THE BROOKINGS INSTITUTION

REFORMING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Washington, D.C.
Tuesday, May 17, 2011

PARTICIPANTS:

Welcoming Remarks and Moderator:

BENJAMIN WITTES
Senior Fellow, Governance Studies

Keynote Speaker:

ORIN S. KERR
Professor of Law
George Washington University Law School

Panelists:

JAMES A. BAKER
Associate Deputy Attorney General
U.S. Department of Justice

VALERIE E. CAPRONI
General Counsel, Office of the General Counsel
Federal Bureau of Investigation

JAMES DEMPSEY
Vice President for Public Policy
Center for Democracy and Technology

ALBERT GIDARI, JR.
Partner
Perkins Coie LLP

* * * * *

P R O C E E D I N G S

MR. WITTES: All right, I think we're going to get started. Welcome to Brookings. My name is Benjamin Wittes, I'm a Senior Fellow here, and I'll be moderating today's panel. One of the great things when you put together the perfect panel to discuss an issue is that the role of the moderator can be exceedingly modest, which I hope to keep my role today in that vane.

The basic subject that brings us here today, and I'm going to actually turn things over to Orin Kerr momentarily to give actually a real briefing on this, is the question of whether and how the Electronic Communications Privacy Act should be updated.

Over the last year and half, two years, there's been a sort of remarkable set of both jurist prudential and legislative activity that has all be predicated on this question of the obsolescence technologically -– of the statute. And there have been a variety of proposals for updating it, and for making it either more protective of information that we're all increasingly leaving all over the web and other architectures, or for expanding its scope to different technologies that it doesn't necessarily now cover. The statute is relatively old, it's relatively complicated, and it was certainly written at a time when the modern communications architecture was both in its infancy and as it has developed almost entirely unimagined.

So I've tried to put together a group of people who can sort of offer sort of a very diverse sense of the equities in the issue. And what I would like to do and what we're going to have is, I will turn it over to Orin Kerr from George Washington Law School, who will give a sort of sense of the issue and the scope of the issues that are sort of contained within it.

And then at that point I will introduce our panel, whose materials you should have, who will debate the relevant equities from a variety of different perspectives.

So I'd like to turn things over to Orin now. Orin is Professor at GW who is certainly the Fourth Amendment specialist in academia whose work I find most consistently illuminating and just in -– when one agrees with him or disagrees with him, sheds just sort of amazing light on the intricacies of a set of very difficult questions, both at a technical level and at a legal level. He also blogs for the Volokh Conspiracy, and a lot of you may know his work from there. He's also a very funny, charming guy, so please make him welcome.

MR. KERR: Thanks, it's a great pleasure to be here. According to the program, this is going to be a keynote address, and I thought, oh good, I can check off that element from my dog eared copies of David Brooks' Bobo's in Paradise that I delivered a keynote address at the Brookings Institute, I thought that's pretty cool.

But this is not actually a keynote address; it's actually more of a summary of the issues. It's come to my attention that, as shocking as it may seem, some of you are not entirely comfortable with the Electronic Communications Privacy Act.

Some of you may be a little bit confused about the issues, some of you may find the statute a little bit technical, may find the questions here a little bit hard to understand. I'm sort of shocked by that, and yet, nonetheless, it's helpful to really just present an overview of what the issues are.

So what I want to do in my so called keynote that is really not a keynote is to give you an idea, an overview of what the issues are that are raised by amending the Electronic Communications Privacy Act, and to give you a historical perspective on how the technologies are changing and how they raise these new legal issues, and a little

bit of the history of how we've dealt with these issues before.

So I want to somewhat artificially, but hopefully helpfully divide the history into three basic technological eras, and I'm going to break them down into the 1960's, the 1980's and today.

So for each of these eras, it's helpful to have in mind the technologies that were in use at the time, and in particular, the surveillance technologies that were in use at the time, and then also what the status was of constitutional law, specifically Fourth Amendment law, which is, of course, important from a statutory perspective, because the state of constitutional law tells us what is open and what is closed from the standpoint of congressional action. So it's helpful to think about both the technology and the law during these three eras, the 1960's, the 1980's and today.

So let's start with the 1960's. The key period in surveillance law occurs in 1967 and 1968. In 1967, the United States Supreme Court concludes that both bugging and wire tapping are covered by the Fourth Amendment, and that, therefore, there need to be some restrictions on both bugging and wire tapping. Now, what does bugging and wire tapping mean? Well, in the 1960's, there were really two types of surveillance technologies that law enforcement were using or wanted to use.

The first one was a bugging device, a little, small microphone that could be installed in some private place to hear what people were doing in a private room, or say, hypothetically, a phone booth, and then also wire tapping devices, which was more of a -- use of a telephone could be monitored by the installation of some wire tapping device say on a public street, where somebody is listening in on a phone call that somebody is making, sending, receiving voice communications.

And it turns out that around the same time the U.S. Supreme Court was

deciding these Fourth Amendment issues, Congress was in the middle of trying to rethink its approach to the statutory regulation of wire tapping.

This had been an issue that had sort of come up in the 1930's, but over several decades, Congress realized it was going to have to come back and really come up with a comprehensive regulatory scheme for wire tapping. And at about the time Congress is finally rethinking these issues, the U.S. Supreme Court quickly decides these two cases, Katz versus The United States and Berger versus New York, basically telling Congress across the street, hey guys, whatever you do, you have to make sure that your statute incorporates these Fourth Amendment limitations on government surveillance involving wire tapping and the use of a bugging device.

Congress responds with a statute that's popularly known as the Wire Tap Act, or Title 3, Title 3 from its place in the omnibus Crime Control Act of 1968, it was the third title, and this statute, Title 3, the Wire Tap Act, whatever you prefer to call it, is a fairly comprehensive regulation of the technology of the 1960's. It handled wire tapping; it handled bugging, and dealt with them specifically as different categories of communications which were specifically protected under the statute passed in 1968.

