are appropriate, required—again, with trying to get the balance right between all these different interests that we are trying to achieve—privacy, innovation, and security.

Senator BLUMENTHAL. Well, I would welcome and I do welcome that willingness to work together. And I wonder whether there is a task force or a working group within the administration that is focusing on this issue, as often there is on matters of policy like this one.

Mr. KERRY. Senator Blumenthal, in fact, there is. There is a Subcommittee of the National Science and Technology Council, which I co-chair with Assistant Attorney General Christopher Schroeder of the Office of Legal Policy, that is carrying forward the work to define what a privacy bill of rights should contain. We are actively at work on that, digesting the comments that we have received on the Commerce Department Green Paper and moving as quickly as we can to an administration white paper that would flesh out these questions and deal with a broad set of issues about commercial data privacy.

Senator BLUMENTHAL. And I know that the President has talked about a privacy bill of rights, which can mean a lot of things to a lot of different people. But I would just suggest—and I would be eager to work with you—that it should encompass this area which is so vitally important to consumers and individuals who may have no idea that very private information has been shared or sold by entities with which they are doing business.

Mr. KERRY. Thank you, Senator. We are hard at work, and I assure you that that is one of the topics we are working on.

Senator BLUMENTHAL. Thank you.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you, Senator Blumenthal.

Let me close first by thanking both of you for your service and for your work on this issue. I think the testimony today has made clear that there is a lot of work to be done, not only on our side but also on the administration's side in arriving at positions, which I assume you consider to be an important part of the equation here. I do not know if it is your position that you are going to raise issues and we are going to resolve them all here without the administration ever taking a position or if this is an area in which you think the administration should take a position, but I am going to assume the latter and hope that to be true.

With respect to the issue of cybersecurity, I am interested in any information that either of you might be able to provide about the timing of the conclusion of the interagency process, and the background to this question is that really I want to say over a year ago the Senate Commerce Committee completed its work, led by Chairman Rockefeller and Senator Snowe, who both also serve on the Intelligence Committee. Homeland Security I think also about a year ago completed its work. I believe it has been nearly a year since, with Senator Mikulski and Senator Snowe, I wrote the Intelligence Committee Cyber Security Task Force report. And in order to proceed to repairing the gaps in our National cyber security, we need to close on this issue. And it is very hard where there are discrepancies between where one Committee or another wants to go to resolve those discrepancies without a position being taken by the administration. And given the fact that the interagency process appears to have taken over a year at this point and that during that time the discussions back and forth between the executive and legislative branch have been reduced to, as best I can tell, zero but, in any event, very, very slender channels of communication, I think it is really important that we begin to open that up so that we can begin to legislate in this area and do so in a meaningful way.

The folks who are attacking us are not waiting. I was visiting with a CEO of an American energy company that announced a new product on the media, and within the first 2 hours of that announcement, the CEO's personal e-mail had been attacked 60,000 times. And, clearly, there are forces outside this country who want nothing more than siphon up all of our intellectual property that they can so that they can compete with us using our own knowledge against us, without paying for it, without licensing agreements, without any of the sort of accoutrements of rule of law in this area. And I would not be surprised if the number in terms of the loss to the U.S. economy is in the trillions at this point. And it is constant. It is thousands of attacks a minute, not thousands of attacks a day.

And so when that is the timeframe of the attack, to spend a year in an interagency process and shut down the engagement necessary between the executive and legislative branches for that period before we can go forward I think is a necessary process, but it is one that is not without peril, and it is one that is not without cost.

So the sooner we can bring it to its conclusion, the better off we will be as a country, and the safer we will be. So I hope very much you can provide some insight into when you think we might begin

to re-engage on the cyber security bill, and even if the interagency process is not concluded to its last final comma and period, at least it will be sufficiently through its path that the administration feels that it can begin to re-engage with us.

What can you tell me about that?

Mr. KERRY. Well, Senator Whitehouse, thank you. It is an urgent process. I can tell you that that interagency process is winding up. Both Mr. Baker and I have participated in a number of deputies Committee meetings to resolve some of the top-line issues. The rest of more detailed proposals are now in the final processes of circulating interagency. So I do not want to put a date on it, particularly with the prospect of a Government shutdown looming. But, you know, I think we are very close, a matter of some weeks away from being able to share proposals with Congress.

Senator WHITEHOUSE. I had not thought of it in the context of the Government shutdown, but I guess you are right. Pretty significant national security cost to precipitate with a Government shutdown.

Mr. KERRY. I think so.

Senator WHITEHOUSE. Mr. Baker, anything to add?

Mr. BAKER. I am not sure exactly when the process will be finished. We have made substantial progress in the past period of time. As you know well, these are very difficult issues. They raise a lot of the same kinds of issues that we talked about today in terms of security in a different context, but security, privacy, innovation, all of these things are front and center in the cyber security debate.

I agree with your assessment of the threat. It is very grave. We need to move forward as expeditiously as possible. These are difficult issues to work our way through, and so we are doing that. And I would say that we have made substantial progress in at least teeing up a lot of these issues for decisionmakers to make a call on. So I think there is a lot of work that has been done.

You may not feel as though it is a communication. I can tell you that from our end it feels like you are shouting with a bullhorn. So we have heard you that you want us to come up with proposals quickly. I am referring to the whole Congress. We get that message loud and clear, and so we are doing our homework and doing what we need to do on our end so that we can have something that is an administration position to come back to you with.

Senator WHITEHOUSE. For sure it will be this year, will it not?

Mr. BAKER. I beg your pardon, Senator?

Senator WHITEHOUSE. It will be for sure within this year, will it not?

Mr. BAKER. I am not going to sit and swear to you in front of the United States Congress——

Senator WHITEHOUSE. You are not under oath.

Mr. BAKER. Yes, Okay.

[Laughter.]

Senator WHITEHOUSE. I am asking for your assessment of—I mean, realistically.

Mr. BAKER. Realistically, I think yes. Yes.

Senator WHITEHOUSE. Okay, good. Because I think it is important that we take up a cyber security bill this year and begin to

move to repair some of the very wide open vulnerabilities that we have that are being exploited to vast effect by our economic rivals and our National security adversaries.

Let me close——

Mr. KERRY. And I would second that view, Mr. Chairman, for what it is worth.

Senator WHITEHOUSE. Yes, thank you. Let me close by saying that I really appreciate Chairman Leahy having called this hearing. Many years ago he was involved very deeply in the drafting of the original ECPA proposal. I think that the principles that he brought to that debate and the determination with which he sought through to a conclusion are lasting ones that should continue to inform what we do going forward and inspire us as we make these corrections.

What has changed in the meantime has nothing to do with those principles or with his personal determination to achieve the right balance, but the landscape itself has changed as technology has changed. And surfaces that used to be in shadow are now in sunlight; surfaces that used to be in sunlight are now in shadow. We have to adapt to those changes, but I do believe that we can bring the same principles and the same desire for a sensible balance and the same determination that Chairman Leahy showed when he originally did it, and I think that will see us in good stead as we work through the updates that intervening events have precipitated.

So I look forward to working with you on that. Thank you very much for your testimony here today and for your work going forward. We will keep the hearing open for an additional week in the event that anybody wishes to add anything to the record—we will keep the record of the hearing open for an additional week. We are not going to keep the hearing open for an additional week.

The hearing is adjourned. Thank you.

[Whereupon, at 11:29 a.m., the Committee was adjourned.]

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

VerDate Nov 24 2008 12:36 Nov 22, 2011 Jkt 070856 PO 00000 Frm 00028 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70856.TXT SJUD1 PsN: CMORC

QUESTIONS AND ANSWERS

Senate Judiciary Committee
Hearing on "The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age"
April 6, 2011

Questions for the Record from U.S. Senator Al Franken
for Associate Attorney General James A. Baker

1. **You stated in your testimony that section 2702(c)(6) of the Electronic Communications Protection Act, 18 U.S.C. 2702(c)(6), may be "insufficiently protective of consumer privacy," and suggested that "Congress could consider whether this rule strikes the appropriate balance between providers and customers."**

   a. **What, if any, role does section 2702(c)(6) play in the Department of Justice's law enforcement operations?**

Proposed DOJ response:

18 U.S.C. § 2702(c)(6) allows providers to disclose records and other information "to any person *other than a governmental entity*," without limitation. 18 U.S.C. § 2702(c)(6) (emphasis added). Accordingly, providers cannot rely on subsection 2702(c)(6) when they wish to report a crime to the Department, although they can rely on this provision to provide data to foreign governments, for example. Indeed, foreign governments sometimes use this provision to obtain voluntary disclosure of information directly from U.S. providers that may be used for their own criminal investigations, because § 2702(c)(6)'s exclusion of "governmental entities" applies only to departments and agencies of the United States or any State or political subdivisions thereof. *See* 18 U.S.C. § 2711(4) (defining "governmental entity"). Section 2702(c)(6) therefore can allow foreign governments to obtain subscriber or customer records or information (but not content of communications) without the assistance of the U.S. government, which may slightly reduce the number of assistance requests that the Department of Justice receives from foreign governments.

   b. **Is section 2702(c)(6) necessary for the Department of Justice's law enforcement operations?**

Proposed DOJ response:

For the reasons discussed above, 18 U.S.C. § 2702(c)(6) is not necessary for the Department of Justice's law enforcement operations.

**Written Questions of Senator Patrick Leahy,
Chairman, Senate Committee On The Judiciary
to Associate Deputy Attorney General James Baker,
Hearing On "The Electronic Communications Privacy Act:
Government Perspectives on Privacy In The Digital Age"**

CYBERSECURITY

1. One of the greatest challenges facing the Nation today is the need to develop a comprehensive national strategy for cybersecurity. A key part of that strategy will be how Congress properly balances the need for more information sharing to combat cyber threats -- within the Government, between the Government and private sector, and among members of the private sector -- with the need to protect personal privacy.

a. Section 2702 of ECPA provides guidelines for when private companies can voluntarily share electronic communications information with the Government. How does Section 2702 impact the way the Government currently combats cybersecurity threats?