So as of 1968, Congress had done a pretty good job regulating these type of surveillance technologies, again, bugging devices, a microphone typically, and wire tapping phone calls. So that worked for, oh, about 20 years or so, 15, 20 years, and that brought us to the period of the 1980's, when a couple things had changed by that point. First, technologically, the government had begun to use pen registers much more widely than it had before. Pen register is one of those terms which, of course, surveillance people talk about, oh, right, a pen register, that anybody outside of this extremely small band of people says what on earth is a pen register.

A pen register historically was a device used to record the phone numbers dialed from a particular telephone call. It could be installed at the phone company to record the numbers dialed from the phone.

In a Supreme Court case called Smith versus Maryland, in 1979, the U.S. Supreme Court had concluded that the numbers dialed from a telephone call was not protected by the Fourth Amendment; it was not covered by the Wire Tap Act of 1968 because the Wire Tap Act only involved the contents of communications. So the Wire Tap Act governing the actual phone calls, the actual message between two people talking on a phone, not the information about the communication, like the number dialed in order to place the call.

So law enforcement was using these pen registers more often than had been at the time of the initial Wire Tap Act, and that was not regulated by statute or the Fourth Amendment as of the mid 1980's. The second thing that it changed is that there had been the introduction of computer networks. And it's kind of surprising, in fact, maybe even shocking that in the 1980's, at a time when most people had not heard of email, Congress was worried about email privacy.

We normally think that –- we always sort of constant reframe (phonetic) is that technology has moved far ahead of the statutes. This is an example of Congress in the 1986 Act getting way ahead of the technology, actually trying to comprehensively solve a technological problem for technology that actually quite few people were using at the time.

As of the 1980's, we were talking fairly primitive use of computer networks sending and receiving email, of course, still around today, with something that had just started to be used. And then there are also remote storage sites, people who

were using these new- fangled computers couldn't store a lot of information remotely, you had to have the cassette tape, for example, to store data, so you could get some sort of an online storage site. Today we would think of this as the brand new idea of the Cloud. Storing information in the Cloud, which actually was a relatively common tool at the time when local storage was much more difficult. So the new problems consisted of really three types of things that the new technologies were not covered by in the law.

First, these pen registers, the non-content surveillance of phone call information was not covered. Second, the Wire Tap Act, which was created to cover bugging devices and telephone calls, did not include computerized communications, because the statute was limited to that which includes the human voice, and that would not include, for example, email.

And then third, there were all sorts of new problems created by the fact that computer networks generally worked by storing and retrieving information, so that was kind of a new category, stored information, that was not included in the original Wire Tap Act.

Remember, the Wire Tap Act is very much about the telephone. We might have voicemail, for example, it would be an example of remotely stored voice communications, but that is a relatively recent development. If you think back to the 1960's, 1970's, phone calls are either in real time or they're gone. So the only surveillance that Congress was worried about was the real time perspective surveillance of an ongoing telephone call. Fast forward to the 1980's, with stored communications on a computer network, now you've got third party providers, these companies that are providing internet service to customers, and they have stored records, stored emails, stored files, and the government might want access to those stored files, so the question

is what to do about it.

Congress responds with the 1986 Electronic Communications Privacy Act. The statute that really created the framework is still in place today. And that statute –- the ECPA did three basic things. First, amend the 1968 Wire Tap Act to include computerized communications by expanding the categories of covered communications to include something called electronic communications, basically data communications that did not include the human voice.

Second, Congress enacted the Pen Register Statute, designed to respond to the Smith versus Maryland case from 1979, in which Congress said, okay, we're not going to require a warrant for government surveillance of the use of the pen register, the installation of device to collect the phone numbers dialed, however, we will require a court order, it can be obtained quite easily by the government, mere certification that the information to be obtained is relevant to an ongoing investigation, but nonetheless, the statute imposed some sort of statutory regulation, court order requirement on the government.

And then third and perhaps most importantly, Congress enacted the Stored Communications Act. So this is part of the broader statute of the Electronic Communications Privacy Act, and it's designed to regulate access to the stored communications, the stored emails, the remotely stored files.

And Congress, in its wisdom, decided to sort of categorize the different ways that individuals could use these remote services and to come up with different levels of protection for each. So the two basic categories that Congress came up with were something called Remote Computing Services and Electronic Communication Services. What did that mean?

Well, the Electronic Communication Service idea is really about email, so there was one set of rules protecting email. And then the second category was about remotely stored files in the Cloud. If you were to hire a service in which you could remotely store your data, that would be what the statute called a Remote Computing Service. And so the Congress came up with rules that regulated when the government can go to these different providers and say we want the stored content held by the provider, relating to a particular customer who may be involved in crime, and, for example, the government wants to compile email that is stored on a provider.

And then the statute also dealt with the flip side of this problem, what if the provider wants to disclose information to the government, when can it do so. So effectively there's a statutory ban on disclosure unless and exception applies.

The broad goal of the 1986 Stored Communications Act was to create kind of a Fourth Amendment like set of rules that would apply to the special relationship in the case of third party providers.

So think about the difference between online privacy and offline privacy. Offline, in the physical world, you would create Fourth Amendment privacy or just practical privacy by storing things in your private places. If you have something you want to hide, you might put it in your bedroom, you might lock it in your basement, you might put it somewhere that you know is enclosed that you control. In the online setting, you control your own device, you control say your own laptop, but mostly you're contracting with third party providers, whether Google or Hotmail or Yahoo, and you want to purchase or in some way contract with these third party providers to store your material.

So we have this third party relationship that's introduced, and the goal of the statute that was enacted in 1986 was to create kind of a Fourth Amendment like

regime by statute, with the understanding that how the Fourth Amendment applied, as of the 1980's, was entirely unclear. Nobody quite knew if when the courts got to these issues of remotely stored email or files stored in the Cloud, whether they would say this is more like pen register information in Smith versus Maryland, it's been disclosed to the provider, therefore, it's not protected, or courts would say, no, this is more like private letters or phone calls, phone communications under Cat versus United States, protected by the Fourth Amendment.