DOJ response:

At the outset, we agree that cybersecurity is a critical challenge. As reflected in the President's 60-Day Cyberspace Policy Review, the Administration recognizes the importance of cybersecurity and the challenges we face in protecting the Nation's private sector and Government networks from an array of threats and vulnerabilities. Information sharing is a vital component of a successful cybersecurity strategy. Without a steady flow of information about rapidly evolving cyber threats and vulnerabilities, both the private sector and the Government will be ill-prepared to prevent and respond to damaging cyber incidents.

We have received anecdotal accounts from Federal incident response entities and electronic communications and remote computing service providers suggesting that ECPA's restrictions on divulging the content of and records associated with stored communications discourage private companies from sharing information that would assist legitimate governmental and private sector cybersecurity efforts.

However, some of these sorts of disclosures reportedly are not occurring even when sharing is not barred by ECPA. For example, we have been told that providers are sometimes reluctant to share non-content records pertaining to cyber threats with other non-governmental providers, even though section 2702 does not prohibit private sector sharing of non-content

records at all. Thus, it is not altogether clear that ECPA is solely responsible for the private sector's reticence. Issues such as private sector competitiveness and aversion to assuming any legal risk—no matter how remote—may also play a role.

b. Could this provision, or other parts of ECPA, be improved to better protect cyber security?

DOJ response:

Amendments to existing law should be made to facilitate information sharing for information used to protect against cybersecurity threats. The Administration's cybersecurity legislative package includes a proposal intended to clarify the private sector's ability to voluntarily share cybersecurity threat information; however, the proposal would amend Title VI of the U.S. Code (Domestic Security) rather than Title 18. It would lift ECPA's restrictions on information sharing between the private sector and the Government for information used to protect computers from cybersecurity threats, subject to safeguards that would protect civil liberties.

c. Should there be different standards under ECPA for when and how private companies can voluntarily share electronic communications information about cyber threats with the Government, verses when and how such information can be voluntarily shared among members of the private sector?

DOJ response:

Both the private sector and the Government play critical roles in cybersecurity. The private sector owns and operates the vast majority of the information systems in the United States and, accordingly, has a primary stake in addressing cybersecurity threats; however, the Government has unique incident response capabilities that may be vital to effectively attributing and neutralizing such threats and to recovery and reconstitution efforts. Moreover, to the extent that privacy concerns may be cited as a reason to distinguish between private-to-private and private-to-government information sharing regimes, we note that privacy concerns are raised by both; nevertheless, when subject to appropriate safeguards, the Nation is better situated to address cyber threats when the private sector and the Government incident response efforts are at parity and informed by similar information. While we believe strongly that we should encourage voluntary sharing by the private sector with the Government, and recognize the importance of

private-to-private sharing, it is important to note that sharing among private sector entities can raise anti-competitiveness and antitrust concerns in certain circumstances.

LOCATION INFORMATION

2. In 1983, the Supreme Court[1] held that the police may track suspects by using an electronic beeper without first obtaining a search warrant. Do you believe that the privacy interests implicated by the Government's use of an electronic beeper to obtain location information are different than the interests implicated when the Government obtains GPS or cell site location information, and if so, why?

Proposed DOJ response:

The Department believes different types of location information may implicate different privacy interests. As your question notes, the Supreme Court has held that the use of a tracking device to monitor the highway movements of a vehicle does not implicate the Fourth Amendment. Similarly, the majority of courts have held that cell-phone users have no reasonable expectation of privacy in providers' historical cell-site location records, both because that information is used to provide service and is retained by wireless carriers as routine business records and because of its relative lack of precision (see response to Question 4 below).

Conversely, the Department recommends that prosecutors obtain a warrant based on probable cause before requiring providers to disclose ongoing precise location data generated using GPS technology embedded in a particular cell phone.

3. During the hearing, you testified that not all location information is subject to the same legal standard under ECPA, in terms of when and how the Government can obtain such information. For example, you noted that the Department's policy is to seek a search warrant in order to obtain GPS location information. But, the Department's policy is to seek a court order to obtain cell site location information. While it is true that cell site location information is somewhat less precise than GPS location data, cell site location information does provide location information that is within a very limited area around a particular cellular tower. Given this, are the privacy and law enforcement interests in cell site location information significantly different from the privacy and law enforcement interests in GPS location information, and if so, why?

[1] *U. S. v. Knotts*, 460 U.S. 276 (1983).

Proposed DOJ response:

See the response to Question 2 above.

4. **You also testified that the legal standards for obtaining location information could vary, depending upon whether an electronic communications device is being used in a Fourth Amendment-protected area, or in an unprotected area. In the case of cell site location information:**

    a. **Should the legal standard for the Government to obtain this information vary depending upon whether a cell phone is being used in a private, rather than public area?**

Proposed DOJ response:

As stated above, cell-site location information is information that a phone provider uses to provide service and retains in its ordinary course of business about which of its cell towers, and usually which of three pie-slice "sectors" covered by that tower, provided service to a user's phone when the user placed or received a call, text message, or data transfer. The legal standard that the Government may use to obtain such "communication-related" cell-site location information should not depend on whether a cell phone is being used in a private, rather than a public area. First, cell-phone providers collect communication-related cell-site location information in the ordinary course of their business and rely on this information to route their subscribers' phone communications. Because the providers collect this information in order to provide service to their subscribers, individuals who choose to use cellular phones do not have a privacy interest in this information vis-à-vis their providers, even when they are using their phones in a private space. Accordingly, no heightened legal standard is required when the government obtains cell-site information from providers about cell phones that are located in private spaces. Indeed, this comports with the rules that have long applied to the use of phones in homes. In light of the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979) (Fourth Amendment does not apply to collection of numbers dialed and other activity indicating use of a phone within a home) and Congress's passage of the Pen Register statute in 1986, the same standard applies whether the phone is located inside a home or on the public street.

Second, cell-site location information is not sufficiently precise to reveal a phone's location within a particular private space. Accordingly, based on the Supreme Court's reasoning in *United States v. Karo*, 468 U.S. 705 (1984), the government's collection of cell-site location information would not invade a phone user's privacy interests, even when the phone happens to

be located in a private space, because the cell-site location information would not allow the government to know it is in any private space, let alone a particular private space.

For both of these reasons, the Department of Justice believes that the legal standard for obtaining cell-site location information should not vary depending on whether a cell phone is being used in a private area, rather than a public one.

b. Does your answer turn on whether the Government can use the location information to track an individual in real-time, as would be the case with a GPS tracking device?

Proposed DOJ response:

We understand this question to be asking whether the legal standard for cell-site location information should be different where the government obtains cell-site information on an ongoing basis and can use this information to monitor an individual's general but non-specific whereabouts in a continuous manner. Cell-site location information rarely, if ever, provides the government with a continuous or near-continuous stream of information about an individual's location over an extended period of time because the information stream typically available for disclosure to the government includes only the cell-site information for a limited set of events–for example, when the phone user makes or receives a phone call or sends or receives a text message. In this sense, and in others, cell-site location information is unlike the information generated by a GPS tracking device. As set forth above, cell-site location information records are generated and used by the provider in the ordinary course of its business, and they do not provide a cell phone's precise location. Therefore, the legal standard for obtaining communication-related cell-site information should not be based on whether the Government obtains cell-site information in real time.

c. Would it matter whether the cell site location information to be obtained was historical or prospective?

Proposed DOJ response:

The Department believes that the Fourth Amendment does not require the government to obtain a warrant for call-related cell-site location information, regardless of whether that information is historical or prospective. This conclusion is particularly clear in the case of historical cell-site location information. When the government obtains historical cell-site location information from a phone provider, it is simply obtaining business records that the provider generated and kept in the ordinary course of business. Although these records may pertain to a particular phone subscriber, that subscriber will not have seen these records [and likely will not even know the specific information they contain, though it is reasonable to expect

that they recognize such information exists as a product of the mobile nature of the service provided]. Rather, these records are simply business records of the provider that contain technical information (such as the tower used to handle a call) that the provider generated and recorded in order to route communications to and from the subscriber. A phone subscriber cannot have a reasonable expectation of privacy in these provider business records, any more than the subscriber could assert a Fourth Amendment interest in other business records that the provider generates about the subscriber for its own business purposes, such as records about the subscriber's billing history or interactions with customer service personnel. (See also response to Question 4(a) above.)

5. Today, many personal electronic devices, such a smart phones, contain GPS location technology.

a. Is it the Department's view that the Government must obtain a search warrant in order to access location information from a smart phone or other electronic communications device that contains GPS tracking capabilities?

Proposed DOJ response:

When the government obtains physical possession of a smart phone or other electronic communications device, the government's search of that phone must comply with the requirements of the Fourth Amendment. Because numerous courts have concluded that cell phones are closed containers, the Department of Justice recommends that the government obtain a warrant before conducting this kind of search, unless an exception to the warrant requirement (such as consent or exigent circumstances) applies. In addition, see the response to Question 2 above.

b. Does your answer change depending upon whether the electronic communications device is being used in a private or public area?

Proposed DOJ response:

See above.

**Written Questions of Senator Patrick Leahy,
Chairman, Senate Committee On The Judiciary
to Department of Commerce General Counsel Cameron Kerry,
Hearing On "The Electronic Communications Privacy Act:
Government Perspectives on Privacy In The Digital Age"**

CLOUD COMPUTING

1. Recently, the Commerce Department released a report entitled "Commercial Data Privacy and Innovation in the Internet Economy," that recommended, among other things, that the Administration address the privacy protections needed for cloud computing.
    a. How does the current uncertainty in the law about the privacy protections for cloud computing impact American businesses?