So Congress is creating kind of a statute with awareness of the fact that the Fourth Amendment rules are uncertain, and Congress certainly knew that at some point the courts might try to take over this area, but in case the courts did not, the statutory protection would be there, that was the basic idea. At the same time, to make matters just a little more complicated, in case they're not complicated enough for you, Congress decided not to give the full Fourth Amendment level of protection to most stored communications.

So there's a warrant requirement for some kinds of communication, but on the other hand, the government can access private communications, contents of communications, with less than a full search warrant in other settings, and then also Congress concluded that they would not include a statutory suppression remedy, instead, there's a damages remedy, so it's kind of a junior varsity statutory form of the Fourth Amendment, not the full level of Fourth Amendment protection, if the Fourth Amendment applies fully to these sorts of facts.

So that was Congress' effort in the 1980's, at least, to my mind, a pretty good job given a quite difficult set of problems that Congress was trying to resolve. And again, Congress was trying to regulate an area of privacy law long before most people

are actually using the technology, so Congress is way out ahead, or at least it was in the 1980's. Fast forward to the third major era, the present, and now Congress, once again, is behind. So there have been two major technological changes, and then some constitutional changes which have also altered the terrain, which really frame the issues for today.

The two technological changes of the last 20 years, first, the use of computer networks has become much more common, much more sophisticated, much more all encompassing, and it's also much more diverse in terms of the types of information that the government might want, that might be available, and the type of information that's on the network that users are making available.

So, for example, the internet of the 1980's would be email or remotely stored files. Today it could be email or other stored messages, like text messages, it could be remote stored files in the Cloud, but it could also be web surfing information, it could be information relating to any particular application of a computer that you can think of.

For every application, there's data that's been sent out into the network, so the issue becomes how – what surveillance rules apply to that particular type of information. So the use of computer networks has become much more sophisticated, leading to new government surveillance methods for collecting new types of information that are available on the network.

The second major category is the introduction, or at least the popularization of the cell phone. I'll hold up my cell phone, which is my watch for purposes of this. So the cell phone introduces many interesting, new surveillance issues, but the most important one is that it brings to the forefront this question of location

information.

So in the case of telephone wire tapping and bugging in the 1960's, the wire tapping could occur anywhere the communication was. The bugging would have to occur in the room where the communication would be picked up. But those methods of surveillance did not generally reveal location information about where somebody might be located.

Similarly, in the 1980's, the introduction of computer networks or the pen registers did not generally reveal location information. Cell phones are different. For those of you who know roughly how cell phones work, they are not magic black boxes, contrary to the belief of at least some judges in this area, they are actually devices which are in communication with a network, and the phone company needs to know roughly where the phone is located in order to know how to send calls to the phone and how to pick up calls from the phone. Those of you that have turned your phone on and it says it is searching, it is not searching for love, it is not searching for a nearby restaurant, it is searching for the network, to basically tell the network, hey, I'm over here, and that then sets up a relationship between the phone and the network in which the network knows where the phone is located to allow the phone to work.

That means that the phone company has records as to roughly, roughly an important word here, as to roughly where the phone is located, which means that the phone company is collecting information, and if asked to do so, may prospectively collect more information about where people are.

Now, where people are isn't necessarily where their phones are, but most of us keep our phones with us, and so as long as your phone is on, it is sending this location information to the network. That information can be very important in criminal

cases, and yet also, of course, raises important civil liberty concerns of the government watching where people are physically located whenever their phones are on, which is most of the time. So these two new technologies really raise some new surveillance issues. In particular, the cell phone introduces this idea of what to do with location information and how should the statute treat that.

In addition to the technological changes, there are some important constitutional changes. The courts have finally, it took them a long time, but the courts have finally started to think about how the Fourth Amendment applies to these new kinds of surveillance. And the decisions we have are tentative. The U.S. Supreme Court has not weighed in on these questions yet, but they offer the following tentative suggestions, again, tentative ideas.

But that is, first, the Sixth Circuit in a case called United States versus Warshak, from last year, concluded that the contents of stored email are fully protected by the Fourth Amendment. So that would institute a full probable cause requirement backed by the exclusionary rule, at least while the Supreme Court says the exclusionary rule is still around.

So we have a full Fourth Amendment protection for email, at least according to the Sixth Circuit's decision in Warshak from last year. If other courts adopt that rule, and if the U.S. Supreme Court adopts that rule, to my mind, that largely preempts one of the major statutory decisions by saying essentially to Congress, it doesn't matter what you do with privacy protection in stored email because that's going to be fully protected by the Fourth Amendment rule.

Generally the statutory question will be whether Congress is regulating, at what level of protection, and sort of the full level of protection is the full Fourth

Amendment standard, so once the U.S. Supreme Court has reached that decision, presumably Congress won't have much to say about it.

So that's been the tentative decisions of the courts so far. There have been some efforts by other courts to get into this question. There have been three circuits that have tried to weigh in and then had their decisions overturned or withdrawn or overturned *en banc*.

So the Fourth Amendment issues here not at all settled, but we have at least one clear Circuit Court decision saying that email is fully protected when stored on the server. On the other hand, we have precedence so far indicating that non-content information involving internet communications is not protected under the Fourth Amendment. The lead case here is called the United States versus Forrester, it's a Ninth Circuit decision from two or three years ago in which the government had installed a surveillance device at the internet service provider of a suspect and recorded internet protocol addresses and email addresses, the two/from addresses that individuals had emailed, and also I believe the internet protocol addresses of the web sites that the person was visiting, as well as the overall volume of information that was recorded.

Effectively, kind of internet equivalent of pen register information which the Supreme Court had held in Smith versus Maryland was not protected under the Fourth Amendment, and the Ninth Circuit concluded by analogy that the internet equivalent of that information is not protected either.

So at least so far we seem to have emerging this distinction between contents, which are presumptively protected, and non-content information, which is not protected, based on the tentative Circuit Court decisions that have been handed down so far. We also have some decisions that are just working their way through the courts on

location information. The Third Circuit handed down a decision, which, to my mind, was rather puzzling, involving what are the rules for prospective cell site location information. So the location information is generally of the cellular powers that were in communication with the phone, and that can be prospective or retrospective, and this distinction runs through the statutes here.