Response: My testimony and that of private sector representatives before this Committee in September 2010, discussed the benefits of cloud computing for American businesses.[1] As defined by the Commerce Department's National Institute of Standards and Technology, cloud computing is "a model for enabling ubiquitous, 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."[2] According to Gartner, Inc., cloud computing was a $59 billion marketplace in 2009, with revenues predicted to increase to $150 billion in 2014.[3] It is important to the retooling and regrowing of the domestic economy and to the competitiveness of American businesses globally.

Research on the willingness of both business and consumers to use cloud computing shows trust is an important barrier.[4] As I testified last September, in an April 2010 Harris Interactive poll, 50 percent of the adults surveyed had limited interest in using cloud-based services or applications.[5] Of those surveyed, 81% expressed concerns about the security of those services. And in a 2009

[1] *See* September 2010 Statement of Cameron Kerry, at 9-10, *available at* http://judiciary.senate.gov/pdf/10-09-22KerryTestimony.pdf. *See also* Statement of Brad Smith, at 4-5, *available at* http://judiciary.senate.gov/pdf/10-09-22SmithTestimony.pdf; Statement of James X. Dempsey, Center for Democracy & Technology, at 6, *available at* http://judiciary.senate.gov/pdf/10-09-22DempseyTestimony.pdf.

[2] NIST Special Publication 800-145 "The NIST Definition of Cloud Computing (Draft)", *available at* http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

[3] Andrew Hickey, "Cloud Computing Services Market to Near $150 Billion in 2014, CRN, June 22, 2010, *available at* http://www.crn.com/news/channel-programs/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm.

[4] *See* Department of Commerce Green Paper, "Commercial Data Privacy and Innovation in the Internet Economy," at 13, *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[5] Harris Interactive, "Cloud Computing – Are Americans Ready?" (Apr. 21, 2010), *available at* http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/80/Default.aspx.

survey conducted for Microsoft, more than 90 percent of those surveyed expressed reservations about the privacy and security of personal data stored in the cloud.[6] While cloud computing services have experienced robust growth in recent years, customer privacy concerns are one factor that stakeholders will need to further address in the future.

International rules can contribute to uncertainty about the rules applicable to cloud computing because of competing legal requirements and potential restriction on the transfer of data across borders. Two Canadian provinces --, British Columbia and Nova Scotia -- passed laws in 2004 and 2006 respectively, prohibiting personal data held by public sector entities from being stored outside of Canada. The reason given for adopting these laws was unfounded concern that the PATRIOT Act would give the U.S. government undue access to information on Canadian citizens stored in the United States. In comments on the Department of Commerce's Notice of Inquiry on consumer privacy, Salesforce.com cited several foreign country restrictions on transborder data flow, including the British Columbia and Nova Scotia laws. Salesforce.com noted that in addition to the barriers that these laws create, they have fostered the misperception that private and public sector organizations not subject to the laws are prohibited from using U.S.-based cloud computing services. The company also stated that the resulting confusion has "at times, prevented outright sales of enterprise cloud services."[7] In 2011, the privacy authority in the German State of Schleswig-Holstein concluded that the transborder transmission of German citizens' personal information for storage outside the European Union likely violates German privacy law, and that storage in the United States is likely illegal for a variety of reasons, including very significantly the paucity of privacy laws in the United States.[8] That decision would, at a minimum, raise the costs for U.S. firms to offer cloud-based services in Germany or other countries that adopt similar requirements as these firms duplicate server locations. Trading partners such as India, Saudi Arabia and United Arab Emirates have threatened to restrict market access for certain firms which do not comply with onerous data security restrictions. While these threats have been resolved on an ad hoc basis thus far, countries (e.g. India) are contemplating new rules and requirements which could result in preferential treatment for local data providers at the expense of U.S. firms.

International privacy protection laws can significantly affect American businesses in another way as well. An American business that stores data in the United States and has a presence in a foreign country must follow United States law and also navigate the foreign court system's demands for information. For example, the local employees of U.S. companies are often threatened with jail if they do not produce data stored in the United States and protected by U.S. laws. If the business cannot follow both sets of laws simultaneously, it may be forced to choose among being sanctioned by the foreign country, leaving the foreign country, and moving data outside the United States.

---

[6] *See* September 2010 Statement of Cameron Kerry, at 10.

[7] Comments of Salesforce.com, at 2, in *Information Privacy and Innovation in the Internet Economy*, Docket No. 100402174-0175-01 (filed June 9, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Salesforce%20Comments.pdf. *See also* Fred H. Cate, "Provincial Canadian Geographic Restrictions on Personal Data in The Public Sector," at 13-16 (2008).

[8] Dr. Thilo Wiechert, "Cloud Computing & Data Privacy," at 6-7 (Feb. 2011), *available at* https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf.

b. How does the current uncertainty in the law about privacy protections for cloud computing impact American consumers?

Response: The impact on consumers is a mirror image of the impact on businesses. As noted in our Privacy Green Paper, trust is necessary to secure the full potential of the Internet as a political, economic, educational, and social medium.[9] In the digital economy, enterprises operate with private information, and consumers must be able to trust that enterprises will operate in accordance with their expectations of privacy. To the extent consumers pass up cloud-based services because of uncertainties about the privacy protections afforded, they will not enjoy the benefits that cloud services can provide to them.

Variance in privacy protection across the country adds to uncertainty about whether information in the cloud is as secure and private as information in other environments. Opened emails may receive greater protection in the 9th Circuit that in other federal jurisdictions; after *Warshak*, emails will be more "private" in the 6th Circuit than in other jurisdictions. As a result, the privacy protection afforded to an individual's communications may turn on the accidents of where the individual lives or where his or her information is stored. A clear set of rules that are consistent with 21st century consumer experiences and expectations that also appropriately take into account public safety and other stakeholder needs could diminish this uncertainty.

c. How does the current uncertainty in the law about the privacy protections for cloud computing impact internet service providers, and other companies offering could computing services?

Response:
As a general matter, the impact on Internet service providers (ISPs) is similar to that of other businesses that provide computing services. Indeed, as forms of access to the Internet and the varieties of services offered by ISPs multiply, the distinctions diminish. Nevertheless, email remains the most widely-used form of stored electronic content subject to the Stored Communications Act, extensively discussed in my testimony, Associate Deputy Attorney General Baker's, and that of other witnesses in September. Since most ISPs also offer email among their services, their business model and relationship with the customers who store email communications with them are especially affected by uncertainties about the scope of protection afforded to those emails under the Stored Communications act and the Fourth Amendment .

USE OF INFORMATION FOR COMMERCIAL PURPOSES

2. The Electronic Communications Privacy Act does not prohibit Internet Service Providers from sharing consumer information for commercial purposes, if the consumer gives his or her consent. But, I am concerned that this consent could be obtained through complicated user agreements that consumers may not fully understand. Should ECPA be

[9] Green Paper, at 13.

amended to prohibit, or restrict, the disclosure and/or use of personal information for commercial purposes?

Response: The Administration has urged Congress to enact a "consumer privacy bill of rights" with a comprehensive set of fair information practice principles to provide baseline consumer data privacy protections.[10] As the Department of Commerce noted in our Privacy Green Paper, consumers may not have enough information about the ways in which providers use and disclose their personal information to make informed choices about whether, or on what terms, to grant consent.[11] We therefore recommended adopting principles to promote greater transparency between service providers and their customers, including "simple notices, clearly articulated purposes for data collection, commitments to limit data use to fulfill these purposes, and expanded use of robust audit systems to bolster accountability."[12]

In my testimony before this Committee on April 6, I stated that, for online information as in the physical world, the legal protection and procedures should be determined by reference to a number of factors, including the privacy expectations of the parties involved, who has access to or control of the information, and the reasonable needs of law enforcement and national security. It is consistent with this principle that the extent to which individuals allow third-party access to their data is relevant to drawing standards under ECPA. What kinds of third-party access to electronic data service providers can or cannot allow, what forms of consent should be required, and what other rights consumers should have are questions best resolved in the context of comprehensive consumer privacy legislation that can address the full range of consumer privacy and business competitiveness issues, rather than in the context of law enforcement access.

[10] *See* Testimony of NTIA Administrator Lawrence E. Strickling before the Senate Committee on Commerce, Science, and Transportation, Mar. 16, 2011, at 6, *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=9e90bd89-dcb9-42c3-a8b7-e59e126b8fad.
[11] Green Paper, at vi.
[12] *Id.* at 4.

SUBMISSIONS FOR THE RECORD

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED

"THE ELECTRONIC COMMUNICATIONS PRIVACY ACT:
GOVERNMENT PERSPECTIVES ON PROTECTING PRIVACY IN THE DIGITAL AGE"

PRESENTED

APRIL 6, 2011

Good afternoon, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). ECPA, which includes the Stored Communications Act and the Pen Register statute, is part of a set of laws that controls the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. These laws serve two functions. They are critical tools for law enforcement, national security, and cyber security activities, and they are essential for protecting the privacy interests of all Americans.

ECPA has never been more important than it is now. Because many criminals, terrorists and spies use telephones or the Internet, electronic evidence obtained pursuant to ECPA is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. In addition, because of the inherent overlap between criminal and national security investigations, ECPA's standards affect critical national security investigations and cyber security programs.

ECPA has three key components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates government access to stored communications; it creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. ECPA was initially enacted in 1986 and has been amended repeatedly since then, with substantial revisions in 1994 and 2001.

Mr. Chairman, the Department of Justice is charged with the responsibility of enforcing the laws, safeguarding the constitutional rights of Americans, and protecting the national security of the United States. As such, we welcome these hearings on this important topic. We appreciate the concerns that some in Congress, the courts, and the public have expressed about ECPA. We know that some believe that ECPA has not kept pace with technological changes or the way that people today communicate and store records, notwithstanding the fact that ECPA has been amended several times for just that purpose. We respect those concerns, and we appreciate the opportunity to discuss them here today. We also applaud your efforts to undertake a renewed examination of whether the current statutory scheme appropriately accommodates such concerns and adequately protects privacy while at the same time fostering innovation and economic development. It is legitimate to have a discussion about our present conceptions of privacy, about judicially-supervised tools the government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both. For example, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a

warrant to obtain the content of emails that are stored for more than 180 days. We are ready and willing to engage in a robust discussion of these matters to ensure that the law continues to provide appropriate protections for the privacy and civil liberties of Americans as technology develops.