The difference would be prospective surveillance is some sort of ongoing surveillance, figuring out information to be collected in the future. You can think of a live phone call, where the call has not happened yet, but the government wants to listen into it in the future. And you can compare that to retrospective surveillance, there's some stored record that exists that the governments wants access to.

The line between prospective and retrospective can be hard to draw, and yet you can see the difference in a case where the government comes into the scene, says, oh, we want to know whether a suspect was in this town last month, that's a case of retrospective surveillance, whereas we want to know where this guy is going tomorrow would be prospective surveillance. The Third Circuit didn't quite answer how the Fourth Amendment applies to location information, but suggested that, at least in some circumstances, location information might be protected by the Fourth Amendment.

I think the best reading is Smith versus Maryland, the 1979 case on pen registers, is that actually the location information is not protected under the Fourth Amendment, that's been the traditional understanding of the issue, because like numbers dialed, it is information needed to connect the call, which is sent to the network, sort of is network generated, network used information.

But at the same time, I think it's fair to say that the Fourth Amendment issues relating to location information are presently uncertain. That uncertainty is aided

by a series of cases involving GPS information, currently working their way up to the United States Supreme Court.

The Justice Department recently asked the Supreme Court to review a D.C. Circuit opinion, concluding that at least long term use of GPS devices, in that case I believe installed on a car, can constitute a search under the Fourth Amendment. On the other hand, there's a recent Ninth Circuit case concluding that the same type of GPS surveillance is not a search under the Fourth Amendment. Right now there are petitions that are before the U.S. Supreme Court. If I had to guess, I would guess that the Supreme Court will agree to review this issue.

GPS location information, Fourth Amendment issues, are quite possibly, probably should be, but quite possibly distinct from Fourth Amendment issues involving cellular location surveillance. At the same time, it's possible that what the Supreme Court does with the GPS cases will shed a lot of light on what the answer is on the cell location information.

And you can think about what the difference is between those two types of location information. The cell site location information is information from the network. We're talking about gathering information collected by the network provider, whereas in the GPS setting, it is typically a device owned by law enforcement, installed by law enforcement on say a suspect's automobile, not a network issue, but rather an installed physical device.

It may raise different issues under the Fourth Amendment or it may not, depending on what the Supreme Court wants to do. So where does that leave us going forward? What are the issues that are really presented by this changing technology and changing Fourth Amendment law or uncertain Fourth Amendment law? I think there are three basic

categories of questions.

First are the content questions. What are the rules for the government compelling third party network providers to disclose the contents of communications, whether it's email or files stored in the Cloud? Is a warrant required by the Fourth Amendment? If a warrant is required by the Fourth Amendment, perhaps that means that the content regulation in the current statute has effectively been preempted, and maybe that's no longer an issue for Congress to really deal with.

At the same time, the Fourth Amendment issues there are unresolved, there's still some room for Congress, and, of course, if the courts conclude that the Fourth Amendment does not extend so far, Congress can regulate, if it so chooses. So that's one set of issues, what are the rules for compelling content from providers.

The next question is, what are the rules for compelling non-content information from providers, so that could mean ongoing surveillance of internet protocol addresses or to/from email address. Congress has traditionally used a different standard, depending on whether the surveillance is ongoing, prospective, or past surveillance, retrospective. Adopting the pen register standard from the 1986 act for electronic communications, that was part of the Patriot Act, which is that mere certification standard for ongoing, non-content surveillance.

And then, on the other hand, retrospective surveillance, gathering stored records, would be, for some communication, some type of information, a mere subpoena standard, which is basically a relevant standard, very easy for the government to satisfy, for some information, and then a heightened standard for other information collected by the provider.

And then the third basic category is location information. And this is, I

would guess, the hardest of the issues, in part, because it's the newest set of issues. So what should the rules be for compelling providers to disclose location information from say cellular phones, and you can think of that either prospectively, on an ongoing basis, or accessing stored records.

And you can break that down into really two issues, one issue is what's the threshold, whether it's relevance, specific and articuable facts, kind of what in Fourth Amendment law we would think of as a Terry stop standard and in the statute, it's called a 2703-D order threshold, or a full warrant probable cause requirement, that would be a third option.

And then also, once we have the threshold settled, we have to figure out over how many records can be collected at that threshold, so think about location records, is it a day's worth of location records that can be obtained, a week's worth, a month's worth, a year's worth, forever, what's the time period over which the location information records can be disclosed.

The location information issues are issues that Congress tried to deal with, I guess this is going back almost about ten years ago, but has really failed to ever pass a comprehensive statutory answer really at any time to the location information.

So what we're left with right now is a series of cases in which the courts grapple with what the standards are based on kind of remnants from the 1986 act, which no one ever thought would apply to location information. And we're sort of stuck with these pre-existing categories. I think that's the area that is the one most demanding of a statutory fix, but if I had to guess, it's also the area that is the hardest going forward. Should there be a warrant requirement, for example, for location information, or should some lower threshold be required? Does it matter on how much resolution there is on

the location information? Should there be a different standard for the suspect that's in this room as compared to the suspect? You know, we can confirm the suspect was in the state of California. What level of certainty should be required for the government to get that kind of information is I think a set of very tricky and important issues.

So to summarize, the things to think about are access to content records which may be settled by Fourth Amendment law, but maybe not, non-content records, where we have a series of thresholds starting that low subpoena standard, going all the way up to the warrant standard that Congress can choose from, and it's pretty clear that, at least so far, there's no Fourth Amendment issues, and then location information, accessing location information for, for example, the location of a cell phone, where the Fourth Amendment issues, at least right now, are not particularly settled, and Congress has never really comprehensively tried to regulate that particular issue, and I think that's the thorniest of them. So thank you for listening to my so called keynote address, and I look forward to the panel. Thank you.

MR. WITTES: I just want to express my appreciation, because I told Orin that this is quite an unenviable task actually, explain the history and current issues and technology and law associated with the Electronic Communications Privacy Act and Stored Communications Act, and don't take more than a half an hour to do it, and make sure that people stay awake. And so you're all awake, he took half an hour, and he gave an incredible overview of the issues we're going to discuss, so many thanks.