As we engage in that discussion, what we must not do – either intentionally or unintentionally – is unnecessarily hinder the government's ability to effectively and efficiently enforce the criminal law and protect national security. The government's ability to access, review, analyze, and act promptly upon the communications of criminals that we acquire lawfully, as well as data pertaining to such communications, is vital to our mission to protect the public from terrorists, spies, organized criminals, kidnappers, and other malicious actors. We are prepared to consider reasonable proposals to update the statute – and indeed, as set forth below, we have a few of our own to suggest – provided that they do not compromise our ability to protect the public from the real threats we face.

Significantly, ECPA protects privacy in another way as well: by authorizing law enforcement officers to obtain evidence from communications providers, ECPA enables the government to investigate and prosecute hackers, identity thieves, and other online criminals. Pursuant to ECPA, the government obtains evidence critical to prosecuting these privacy-related crimes.

I. ECPA Plays a Critical Role in Protecting Public Safety.

The government is responsible for catching and punishing criminals, deterring crime, protecting national security, and guarding against cyber threats. The government also plays a significant role in protecting the privacy and civil liberties of all Americans. The government enforces laws protecting privacy, and pursues cyber criminals and others who engage in identity theft and other offenses that violate privacy laws. Over the decades, government access to certain electronic communications, including both content and non-content information, has become even more important to upholding our law enforcement and national security responsibilities.

Pursuing criminals and tracking national security threats, however, is no simple task. Not only does the rapidly changing technological environment affect individual privacy, it also can impact adversely on the government's ability to investigate crime and respond to national security and cyber threats. As originally enacted, ECPA endeavored to establish a framework for balancing privacy and law enforcement interests – and to do so notwithstanding technological change. But the actual pace of change puts pressure on that framework that has in the past necessitated periodic amendments to it. As noted above, we look forward to working with the Congress to assess whether amendments to ECPA are appropriate at this time to keep pace with changes in technology.

It is important to understand both the kind of information that the government obtains under ECPA and how that information is used in criminal investigations. Under ECPA, the government may compel service providers to produce both content and non-content information related to electronic communications. It is obvious that the contents of a communication – for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography – can be important evidence in a criminal case. But non-content information may be equally important, particularly at the early stages of a criminal or national security investigation.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Service providers often collect and store such records in order to operate their networks and for other legitimate business purposes. Non-content information about a communication – also referred to as "metadata" – may include information about the identity of the parties to the communication, the time and duration of the communication, and the communicants' location. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without ready access to non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant for a physical search.

In my September 22, 2010, testimony before the Committee, I discussed several examples of how ECPA currently assists law enforcement in accomplishing our mission to protect public safety. For the sake of completeness of the record before the Committee in this Congress, I repeat them below.

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 agents obtained an arrest warrant 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 the suspect's 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 non-content 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 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 effectively available law enforcement resources. They successfully captured the fugitive in nine hours without placing officers, or the public, at undue risk.

These are only a few examples of how ECPA has become a critically important public safety tool. The Department of Justice thinks it is important that any changes to ECPA be made with full awareness of whether, and to what extent, the changes could adversely affect the critical goal of protecting public safety and the national security of the United States. For example, if an amendment were unduly to restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost.

Congress should also recognize that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations. In general, it takes longer for law enforcement to prepare a 2703(d) order application than a subpoena, and it takes longer to obtain a search warrant than a 2703(d) order. In a wide range of investigations, including terrorism, violent crimes, and child exploitation, speed is essential. In drug investigations, where targets frequently change phones or take other steps to evade surveillance, lost time can eliminate law enforcement's ability to collect useful evidence.

II. Portions of ECPA May Be Appropriate for Further Legislation or Clarification.

ECPA was enacted in 1986, but it has been amended on numerous subsequent occasions in light of the advance of technology and privacy concerns. Congress amended its provisions as recently as 2009; substantial revisions occurred in 1994 and 2001.

As we previously have testified, the Department of Justice stands ready to work with the Committee as it considers changes to portions of ECPA and the Pen Register statute (which was also enacted as part of the Electronic Communications Privacy Act in 1986). Although the Department does not endorse any particular legislative changes in today's testimony, we discuss matters that may be appropriate for amendment and the problems we see in those areas. In particular, this testimony addresses eight separate issues: the standard for obtaining prospective cell-site information, providing appellate jurisdiction for ex parte orders in criminal investigations, clarifying the standard for issuing 2703(d) orders, extending the standard for non-content telephone records to other similar forms of communication, clarifying the exceptions in the Pen Register statute, restricting disclosures of personal information by service providers, provider cost reimbursement, and the compelled disclosure of the contents of communications.

(1) Prospective cell-site information

One appropriate subject for further legislation is the legal standard for obtaining, on a prospective basis, cell tower information associated with cell phone calls. Cellular telephones operate by communicating through a carrier's infrastructure of fixed antennas. For example, whenever a user places or receives a call or text message, the network is aware (and makes a record) of the cell tower and usually which of three pie-slice "sectors"" covered by that tower serving the user's phone. This information, often called "cell-site information," is useful or even critical in a wide range of criminal cases, even though it reveals the phone's location only approximately (since it can only place the phone somewhere within that particular "cell" and sector). It is also often useful in early stages of criminal or national security investigations, when the government lacks probable cause for a warrant.

The appropriate legal standard for obtaining prospective cell-site information is not entirely uniform across the country. Judges in many districts issue prospective orders for cell-site information under the combined authority of a pen/trap order under the Pen Register statute and a court order under ECPA based upon "specific and articulable facts." (CALEA prohibits providers from making wireless location information available "solely pursuant" to the Pen Register statute.) Starting in 2005, however, some magistrate and district judges began rejecting this approach and holding that the only option for compelled ongoing production of cell location information is a search warrant based on probable cause. Courts' conflicting interpretations of the statutory basis for obtaining prospective cell-site information have created uncertainty regarding the proper standard for compelled disclosure of cell-site information, and some courts'

requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes. Legislation to clarify and unify the legal standard and the proper mechanism for obtaining prospective cell-site information could eliminate this uncertainty.

It should be noted that cell-site information is distinct from GPS coordinates generated by phones as part of a carrier's Enhanced 911 Phase II capabilities. Such data is much more precise, although wireless carriers generally do not keep it in the ordinary course of business. When the government seeks to compel the provider to disclose this sort of GPS data prospectively, it relies on a warrant. When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department recommends the use of a warrant based on probable cause. Some courts, however, have conflated cell site location information with more precise GPS (or similar) location information.

(2) Appellate jurisdiction for ex parte orders in criminal investigations

A second potential topic for legislation is to clarify the basis for appellate jurisdiction for denials of warrants or other ex parte court orders in criminal or national security investigations. Appellate review serves to clarify the law. Differences among district courts are typically resolved through review by a court of appeals, and the normal way to resolve differences among courts of appeals is through Supreme Court review. But under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact.

The lack of clear jurisdiction for appeals of denials of *ex parte* orders in criminal cases has led to some confusion in the federal courts. For example, although there are numerous written opinions from magistrates and district courts on hybrid orders for prospective cell-site information, there remains no appellate authority addressing this issue. Congress could examine this issue further.

(3) Clarifying the standard for issuing 2703(d) orders

A third potentially appropriate topic for legislation is to clarify the standard for issuance of a court order under § 2703(d) of ECPA. ECPA provides that the government can use a court order under § 2703(d) to compel the production of non-content data, such as email addresses, IP addresses, or historical location information stored by providers. These orders can also compel production of some stored content of communications, although compelling content generally requires notice to the subscriber.

According to the statute, "[a] court order for disclosure... 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." 18 U.S.C. § 2703(d).

Until recently, no court had questioned that the United States was entitled to a 2703(d) order when it made the "specific and articulable facts" showing specified by § 2703(d). However, the Third Circuit recently held that because the statute says that a 2703(d) order "may" be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach thus makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not. For example, some judges will issue these orders based on the statutory "reasonable grounds" standard, while others will devise higher burdens.

In considering the standard for issuing 2703(d) orders, it is important to consider the role they play in early stages of criminal and national security investigations. In the Wikileaks investigation, for example, this point was recently emphasized by Magistrate Judge Buchanan in the Eastern District of Virginia. In denying a motion to vacate a 2703(d) order directed to Twitter, Judge Buchanan explained that "at an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation." *In re 2703(d)*, 2011 WL 900120, at *4 (E.D. Va. March 11, 2011).

Other statutes and rules governing the issuance of legal process, such as search warrants and pen/trap orders, *require* a magistrate to issue legal process when it finds that the United States has made the required showing. The Third Circuit's interpretation of § 2703(d), under which a court is free to reject the government's application even when it meets the statutory standard, is at odds with this approach. Legislation could address this issue.

(4) Extending the standard for non-content telephone records to other similar forms of communication

A fourth potential subject for legislation is the standard appropriate for compelling disclosure of addressing information associated with communications, such as email addresses. Traditionally, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA has followed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Although an officer can obtain records of calls made to and from a particular phone using a subpoena, "to" and "from" addressing information associated with email can be obtained only with a court order or a warrant. This results in a different level of protection for the same kind of information (e.g. addressing information) depending on the particular technology (e.g. telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal investigations as diverse as identity theft, child pornography, and organized crime and drug organizations, as well as national security investigations. Moreover, email, instant messaging, and social networking are now more common than telephone calls, and it makes sense to examine whether there is a reasoned basis for distinguishing between the processes used to obtain addressing information associated with wire and electronic communications. In addition, it is important to recognize that addressing information is an essential building block used early in criminal and national security investigations to help establish probable cause for further investigative techniques. Congress could consider whether this is an appropriate area for clarifying legislation.