So I wanted to organize this panel in the following way, which was to say there are groups and entities that are making a case for change, which, in the statutory landscape, which, generally speaking, the government is not enthusiastic about or not as enthusiastic about.

And so what I would like to do is have our civil liberties and industry related panelists talk first and talk about sort of why the statutory landscape, as it exists now is, from their point of point, inadequate, and then have our government speakers talk about what some of the cautionary notes that one might associate with change surgery, radical and minor to the existing statutory architecture and what that might mean for investigations and collateral interests that may also be important.

So I'd like to start with Jim Dempsey, whom I've known for close to 20 years now, since I was a cub reporter at Legal Times many years ago, and Jim was on the Hill. Jim is a long time civil liberties activist in cyberspace related issues and other issues, and put together a sort of remarkably diverse coalition of civil liberties and industry groups that are interested in this, with a very sort of coherent document describing proposed reforms to the statute. And I'd like -– Jim, take a few minutes and walk us through what's wrong with the current architecture and what you guys are proposing.

MR. DEMPSEY: Okay. I'm checking my blackberry here, not out of disrespect, but just to check to see if what I think has happened has happened, which is that Senator Leahy was going to be introducing legislation today on ECPA reform, so this is a very timely panel. Senator Leahy, Chairman of the Senate Judiciary Committee, is the author really, along with Bob Klostermeyer, the author of ECPA, has shepherded it through the Senate in 1986, has been saying for a number of years that it's outdated and in need of update, that he's committed to working with all parties, including law enforcement and industry, to update the legislation, and he's planning to introduce legislation today, a bill which really will just be the beginning of a process.

As Orin said, these are some very, very complicated issues here, and

working them through is not going to be easy. So the introduction of legislation today is really the next step in an ongoing process.

Orin did a great job of laying out the issues, and in a way, I'm going to echo and repeat a couple of his themes, a number of his themes, but I think it's useful to hear the same thing several times given the complexity of this issue.

My starting point really on this issue is a recognition that there are very significant law enforcement and national security interests at stake. Clearly, the government has tremendous responsibilities in terms of crime prevention and investigation and prosecution, just very significant responsibilities on the national security side. And even from a privacy perspective, my starting point is that there is no information which is legally off limits to the government. I mean the government under our system has the power to plant a bug in your bedroom and listen to what goes on in your bedroom. They certain have the power, authority to, and should have the power and authority to access email and all the kinds of associated data with it and all this rich, rich, rich ocean really of information that we generate in our daily lives.

So the question becomes -- and it's really the question in our society, which is, what are the standards, what are the checks and balances that should apply? And again, echoing a theme that Orin outlined, we have currently, and I believe it is a correct framework, a sliding scale, sort of a set of building blocks of the investigative process as the government becomes more certain of its focus, more certain of its suspicion that someone is engaged in illegal activity. And as the government's access to information becomes more intrusive, the standard applicable becomes more stringent up to the constitutional standard, the Fourth Amendment standard, which is the standard of a warrant issued by a judge based upon a finding of probable cause to believe that a

crime has been committed, or is about to be committed, and that the search would uncover evidence of that crime. And I think in any effort to either judicially or legislatively to address the implications of modern technology, it's important to recognize and maintain that set of building blocks.

Orin gave a brief overview, a historical overview of the effort of both courts and the Congress to take this very, very broad and general language of the Fourth Amendment and apply it to technology as technology changes. And Orin I think started his history in the 20th century. I think he can go back to the 19th century, and I think history does help us understand where we are and sort of what the context and framework is.

In the 19th century, the Supreme Court held that the Fourth Amendment protects letters in the mail, and that it requires a warrant issued by a judge, that is, a search or seizure to open a letter. Even though you voluntarily give the letter, in fact, to a government agency, you surrender control of your mail to a government agency, and yet you still have a Fourth Amendment right, held the Supreme Court back in the 19th century.

In the 1920's, the Supreme Court held that when you voluntarily surrender your telephone conversation to the telephone company, you lose your Fourth Amendment protection, said the Supreme Court. Anybody should know the Supreme Court said, that your telephone call passes through the wires of a third party, the telephone company, and you've given up any hope of privacy there.

Congress responded in the 1930's and passed a law that seemed to say that you could not wire tap. A very clever lawyer at the Justice Department of the FBI, J. Edgar Hoover, read that carefully, and it said it's illegal to intercept and disclose, so

Hoover said, well, I'll intercept, I just won't tell anybody and that will be fine.

But ultimately, again, the courts, over a series of decisions culminating in the 1970's, ruled that the telephone call is pretty much like the letter, constitutionally, as it passes through the telephone company, it's protected by the Fourth Amendment, and famously held, the Fourth Amendment protects – stated that the Fourth Amendment protects people, not places.

And then again, technology continued to change. 1986, ECPA, as Orin said, at the time, a very good, very sightful effort to address then emerging technology, both the wireless technology and the data communications technology now represented by the internet. 1986, of course, was light years ago in terms of technology, in terms of internet time, www didn't even exist in 1986, cell phones were relatively rare, a device, et cetera.

And if you look at the trend of technology since 1986, just this –- the way it's become woven into our business and personal lives, the amount of information that is now generated electronically, and the trends that Orin referenced, storage, the way that this information no longer is a femoral, in the way that a telephone call is, and that it's no longer physical, in the way the letter is, the letter, just one or maybe two copies of that letter, you put it in the mail, and maybe you keep a copy, but those are the only two copies.

In a way, you have to think of the internet as a copying machine, making copies of this communication, and now, increasingly, those copies are held by the third party, and how do we deal with that?

ECPA deals with it imperfectly. Orin didn't even go quite into the depths of the complexity and imperfection of this, but if it's in transit, it's fully protected by the

Wire Tap Act, if it's in storage waiting to be opened, less than 181 days old; it's protected by the warrant requirement. After 181 days old, it becomes subject to a subpoena. A subpoena, I always say, is Latin for no judge has ever seen this. Subpoenas are not approved by judges; they're issued by prosecutors, sometimes given in blank to the FBI agent to fill out in the course of an investigation.

The Justice Department maintains that as soon as the email is opened, it becomes unprotected, available with a subpoena, Ninth Circuit has rejected that, the rest of the country remains uncertain. So you have this mishmash of rules, and yet it's the same content, and we all treat it as if it were the same, that the email in transit, the email in storage, the email here on my device even when I'm not connected to a network, the email that you print out, all the same content, and yet, increasingly, it sits in a place where ECPA says it's unprotected, and where the courts, but for the Sixth Circuit, have yet failed to grapple with it.

Basically the Supreme Court held in Warshak that ECPA is now unconstitutional to the extent that it allows information held by a third party, content of communications, unconstitutional to the extent that it allows that to be accessed by the government without a court order. So I think while the courts are likely to continue trending in that direction, you have one circuit out of 11 or 12, it could take a very long time for the other courts to catch up, meanwhile, you've got questions of what are the exceptions, there should be exceptions, there will be exceptions, who gets reimbursed and how do you deal with that, are carriers immune for complying, a whole host of other issues that are addressed in the statute, which, if you leave it just to the courts, would have to be worked out case by case, creating further uncertainty.

We can go into the same issues on location. I think I'll leave it there

now. Ben is eager to move onto the next speaker, and I am, as well, so just barely scratching the surface, but I hope you get some sense of the importance of updating the statute while preserving the critical law enforcement capabilities and the sort of building blocks approach to investigations, protecting the most sensitive information through a constitutional type standard, this warrant requirement.

MR. WITTES: Thanks, Jim. So our next speaker is Al Gidari, who is a lawyer at the Perkins Coie firm in Seattle. Al represents a variety of industry related clients, none of whom he is here representing today, he's here in his personal capacity. But I've asked him to talk about sort of some of the industry concerns that have caused sort of, on a policy level, a sort of effective alliance between civil liberties interests and industry interests on sort of one side of this debate.

MR. GIDARI: I'm a technology lawyer.

MS. CAPRONI: I'm from the government, I'm here to help.

MR. GIDARI: And we work together, it's really good. You know, I love these conferences because they tend to be absolutely divorced from reality, and people spend a lot of time talking about changes we'd love to see, that lawyers write, that they write for interest groups, that in the field, absolutely nobody understands.

There's a whole common law of ECPA that occurs today without the intercession of a legislator, an academic, deference to my good friend, Orin, a civil liberties person like Jim, or even the government.

You know, every day decisions are made about what the law means by people who tend to be about 28 years old, may have graduated college, they typically say the same thing over and over again, and so repeat the insanity, if they did it wrong the first time, they'll do it wrong the next 52 times. Those are the people that work on the

front line of most providers who receive the legal process and have to evaluate it and decide whether to give your email away or not.

That is where the common law develops. And where some people see uncertainty, some of my friends in government would call that elasticity. And that ability to have an elastic decision results in an incredible disarray of procedures and policies amongst providers.

Some in the privacy community have said, if only we knew those policies, people could make rational decisions on which provider to use. Would you use – I won't pick names, but you can pick out one or two big carriers, would you use them if you knew they were rolling over and giving everything to the government without looking twice, or would you go to somebody that used encryption or security or data and applied the strictest rules possible?

Well, I mean that's a good question. Congress, on the other hand, is trying to make decisions about what to change in ECPA and how to apply some uniform standards. Everybody loves clarity, the more clarity we get, the better, but they're doing it without data. How many phone records are captured every year, anybody have a clue? Anybody know what happens to them when they're captured? How many times are cell phones pinged by the government every day, anybody know? Anybody know what happens to that location when it is captured? How about your emails, anybody know? We have an absolute absence of data and yet we're going to ask Congress to make decisions on what the appropriate standards are.

I think actually kudos to the government for trying to make their case about why they need enhanced techniques. At least they're coming forward and saying here are the circumstances under which we need better tools and better access. So that's a good

thing, but where's the evidence?

Some of it you can't share because national security comes into play. Some of it certainly could be shared, but it is not. And some of it historically is available by reading the cases that ultimately do get litigated and reported, but those are old stories and generally not interesting and typically don't get picked up by the media because the media would prefer to go to hearings where congressmen attack companies, and argue about the privacy practices that are in play, and location is a great example. My good friend Orin is talking about location in cellular networks, that's yesterday's world, right. We're going to legislate for cell phone technology that is rapidly being supplanted by operating systems on smart phones.

So if I were standing on the corner and I turned to my friend and said I'm on Fifth and F Street, my oral communication is protected unless I don't have an expectation of privacy, and if the government wants to wire somebody up or do whatever, there's a process for that.

If I put in an email or a tweet that I'm Fifth and F, that's protected, that's my content, I'm telling somebody that. Now when I program my smart phone to automatically tell somebody where I am, how does that magically get converted from content into network information that is something the government can get in a subpoena? Why is, when I program any device I have to communicate with somebody else, anything other than the content of my communication? And then when that provider obtains that information, stores it, strips it of your personal identity, isn't it still content and protected? Can the government get email just because they don't know who sent it? And then if the provider, with your consent, wants to turn that content around and share it with others and say, hey, here are all the places that are near you where you stand right

now, isn't that the content of communication? And yet we have this whole debate about location information and what standards to apply as if we're speaking with a capital L, and that location is ubiquitous in its nature and form, and one rule will fit all of those cases.

While I think Senator Leahy is doing great work on crafting a solution to this, it will inevitably fall short because it does not actually encompass the whole framework of the location ecosystem that's out there today.

So we end up with a hodgepodge of, in the end, the common law of the provider making a decision, as is done every single day on location today.

It's also interesting -- content is content, I don't care how many times you try to repackage it into something else, content is still content, and the standards that we try to apply that give lesser protection to that content inevitably falls short, as well, when people stop and think about it.

It is true that, if you have a Facebook account and you post a lot of stuff on the wall for a lot of your friends to see, maybe your expectations of privacy are a little bit less than that. But it's never been the case that just because you talk to ten people, that your content of those communications somehow were less protected as a matter of Fourth Amendment law.