(5) Clarifying the exceptions in the Pen Register statute

A fifth potential topic of legislation is to clarify the exceptions to the Pen Register statute. The Pen Register statute governs the collection of "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed and "to" and "from" fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception.

It makes sense that a person using a communication service should be able to consent to another person monitoring addressing information associated with her communications. For example, a person receiving threats over the Internet should be able to consent to the government collecting addressing information that identifies the source of those threats. And indeed, the Pen Register statute does contain an exception for use of a pen/trap device with the consent of the user. But there is an issue with the consent provision: it may only allow the use of the pen/trap device by a provider of electronic communication service, not the user or some other party

designated by the user. So in the Internet threats example, the provider is the ISP, not the victim herself or the government. If the provider is unwilling or unable to implement the pen/trap device, even with the user's consent, the statute may prohibit the United States from assisting the victim. Clarifying the Pen Register statute on this point may be appropriate.

(6) Restricting disclosures of personal information by service providers

A sixth potentially appropriate topic for legislation is the disclosure by service providers of customer information for commercial purposes. Under § 2702(c)(6) of ECPA, there are currently no explicit restrictions on a provider disclosing non-content information pertaining to a customer or subscriber "to any person other than a government entity." This approach may be insufficiently protective of customer privacy. Congress could consider whether this rule strikes the appropriate balance between providers and customers.

(7) Provider cost reimbursement

A seventh potential subject for legislation is ECPA's § 2706 cost reimbursement provision. Currently, ECPA does not require the government to pay providers when it obtains "telephone toll records and telephone listings" from a communications common carrier, unless the information obtained is unusually voluminous or burdensome. Other than this narrow category of information, ECPA requires the government to pay providers for producing information under ECPA.

As an initial matter, ambiguity has arisen in the phrase "telephone toll records and telephone listings," as most users now have nationwide calling plans. Some phone service providers claim that because of the billing methods they use, they do not maintain "toll records" or "telephone listings," and thus they seek payment for all compliance with legal process. Legislation could clarify this issue.
In addition, as criminals, terrorists, spies and other malicious actors shift from voice telephone to other types of electronic communications, the category of "telephone toll records and telephone listings," is diminishing in importance. Moreover, the cost to law enforcement to pay providers for responding to subpoenas is substantial. For example, it is not unusual for the United States to be billed $40.00 by a provider merely to produce a customer's name, address, and related identifying information. Congress may wish to consider the extent to which it remains appropriate to require law enforcement agencies to pay for records of non-telephone forms of communication.

(8) Compelled disclosure of the contents of communications

Finally, the eighth and last potentially appropriate topic for legislation is the standard for compelling disclosure of the contents of stored communications. As noted above, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a warrant to obtain the content of emails that are stored for more than 180 days. Indeed, some have argued recently in favor of a

probable cause standard for compelling disclosure of all such content under all circumstances. Because communication services are provided in a wide range of situations, any simple rule for compelled disclosure of contents raises a number of serious public safety questions. In considering whether or not there is a need to change existing standards, several issues are worthy of attention.

First, current law allows for the acquisition of certain stored communications using a subpoena where the account holder receives prior notice. This procedure is similar to that for paper records. If a person stores documents in her home, the government may use a subpoena to compel production of those documents. Congress should consider carefully whether it is appropriate to afford a higher evidentiary standard for compelled production of electronically-stored records than paper records.

Second, it is important to note that not all federal agencies have authority to obtain search warrants. For example, the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) conduct investigations in which they need access to information stored as the content of email. Although those entities have authority to issue subpoenas, they lack the ability to obtain search warrants. Raising the standard for obtaining stored email or other stored communications to a search warrant could substantially impair their investigations.

Third, Congress should recognize the collateral consequences to criminal law enforcement and the national security of the United States if ECPA were to provide only one means – a probable cause warrant – for compelling disclosure of all stored content. For example, in order to obtain a search warrant for a particular email account, law enforcement has to establish probable cause to believe that evidence will be found in that particular account. In some cases, this link can be hard to establish. In one recent case, for example, law enforcement officers knew that a child exploitation subject had used one account to send and receive child pornography, and officers discovered that he had another email account, but they lacked evidence about his use of the second account.

Thus, Congress should consider carefully the adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications.

* * *

In conclusion, these topics appear appropriate for further clarification or legislation, but I want to emphasize that Congress should take care not to disrupt the current balance of interests that is reflected in ECPA. ECPA is complex because our nation's communications systems are complex, and because governing the government's access to that system must resolve competing interests between privacy, innovation, international competitiveness, public safety and the national security in many different contexts. When making changes to ECPA, public safety, national security, and legitimate privacy interests must not be compromised.

The Department of Justice stands ready to work with the Committee as it considers whether changes to ECPA are called for. But we urge Congress to proceed with caution. Congress must protect privacy and foster innovation, but it also should refrain from making changes that would unduly impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations.

Law enforcement agents and prosecutors have extensive experience with actual application of ECPA, and this experience can serve as an important resource in evaluating the tangible impact of changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

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

Statement of

The Honorable Chuck Grassley

United States Senator
Iowa
April 6, 2011

Statement of Ranking Member Chuck Grassley
U.S. Senate Committee on the Judiciary
The Electronic Communications Privacy Act:
Government Perspectives on Protecting Privacy in the Digital Age
Wednesday, April 6, 2011

Chairman Leahy, thank you for calling this hearing today to examine the Electronic Communications Privacy Act. This hearing provides us the opportunity to hear the government's view on the need to reform this law, which also includes the Stored Communications Act and the criminal pen register and trap and trace statute.

This hearing comes on the heels of a September 2010 hearing that this committee held on the same topic. At that hearing, the Departments of Justice and Commerce both testified about the need for our laws to keep pace with technological developments. Both witnesses agreed that technology has changed significantly since Congress passed the law in 1986, but neither witness offered a proposal to amend the law. The hearing focused largely upon changes sought by private sector businesses and interest groups that have formed a coalition seeking to reform the law by expanding privacy protections.

I agree that we in Congress need to work to ensure that our laws are up to date and do not negatively impact business innovation and development. We also need to address legitimate privacy concerns.

I also believe we need to hear from the law enforcement community to ensure that we don't limit their ability to obtain information necessary to catch criminals and terrorists who use electronic communications to further their crimes. This statute, just like the PATRIOT Act, has specific meanings and definitions and any amendment requires careful consideration to ensure that we do not create loopholes that make it harder for law enforcement to do their jobs and allow criminals and terrorists to operate with impunity.

Today's hearing offers us an opportunity to follow-up with both departments. It is my understanding that no legislative proposal has been put forward or has been endorsed by the administration. Instead, the witnesses will point out areas where changes could be made to bring clarity to the law.

I'm interested to hear from the Department of Justice regarding what changes they view as necessary and what they feel will harm investigations. I also want to hear from the Department

of Commerce what changes they feel are necessary to ensure that we remain competitive in a global economy and how reforming our privacy laws could enhance business opportunities. That said, there is clearly a tension between the two points and that was how we arrived at the current law. The 1986 statute was a carefully crafted compromise in Congress that struck the balance between privacy and law enforcement access. Replicating that balance will be the key to any possibility of successful legislation.

The proposed changes put forth by the Digital Due Process Coalition are the only guidepost we have to start this discussion. After an initial read, I have some concerns about how this proposal will impact the way the Department of Justice currently operates. That coalition has proposed increasing the standard of proof for obtaining certain information from electronic communications providers.

This proposal seeks to increase current law to an across the board requirement that criminal investigators obtain a warrant based upon probable cause before obtaining electronic communications. Under this proposal, this standard would apply to both content and non-content information, including subscriber information and location information.

Given that the Supreme Court has long held that an individual has no reasonable expectation of privacy in information that he or she provides to a third party, this change raises a number of questions. First, how far should Congress go in creating new privacy protections for third party held documents?

The coalition proposal wants to apply new protections to electronic and wire communications, but where does it stop? Should it go further and apply to bank records for instance? Should it also include hotel records or rental car records?

Further, the proposal raises other questions about how the department would be able to quickly operate on fast moving investigations such as terrorism, violent crime, drug trafficking, and child pornography crimes. Obtaining a search warrant takes more time to obtain than a subpoena for records. How will this impact cases where time is of the essence?

Further, how would the federal courts handle the increased volume of search warrant applications? Would this require an increase in the number of federal judges in the judiciary? What about magistrate caseloads? These are important questions we should consider before we take action to amend this law.

In addition to the questions that arise in response to the proposed changes to the Electronic Communications Privacy Act, we should also discuss some other issues that are substantially related. First, we should consider what additional privacy restrictions should be placed upon providers. In the written testimony, the Department of Justice states that there are no restrictions on providers for disclosing non-content information to third parties. Should we consider adding such a restriction?

Another area of concern is the growing problem referred to by FBI Director Mueller as "going dark". This involves not the legal authority of law enforcement to obtain electronic records or

communications, but the ability of service providers to provide law enforcement real-time access to communications for wiretap purposes. Director Mueller has testified that a growing gap exists in the ability to collect information after a court order is obtained.

I think that if we are considering amending standards to obtain this information, we should simultaneously be working to ensure that these same providers are granting law enforcement the necessary access.

We have a lot to discuss and I look forward to asking the witnesses some questions.

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:
Government Perspectives on Protecting Privacy in the Digital Age"

April 6, 2011

I. Introduction.

Chairman Leahy, Ranking Member Grassley, and Members of the Committee, thank you for the opportunity to testify on behalf of the Commerce Department to discuss updating the Electronic Communications Privacy Act of 1986 (ECPA). I am pleased to again appear before you with the Department of Justice.

The Administration fully understands the Committee's rationale for reexamining ECPA. In the twenty-five years since ECPA was enacted, there has been a revolution in how Americans communicate and in how they transmit, manipulate, and store records and information. As this Committee wisely stressed in 1986, privacy protections "must advance with technology" or privacy will "gradually erode as technology advances."[1] Indeed, the rapidly changing technological environment raises not only privacy and civil liberties issues -- it also presents challenges for law enforcement and national security personnel as they seek to prevent terrorism, espionage, and other criminal and malicious acts from being committed online and in the electronic world. To ensure that ECPA continues to accommodate privacy, civil liberties, innovation, the needs of law enforcement and national security, and other important interests, the law must not remain static as technology, business practices, and consumer behavior change.

[1] S. Rep. No. 99-541, at 5, reprinted in 1986 U.S.C.C.A.N. 3555, 3559.

Since Mr. Baker and I testified before this Committee last September, the Department of Commerce and the Department of Justice have been working together to develop a specific set of legislative proposals to share with you. We have not completed this process, but we continue to discuss options for possible ECPA amendments.

II. Private Sector Stakeholders' Perspectives on Our Current ECPA Framework.

The Internet-based digital economy has sparked tremendous innovation. During the past fifteen years, networked information technologies – personal computers, mobile phones, wireless connections and other devices – have transformed our social, political, and economic landscape. A decade ago, going online meant accessing the Internet on a computer in your home, most often over a copper-wire telephone line. Today, "going online" also includes smartphones, tablets, portable games, and interactive TVs, with numerous companies developing global computing platforms in the "cloud."

These powerful and exciting developments also raise new privacy and civil liberties issues and new challenges for law enforcement. For this reason, the Commerce Department's Internet Policy Task Force has been charged with identifying and developing a privacy framework for Internet-based communications that meets the needs of the 21st century information economy. On April 23, 2010, we released a Notice of Inquiry on "Information Privacy and Innovation in the Internet Economy," which prompted more than seventy comments. Although this Notice of Inquiry did not mention ECPA, multiple commenters highlighted a critical need to reexamine the statute.[2] Those comments, as well as information gathered in various listening sessions, called attention to the impact of technological changes on ECPA.

---

[2] *See, e.g.,* Google Comments, at 4, in *Request for Reply Comments on Information Privacy and Innovation in the Internet Economy*, Docket No. 101214614-0614-01 (filed Jan. 28, 2011), *available at* http://www.ntia.doc.gov/comments/101214614-0614-

On December 16, 2010, the Commerce Department published ECPA findings (among other proposals) in a report entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Privacy Framework" (a copy of which is attached for the record). Our report contained the following recommendation:

> The Administration should review the Electronic Communications Privacy Act, with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

In response to this recommendation, the Commerce Department received further written comments from industry and consumer groups. All comments endorsed updating ECPA.[3]

01/attachments/FINAL.CommentsonDepartmentofCommercePrivacyGreenPaper%20(3).pdf (Google Comments). For convenience, all subsequent citations to "Comments" or "Reply Comments" refer to pleadings submitted on January 28, 2011, in Docket No. 101214614-0614-01. *See also* Microsoft Comments, at 10-11, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Microsoft%20Comments%20on%20Commerce%20Privacy%20Green%20Paper%20-%20final.pdf; Digital Due Process Coalition Comments , at 26-27 (filed June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Digital%20Due%20Process%20Coalition%20Comments.pdf (DDPC Comments); Comments of AT&T, Inc., at 34-35, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ACF320.pdf (AT&T Comments); Comments of the American Civil Liberties Union Comments, at 10-11, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Final%20Commerce%20Comments%20January%202011%20on%20DNT.pdf (ACLU Comments); Center for Democracy and Technology, at 5-6, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/CDT%20privacy%20comments.pdf; (CDT Comments); Computer and Communications Industry Association Comments, at 4-7, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/CCIA%20Commerce%20Comments.pdf (CCIA Comments); Deirdre K. Mulligan Comments, at 3 (June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Deirdre%20K%2E%20Mulligan%20Comments%2Epdf (Mulligan Comments); Information Technology and Innovation Foundation, at 6 (June 14, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/ITIF%20Comments%2Epdf.

[3] In response to the Commerce report's ECPA recommendation, supportive comments were submitted by eBay, Inc., Net Choice, Privacy Rights Clearinghouse, AT&T, Verizon, ACLU, General Electric, Microsoft, Google, Electronic Frontier Foundation, World Wide Web Consortium, and the Computer & Communications Industry Association, among others. All comments are available here: http://www.ntia.doc.gov/comments/101214614-0614-01/. In addition, the following companies and consumer groups have publically called for simplifying, clarifying, and unifying the ECPA standards, in response to changes in technology and new services and usage patterns: AOL, Amazon, Data Foundry, Facebook, Hewlett-Packard, Intel, Intuit, Qwest, Salesforce.com, American Library

Commenters drew attention to privacy issues surrounding new technologies, noting that the laws permitting government access to Internet communications (and records associated with customer accounts) under certain conditions prompt consumer concerns about the privacy and security of their online personal data. Commenters also stressed that "[c]ompliance with ECPA's requirements should not depend on the nature of the technology, but rather on the nature of the information sought and on Congressional determinations about consumers' reasonable expectations of privacy."[4] AT&T pointed out that ECPA's provisions have been interpreted inconsistently, raising the specter of liability and the possibility that a vast amount of personal information generated by today's digital communications services may not be protected in the same ways as comparable information in other forms.[5]

Commenters also reminded us of the social importance and economic value of recent digital communications innovation and new types of information, such as geolocation data collected from cell phones and content (text, voice, and video) stored online and accessible from anywhere on the Internet. These technologies allow companies tremendous flexibility in how they manage and store data, relate to customers, and assemble their workforces. They also provide new avenues for everything from forming friendships to organizing for political advocacy. As the Committee heard from the private sector panel on this issue last September,

---

Association, Americans for Tax Reform, Citizens Against Government Waste, Consumer Action, Future of Privacy Forum, NetCoalition, Software and Information Industry Association, TechAmerica, TechFreedom, and the Telecommunications Industry Association.

[4] Comment of Verizon and Verizon Wireless, at 14, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/01%2028%2011%20Verizon,%20Verizon%20Wireless%20Comments%20NTIA%20Privacy%20NOI.pdf. *See also* Mulligan Comments, *supra* note 2, at 3

[5] AT&T Comments, *supra* note 2, at 34 ("It is reasonable to conclude that law enforcement and private sector actors, such as ISPs and other service providers in the telecommunications and technology sectors, would benefit from specific guidance on how, to what extent, and by what means law enforcement may properly request and obtain access to the data collected incidental to the services that are provided.").

uncertainty about how ECPA applies to these types of data may hinder the adoption of new technologies by individuals and businesses and may impede innovation.[6]

The revolution in how Americans communicate and how they transmit, manage, and store information continues at an accelerating pace. Internet traffic in the United States alone approaches three petabytes per month (that is a three followed by fifteen zeros), and is growing by 40 - 50 percent annually.[7] This astonishing flow of traffic reflects how the Internet has become the communications medium of choice for most Americans, especially younger Americans. Increasingly, emails, mobile text messages, and documents stored and shared online are replacing letters, phone calls, and desktop computing. The traffic includes not only email messages, but also friend updates, photo comments and tags, and status changes; storage involves photos and videos, as well as emails and documents. Moreover, as one commenter pointed out, as Internet usage intensifies, Americans leave a myriad of "traceable trails online – the websites we've visited, the search terms we've used."[8]

III. ECPA Should Reflect Changes in Technology and Consumer Uses and the Needs of Law Enforcement and National Security.

At September's hearing, Mr. Baker and I agreed that these changes in technology, businesses practices, and consumer habits and expectations naturally raise the question whether changes in ECPA are needed to ensure that the balance originally struck in 1986 between privacy, law enforcement, and national security needs remains fair and appropriate today.

---

[6] *See The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 4 (2010) (statement of Brad Smith, General Counsel, Microsoft Corporation), *available at* http://judiciary.senate.gov/pdf/10-09-22SmithTestimony.pdf; *id.*, at 14 (Statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology), *available at* http://judiciary.senate.gov/pdf/10-09-22DempseyTestimony.pdf. *See also* Comments of AT&T, *supra* note 5, at 34 (noting that "heightened uncertainty may stifle innovation").

[7] University of Minnesota, "Minnesota Internet Traffic Studies," *available at* http://www.dtc.umn.edu/mints/.

[8] Reply Comments of NetChoice, at 19, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NetChoice%20Comments%20on%20Commerce%20Green%20Paper%20FINAL.pdf.

Today, the Administration supports the Committee's decision to consider this question and looks forward to engaging with you and other Members of Congress in the task.

ECPA itself embodies Congress's recognition that the law must adjust as technology advances. When Congress enacted the landmark Wiretap Act in 1968, it specifically excluded transmission of data from that statute's protection against interception. In 1986, Congress extended these protections to data transmissions because "[i]n the intervening years, data transmission and computer systems have become a pervasive part of the business and home environment."[9] As Mr. Baker pointed out in September, Congress substantially amended ECPA twice since 1986 to ensure that its provisions "evolved to account for changing times."[10]

There is another reason why your ongoing reexamination of ECPA is timely. In recent years, a number of courts have struggled to apply the law to a rapidly changing communications environment. One result has been several decisions that create uncertainty and confusion for consumers, law enforcement, the business community, and the Nation's innovators. I would like to discuss two recent cases.