You're entitled to talk to as many people as you want, and your words are every bit as protected, unless you do so in a way where there's no expectation of privacy. And yet we seek to find ways in the statute and otherwise to redefine what Facebook is, to redefine what the Cloud is, and to give it, in some sense, less protection.

I do think that finally stars are starting to align a little bit. And the government actually is with a small G, not with a big G, they get to talk out of both sides

of their mouth sometimes. We'll have the Federal Trade Commission telling you that every user has a reasonable expectation to privacy in everything that they do online; all of it should be protected. You should not have your information used in a way that you didn't expect, and to the envy of every U.S. attorney out there, they can get a 20 year sentence if you abuse it with a consent decree.

Yet at the other side of that coin, the government files briefs and says, you don't have any expectation of privacy in anything you've given to a third party. And yet I think today, and Senator Leahy's bill will go a long way towards this, the government will actually get a capital G and will end up I think with a more uniform approach to this. And I think that, in essence, that clarity will serve everybody very well, because I think the last thing you want really when it comes to your privacy is a 28 year old customer service representative deciding what ECPA really means. Thanks.

MR. WITTES: Thank you very much. So I'm going to turn it over to Valerie Caproni, who's the General Counsel of the FBI, to give us a sense of the sort of investigative stakes in raising the bar here, and how as a practical matter is this sort of content and location information used, and what would be the consequences in real life as an investigative matter of making it more difficult to get it.

MS. CAPRONI: Thanks, Ben, and good morning, everybody. Who would have thought that on a rainy Tuesday morning, this many people would come to talk about ECPA? Reading the materials that we were given for this, it struck me that one of the things that might be useful to talk about is really how investigations use the data, what do we gather and why, because in some respects, I think some of the people who talk about this seem to think that law enforcement just sucks up like a vacuum cleaner vast quantities of digital data and then peruses it just kind of for the purian

(phonetic) interest of looking through other people's emails, and that the solution to keep that from happening, which I would agree would be a bad thing, is to impose increasingly high standards and higher hurdles that law enforcement has to jump over in order to get to digital data.

At the end of the day, there's a lot of policy judgments that have to be made here. I'm sure with Senator Leahy's bill, there's going to be a lot of discussion about what is the right policy balance. But part of that policy balance has to be the legitimate needs of law enforcement, because if you don't protect those needs, you're creating a concomitant risk to public safety and to the national security.

So let me start with, whatever you may think of law enforcement, their investigations tend to be fairly methodical, or that's what they're taught to do and that's the goal of the investigation. And they will gather information that is of interest and of value to that investigation, and they try not to gather information that is of no value and of no interest. It's not always possible to do really surgical strikes on the information that you gather, but that still is the goal, because we have limited resources, we have limited people who can do this. As you may have heard, FBI has certain issues with information technology, so we don't really want a lot of data that's not pertinent to what we're doing.

So with that sort of overarching, let's talk about sort of types of investigations where we might be looking for digital data. So a lot of times, the way law enforcement works is that we start with a suspect, and we're going to work to see whether, in fact, the suspect has committed or is committing a crime. So let's talk hypothetically.

Let's say we have an informant of unknown reliability who comes to us and he says, John is a drug dealer, well, an informative, unknown reliability is not alone

enough to do much of anything with. You can't get a search warrant with that because you don't know whether the information is reliable or not, and you wouldn't want to. So what law enforcement wants to do at that point is to see whether or not the informant is telling the truth, is John a drug dealer. So there are a lot of things we can do without dealing with digital data at all, and that we can do it without a warrant, and we can do it without a subpoena. We can conduct physical surveillance of John. We can follow him around and see where he's going, is he going to places that are known drug locations or is he going to places that appear to be stash houses, et cetera.

We can talk to his neighbors; we may even lie to his neighbors about why we're talking about him in order to see whether the neighbors see unusual comings and goings from John's house.

We may issue an administrative subpoena, which AUSA will not see, because –- we can do that because this is a narcotics investigation. We may issue an administrative subpoena to get his telephone records of both his home phone and his cell phone to see whether the numbers that he's calling or are calling him are numbers that we know to be associated with other drug dealers.

If things look promising, we may get a pen register and trap and trace device on his telephone. Just for those of you who don't know, a trap and trace is sort of like a pen register except it's for incoming calls. That used to be very exotic back before we all had caller ID, now it's much easier to do, but it gets both the phone calls incoming and the phone calls outgoing. We may even put on a slap on GPS device onto his car. A slap on GPS device is a device that we attach to the car, we don't need a warrant to do it, we can do it because it's observing that car, it's telling us where that car is during times when the occupants of the car don't have a reasonable expectation of privacy because

it's out in public space. So we might do that, we might not.

We may go for his bank records, issue a grand jury subpoena to his bank to find out whether the amount of money going in and out of his bank account is consistent with the style of living that we're seeing, or is the style of living radically higher, suggesting that perhaps there's cash income that is not flowing through is bank account. We can do that with a grand jury subpoena, we don't have to go to a court.

We were talking a little bit about location; I want you to start thinking about location, because when we get someone's bank account records, part of those records will show ATM withdrawals. That gives you a really good idea about where someone has been at particular times, because they had to be at the ATM in order to get their money. We may task an informant to buy drugs from John. We may even have the informant wired up even with a video camera to go inside John's house. Very substantial invasion of privacy, does not require a warrant, does not require a subpoena.

There is process; it's all internal, departmental process. The Attorney General has issued guidelines for how you can do that, we would follow those. But the point being, you have an invasion of John's privacy, but it's done as part of an ongoing investigation and without court intervention. So that would be one way.

So in that scenario, we've gotten a lot of location information, we've gotten records from banks, which are very -– lots of private information that you can get from a bank, and we've gotten telephone records, and maybe even installed a pen registered device, so we've gotten some digital data, but it's all metadata type non-content information. So that's one way investigations run.