The first case, a September 2010 decision by the U.S. Court of Appeals for the Third Circuit, concerns the procedures and standards by which law enforcement agencies may obtain certain cell location information.[11] There have been a series of decisions from district courts and magistrates on this issue, without any consensus about what the law including section 2703(d) of ECPA requires. The Third Circuit was the first appellate court to consider the question. It concluded that a court may refuse to issue an order pursuant to section 2703(d) to enable the

---

[9] H. Rep. No. 99-647, at 21, 99th Cong., 2d Sess. (1986).
[10] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 6 (2010) (statement of James A. Baker, Associate Deputy Attorney General, United States Department of Justice), *available at* http://judiciary.senate.gov/pdf/10-09-22BakerTestimony.pdf.
[11] *Application of the United States*, 620 F.3d 304 (3d Cir. 2010).

government to obtain cell location information, even if the government satisfies the legal standard set forth in that section.[12] At the same time, the Third Circuit articulated no clear standards to guide lower courts' exercise of the discretion it accorded them.[13] Congress should examine ECPA's standards and procedures concerning government access to such information, and ensure that principled reasons continue to support those standards and procedures.

The second case is *United States v. Warshak*, a December 2010 decision in which the U.S. Court of Appeals for the Sixth Circuit held that, under certain circumstances, an individual has a Fourth Amendment-protected privacy interest in private emails, even when those emails are in the possession of a third-party. The court reasoned that "[a]s some forms of communications begin to diminish, the Fourth Amendment must recognize and protect nascent ones as they arise."[14] The Sixth Circuit wrote that email "plays an indispensible part in the Information Age," and it "requires strong protection under the Fourth Amendment . . ."[15]

The *Warshak* court also relied in part on the Supreme Court's June 2010 decision in *City of Ontario v. Quon*,[16] which considered the reasonableness, under the Fourth Amendment, of the city's audit of text messages that Quon transmitted via a city-provided communications service. In considering whether Quon had a reasonable expectation of privacy in those messages, the Court acknowledged that "cell phones and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[17] It also noted, however, that "employees who need cell

---

[12] *Id.* at 315-316.
[13] *Id.* at 316-319.
[14] *United States v. Warshak*, 631 F.3d at 284, 286.
[15] *Id.* at 286.
[16] *Id.* at 286 (quoting *Quon*, 130 S.Ct. 2619, 2630, 2631 (2010)).
[17] *Quon*, 130 S.Ct. at 2630.

phones or similar devices for personal matters can purchase and pay for their own."[18] Ultimately, the Court did not resolve the privacy issue; instead, the Court assumed without deciding that Quon had a reasonable privacy interest in text messages conveyed over the city-provided communications service.[19] It nevertheless held that the city's audit of those messages was reasonable because, among other things, the audit of "Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his phone line, would have been."[20]

Warshak is the law only in the Sixth Circuit, and the U.S. government is determining whether to seek Supreme Court review. Until such time as the Court squarely addresses the issue, the law as to what protection the Fourth Amendment affords to the messages and other customer content transmitted and stored electronically will be unsettled, and the resulting uncertainty will create challenges for consumers, businesses, and law enforcement. As Congress reassesses ECPA, one clear goal should be establishing clear and consistent rules in the area for the new communications marketplace.

The Internet offers users the ability to store and access information content anywhere across the Web (what ECPA called 'remote computing') with equal ease as was traditionally done on a user's local computer. An important subject for legislative consideration is whether there should be identical statutory protections regardless of whether a user stores information on a provider's computer or locally in the user's own computer.

In determining whether to modify ECPA's current framework with respect to customer content, Congress should be guided by two overarching considerations. First, there should be a

---

[18] *Id.*
[19] *Id.*
[20] *Id.* at 2631.

principled relationship between the legal protections and procedures that apply to law enforcement access to electronic information (including both content and customer identification and transactional information) and the legal protections and procedures for comparable materials in the physical world. What those legal protection and procedures are should be determined by reference to a number of factors, including the privacy expectations of the parties involved, who has access to or control of the information, and the reasonable needs of law enforcement and national security.

Second, the legal protection afforded to electronic content should not turn simply on factors that are disconnected from ordinary citizens' reasonable privacy interests. As Senator Cardin noted at September's hearing, one may question whether the so-called 180-day rule – the notion that privacy protection accorded to an electronic message should be different 180 days after it is sent from the protections that apply on day 181 – should continue to be the law. If Congress wants to revisit this issue, as in the physical world, the appropriate level of privacy protection for online information should flow from an assessment of other factors, including the expectation of privacy surrounding the mode of communication used in connection with the content, who has access and use of that information, and the interests of law enforcement and national security.

These considerations, of course, cannot by themselves define the appropriate legal protection for electronic content. Close questions remain on which reasonable minds can differ. The resolution of those questions will require Congress once again to strike a fair balance

between the competing interests, including privacy, the needs of law enforcements and national security, innovation, and international competitiveness.[21]

Applicable rules should also recognize the need of law enforcement and national security agencies' timely and effective access to content needed to enforce the law and to protect the public, especially in circumstances where such access is time-sensitive. The Fourth Amendment applies most clearly to materials in my home, including content stored on my home computer. If law enforcement agents wish to seize my computer from my home, without my consent or the consent of someone else with access to and control over my home, under most circumstances, they must first obtain a warrant. Alternatively, they could issue a subpoena commanding me to bring my computer to them. In either case, there are opportunities for a court to review, or for an affected individual to challenge, the sufficiency of law enforcement's basis for access. By contrast, one criticism of ECPA is that, although government must notify the targeted individual if it seeks content from a service provider subject to ECPA without a warrant, it can delay notice to the individual for a considerable period of time upon a demonstration that the notified individual is likely to destroy evidence, threaten witnesses, flee, or cause some other adverse result spelled out in the statute.[22] Any rule or procedure must accommodate exigent circumstances; there are conditions that justify not informing an individual in the midst of an

---

[21] *See* Baker Testimony, *supra* note 10, at 7; *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong., 2d Sess., at 2 (2010) (statement of Cameron F. Kerry, General Counsel United States Department of Commerce), *available at* http://judiciary.senate.gov/pdf/10-09-22KerryTestimony.pdf.

[22] *See Warshak v. United States*, 490 F.3d 455, 468-469, 475 (6th Cir. 2007), *vacated, 532 F.3d 521 (6th Cir. 2008)* (government's attempt to seize emails from an ISP without a warrant was unlawful because defendant did not have adequate notice and an opportunity to challenge). In the *Warshak* litigation, the defendant was not aware that the government had seized some of his emails for more than a year after the seizure occurred. *See id.* at 460. *See also* Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," at 31 (2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

ongoing criminal or national security investigation, such as kidnappers, child molesters, or foreign spies.

IV. Conclusion.

Thank you again for inviting the Department of Commerce to testify on this important issue. As I stated last September, in establishing a clear and predictable privacy framework for electronic communications, ECPA contributed to the explosion in electronic communications that has produced enormous economic and social benefits for our nation over the last quarter century. Today, the communications revolution ECPA helped to fuel has produced new technologies, new services, new usage patterns, and new habits and expectations that require close examination of ECPA. The task is to determine whether additional changes are now needed to enhance privacy and to enable the government to carry out its law enforcement and national security responsibilities, so that in the future, as in the past, ECPA will provide a well-marked road map for providers, law enforcement, and citizens, and will enable further innovation and growth in technology, the digital economy, and society. The Department stands ready to work with this Committee in that effort.

That concludes my remarks, Mr. Chairman. I would be happy to answer any questions from you and other members of the Committee.

Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
April 6, 2011

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary
Hearing On
"The Electronic Communications Privacy Act:
Government Perspectives on Privacy In The Digital Age"
April 6, 2011

Today, the Committee holds a timely and important hearing on the Federal Government's use of the Electronic Communications Privacy Act (ECPA) -- one of the Nation's premier digital privacy laws. The Electronic Communications Privacy Act has been a bridge between legitimate law enforcement needs and the privacy rights of Americans. When the Committee held its first hearing on ECPA reform last September, I said that while there is general agreement that ECPA has become outdated by vast technological advances and changing law enforcement missions since the law's initial enactment, the question of how best to update this law has no simple answer.

Congress is considering many different approaches to ECPA reform, but a few core principles should guide our work. Meaningful ECPA reform must carefully balance privacy rights, public safety and security. Reforms must also encourage American innovation and instill confidence in American consumers, law enforcement and the business community.

For many years, ECPA has provided vital tools to law enforcement to investigate crime and to keep us safe. At the same time, this law has been crucial to safeguarding Americans' digital privacy rights. With the explosion of cloud computing, social networking sites and other new technologies, determining how best to bring this privacy law into the Digital Age will be one of Congress's greatest challenges.

While still a useful tool for our Government, today, ECPA is a law that is hampered by conflicting standards that cause confusion for law enforcement, the business community and American consumers alike. 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.

Today's hearing is an opportunity for this Committee to examine how these and other shortcomings impact the Government's ability to fight crime and protect national security. We

will also examine the government's views about various proposals being considered by Congress to update this privacy law.

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 also 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.

I thank both of our witnesses for appearing today. I look forward to a good discussion.

# # # # #

April 6, 2011

The Honorable Patrick J. Leahy
Chairman
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Charles E. Grassley
Ranking Member
United States Senate Committee on the Judiciary
152 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Grassley:

As public interest groups dedicated to limited, Constitutional government, we write to urge Congress to extend the Fourth Amendment's protections to Internet-based "cloud" and mobile location services. Specifically, Congress should amend outdated U.S. laws originally intended to protect citizens against unwarranted law enforcement access to their private information held electronically by third parties. The laws protecting such information, while robust at the time of their enactment, have been eroded by technological change. By closing the resulting gaps in legal protection, Congress can restore Americans' individual liberties in the digital age and ensure the Internet remains a powerful engine of economic growth, while preserving the tools needed by law enforcement investigations and removing legal uncertainty that may hamper law enforcement's effectiveness.

Bringing the Fourth Amendment into the Digital Age

Among the chief causes of the American Revolution was widespread outrage at the use of "general warrants" and "writs of assistance" by British officers to conduct searches and seizures without judicial oversight.[1] George Mason's Virginia Declaration of Rights, adopted mere months before the U.S. Declaration of Independence,[2] set forth the basic warrant requirements for lawful searches that were ultimately enshrined in the Fourth Amendment—which protects our "persons, papers and effects" from such arbitrary invasion by requiring law enforcement to obtain warrants issued by a court upon a showing of probable cause.

The Fourth Amendment's protection of the "right of the people to be secure ... against unreasonable searches and seizures" is the crown jewel of our constitutional liberties and our greatest bulwark against tyranny. Yet most U.S. courts have declined to extend Fourth Amendment protection to digital "papers" stored with third parties, even those reasonably expected to remain private. In 1986, Congress attempted to fill this gap with the Electronic Communications Privacy Act (ECPA), which remains the primary federal law governing law enforcement access to electronic communications.

For its time, ECPA was a forward-looking, liberty-enhancing statute. But new technologies have changed how individuals and businesses communicate in profound ways unforeseeable in 1986. For example, with storage costs plummeting,[3] more and more sensitive information once stored locally (and protected by the Fourth Amendment) is being stored remotely (where it is only partially protected by ECPA). Mobile phones track users' movement to support a variety of beneficial services and applications—yet under ECPA, this locational data may be obtained by law enforcement without a search warrant.

Congress has tried—unsuccessfully—on several recent occasions to update ECPA to keep pace with technological change. In October 2000, for instance, the Republican-controlled House Judiciary Committee voted 20-1 to approve reforms very similar to what we propose here.[4] Unfortunately, that legislation never made it to a floor vote.

ECPA Reform Would Enhance U.S. Economic Competitiveness

Cloud computing has already been a boon for global commerce and communication.[5] In coming years, this revolutionary shift is expected to generate massive efficiency gains, and cultivate economic growth worldwide.[6] Cloud computing substantially lowers overall IT costs, allows companies to switch from large and infrequent capital expenditures to consistent recurring operating expenditures, and can easily accommodate fluctuations in computing needs.[7] This makes cloud computing especially valuable to start-ups and small businesses—the dynamos of our economy.

But because most information stored with third-party cloud providers often enjoys no Fourth Amendment protection—unlike data stored on first-party (*i.e.*, local) computers[8]—even IT professionals are worried about the privacy of information stored with cloud computing providers,[9] and thus hesitate to embrace cloud computing.

Cloud computing and mobile service providers receive thousands of governmental demands for private user information annually.[10] Despite the sensitive nature of the information sought, many of these demands were made without meaningful judicial review, or any review at all—due to ECPA's inadequate protections.[11]

Protecting Cell Locational Data Will Safeguard Liberty & Foster Burgeoning Mobile Ecosystems

Most smartphones sold today include GPS transceivers and support network-based location (*i.e.*, triangulation by cell towers) when no GPS signal is available. Under ECPA, however, the standards governing law enforcement access to mobile locational information are not explicitly spelled out. Many courts have authorized such demands without requiring a search warrant—contrary to our Fourth Amendment heritage.[12]

Our proposed reforms would not only protect our constitutional liberties, but also promote the growth of the mobile ecosystem. Mobile apps increasingly use location-based functionality to deliver a variety of services to users, from navigation to localized ads to location-based social networking. These services are expected to generate $12.7 billion in revenues by 2014.[13]

ECPA Reform Will Bring Needed Clarity to Law Enforcement Investigations

Law enforcement has effectively fought crime within the constraints of the Fourth Amendment—largely because those constraints are generally clear, predictable and well-understood. By contrast, ECPA's rules governing access to electronic information are a confusing, byzantine mess. Compounding this complexity, a series of conflicting court decisions has resulted in dramatically different standards between jurisdictions for law enforcement demands for electronic information. The resulting legal uncertainty impedes law enforcement efforts and greatly complicates the training of computer crime investigators.[14]

Our proposed ECPA reforms would resolve these ambiguities by creating a single set of nationwide standards that are consistent with the Fourth Amendment. Moreover, unlike ECPA's existing rules, the rules we propose would map readily to cloud and mobile services and reflect users' reasonable privacy expectations in the digital age. Our proposed reforms would not affect the tools used by intelligence agencies and law enforcement authorities to track terrorists and spies.[15]

The Time for Reform is Now

Major decisions regarding the future architecture of cloud computing are being made right now. If Congress fails to enact ECPA reform, cloud computing services may be designed to rely on servers outside the U.S. Not only would this harm U.S. competitiveness, it could also, ironically, deny U.S. law enforcement access to cloud data—even with a lawful warrant.

We urge Congress to act immediately to amend ECPA to extend the Fourth Amendment's protections against the unreasonable search and seizure of digital documents and other electronic information. Specifically, Congress should require that law enforcement:

1. Obtain a search warrant before it can obtain private content stored online;
2. Obtain a search warrant before it can track the location of a mobile communications device;
3. Persuade a court that demands for information about the parties with whom an individual has communicated are relevant and material to a criminal investigation; and
4. Demonstrate to a court that the information it seeks through a bulk data request pertaining to an entire class of users is needed for a criminal investigation.

Indeed, at least one federal appellate court has found a key part of ECPA inconsistent with the Fourth Amendment, just as we argue.[16] By making ECPA consistent with the Fourth Amendment, Congress can avoid protracted litigation in other circuits and clarify proper procedures for law enforcement to obtain access to information with a warrant, just as the Founders intended.

In liberty,

TechFreedom

Competitive Enterprise Institute

Americans for Tax Reform's Digital Liberty Project

FreedomWorks

Campaign for Liberty

Washington Policy Center

Liberty Coalition

Center for Financial Privacy and Human Rights

Less Government

CONTACTS:

Berin Szoka, bszoka@techfreedom.org

Ryan Radia, rradia@cei.org

Kelly Cobb, kcobb@atr.org

[1] Cuddihy, William J. "'A Man's House is His Castle': New Light on an Old Case", review of The Writs of Assistance Case by M. H. Smith. Reviews in American History 7, no. 1 (March 1979), 64–69.
[2] Virginia Bill of Rights, § 10. *available at* http://www.constitution.org/bcp/virg_dor.htm
[3] Chip Walter, *Kryder's Law*, SCIENTIFIC AMERICAN, July 25, 2005, available at http://www.scientificamerican.com/article.cfm?id=kryders-law.
[4] *Cf.* Electronic Communications Privacy Act of 2000, H.R. 5018, http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.05018: and Digital Due Process, *Our Principles,* http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163
[5] Gartner, *Gartner Says Cloud Computing Will Be As Influential As E-business*, June 26, 2008, http://www.gartner.com/it/page.jsp?id=707508
[6] IDC, Worldwide and Regional Public IT Cloud Services 2010–2014 Forecast, June 2010, http://www.idc.com/research/viewdocsynopsis.jsp?containerId=223549&sectionId=null&elementId=null&pageType=SYNOPSIS. ("The cloud model will propel IT market growth and expansion for the next 20 years and will help the industry to more rapidly develop and distribute a new generation of killer apps.")
[7] Ben Kepes, Diversity Limited, *Moving your Infrastructure to the Cloud: How to Maximize Benefits and Avoid Pitfalls*, Dec. 20, 2010, http://www.rackspace.com/hosting_knowledge/whitepaper/moving-your-infrastructure-to-the-cloud-how-to-maximize-benefits-and-avoid-pitfalls/.
[8] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, *available at* http://www.minnesotalawreview.org/sites/default/files/Couillard_MLR.pdf.
[9] Andrew R Hickey, Cloud Computing Security Risks Outweigh Benefits: Survey, CRN, Apr. 9, 2010, http://www.crn.com/news/security/224202475/cloud-computing-security-risks-outweigh-benefits-survey.htm ("nearly half of IT professionals in the U.S. say the risk of cloud computing eclipses the perceived benefits")
[10] *See, e.g.*, Google Transparency Report, http://www.google.com/transparencyreport/governmentrequests/ (Noting 4,287 data requests from 1/1/10 to 6/30/10); *see also* Jon Stokes, Sprint fed customer GPS data to cops over 8 million times, ArsTechnica, http://arstechnica.com/telecom/news/2009/12/sprint-fed-customer-gps-data-to-leos-over-8-million-times.ars; *see also* Nick Summers, Walking the Cyberbeat, Newsweek, May 1, 2009, http://www.newsweek.com/2009/04/30/walking-the-cyberbeat.html ("Facebook … says it tends to cooperate fully and, for the most part, users aren't aware of the 10 to 20 police requests the site gets each day.")
[11] Tracy Mitrano, *Taking the Mystique out of the USA-Patriot Act: Information, Process and Protocol*, May 2002, http://www.cit.cornell.edu/policies/esurveillance/article.cfm ("Prior to the Patriot Act, law enforcement required a traditional subpoena in order to acquire 'routing' information, information that by and large is in the realm of telephonic communications and would not require a high level of authorization. Since the Patriot Act, a new method of what some observers have called 'rubber stamp' subpoenas has replaced that traditional authorization standard.").
[12] Orin Kerr, Third Circuit Rules That Magistrate Judges Have Discretion to Reject non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records, Volokh Conspiracy, September 8, 2010, http://volokh.com/category/cell-site-information/. ("The Third Circuit… ruled that… the government can obtain historical cell-site records under 2703(d) without getting a warrant.")
[13] Giselle Tsirulnik, Total mobile LBS revenues to reach $12.7B by 2014, Mobile Marketer, May 20, 2010, http://www.mobilemarketer.com/cms/news/search/6309.html
[14] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); *see also* In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, No. 08-4227 (3d Cir. Sept. 7, 2010).
[15] The Digital Due Process proposals would leave unchanged the Foreign Intelligence Surveillance Act and the amendments to ECPA contained in the USA PATRIOT Act of 2001.
[16] U.S. v. Warshak II at 23, http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf (6th Cir. Dec 14, 2010).