Let's look at another type of investigation, where we start with a crime, and we don't know who committed it. So let's say we have two murders, different times,

but the exact same MO, and it's a bizarre MO: a green rope was used to strangle the person and they were left without shirts, but with their pants on, so a very odd MO, two separate locations. So what might we do at that point? And let's say there's no -— the DNA that's on the scene doesn't match to anything that we have in our databases, so we've essentially got no leads on this person.

Well, one thing that we might do, and it might be very useful, is to serve a 2703-D order under ECPA to get the cell powers that would cover the areas of the two murders, to get them to give us the records of what cell phones pinged your tower at or around the time of the two disport murders.

We then cross-correlate those records and see do we have any common cell phones that were pinging the towers that covered the area of the murder at or around the time of the murder. If we do, that's great, it's not proof positive, it's not even probable cause, but it's only good circumstantial evidence and it will give us some suspects to look at once we figure out who belongs to those cell phones.

Along that line, just be aware -- and I think somebody, either Jim or Al just sort of referenced this -- cell phone tower information is not latitude and longitude. If we got the cell towers that cover this room, it wouldn't tell us that we were in this room. It probably is going to cover a much larger area than that, will cover probably down to whatever the next circle is up to Dupont Circle, it kind of depends how big an area it covers, how many towers are in the area, is it an urban environment or not, but it'll give us kind of a general area where that person would be.

So in that case, we would have had to have gone to a court, shown relevance, the court would issue the order, we could get the records and off we go. Still no content, metadata very important in that kind of an investigation, gives you a lot of

help in trying to figure out who the suspect is.

But our need for records are not limited to metadata. I wish it were; it would make this whole discussion much easier because I think we would probably all reach agreement pretty readily.

Sometimes we actually have needs for content. And I guess from law enforcement's perspective, my concern is that we not end up with radically different rules that govern physical hard copy documents versus what governs electronic documents, because that would seem, to me, from a law enforcement perspective, to be an odd dichotomy. So let's think about that. So let's say we have a big, white collar case, okay, a big fraud. The FBI suspects that a company has engaged in financial shenanigans, they've managed their company's earning, we know that something went wrong because they just restated their earnings, so we have reason to believe that there was some fraudulent conduct.

We're pretty sure because we operate in the same world as everybody else, their email records and the drafts of the various financial statements will be good evidence and will help us figure out whether this was a rogue employee or was actually management earnings by the management of the company.

We can serve a grand jury subpoena on the company asking them for all of the drafts of all their financial statements and their emails, right, so the emails that are on the company.com account, that relate to the restatement or to their prior financial statements that were misstated. They would give us those records. Now, the company might argue, and this is some of the complexity of the statute, they may argue, no, wait, we are an electronic communications service providers, vis-à-vis our employees, and therefore, you need to get some other process rather than simply a grand jury subpoena

in order to get the content of our email.

So we may go around and around on that, but basically we'll be able to get both their paper records and the content of their emails in order for us to continue with our investigation.

Footnote, if we had to get a search warrant at that point, we couldn't do it, because we don't have close to probable cause that the company has engaged in felonious conduct. So for white collar cases, it's very important that we be able to gather the documents, whether they're electronic or physical, that provide evidence of whether there's been misconduct.

So let's change it a little more, and let's say that we have a whistle blower who comes in with some other white collar case, we, again, don't know whether this person is reliable or not, and they tell us that the company is doing something bad, maybe they're selling adulterated food, adulterated drugs, that they're engaged in an ongoing environmental crime, something, but it's an ongoing crime, and it gives us the opportunity to do something proactively. Now, in white collar cases, and for all of you who have been very frustrated because you feel like nobody has gone to jail for the Wall Street excesses and the mortgage fraud problems, et cetera, et cetera, that was a situation where it happened and we're investigating backwards.

White collar cases, much better to investigate it when it's ongoing if you can act proactively. And on that regard, think about the Gallant case in Southern District of New York that just ended, where they convicted someone for insider trading based on wire taps, where they actually intercepted the tips and then saw the trade afterwards. So in white collar case, it's helpful to have prospective investigations.

So here we've got the possibility of a prospective investigation, and our

whistle blower says, look, the evidence that they're doing this is contained in the electronic company documents that are stored, they're actually -– the company doesn't store them on site, they store them with Amazon's Cloud or somebody else's Cloud. So we've got the documents that show ongoing criminal conduct in the Cloud. If we notify the company that we want those records, we will have just upset the apple cart in our ability to do a prospective investigation, so that's not good from a law enforcement perspective.

If those records were hard copies and they were sitting with our mountain in a storage bin somewhere, but they had been provided to a third party, we could subpoena the third party. The question is how do we get those records now under the Electronic Communication Privacy Act? And how should we be able to get those records?

My view is we ought to be able to subpoena them. They're with a third party, the company has given them voluntarily to a third party, from a Fourth Amendment perspective, a subpoena should suffice, from a law enforcement perspective, that's what we want to be able to do, is to be able to get those records, get them surreptitiously so that we can continue with our ongoing investigation and not have people doing things to thwart our investigation like destroying documents or otherwise covering the tracks of their misconduct.

So I think I probably used up my time for now. But I think those are the issues that we struggle with, is how do we do our law enforcement investigations consistent with a statutory structure that is very complicated.

MR. WITTES: Thanks so much. Our last speaker before we go to questions is Jim Baker, who's the Associate Deputy Attorney General and who has

handled a wide variety of surveillance issues both in his current capacity and prior capacities at the Justice Department, and I will turn it over to him.

MR. BAKER: Thanks very much, Ben, I really appreciate your having this panel; I really appreciate the opportunity that you've given us to discuss these matters. It's very important, as some of the folks have referenced, that the public does have confidence in what it is that the government is doing in this area.

And so I think, I'm not sure, I think it was Jim, I'm not going to show up today with a stack of documents to disclose under FOIA that will reveal everything that the government is up to, but it's important that we're out here talking about these issues, and so thanks to you and thanks to Brookings for hosting this event.

One of the advantages of going last on the panel is that I get to hear what everybody else has said. One of the disadvantages, that everybody has touched on a variety of things that I was going to talk about, so I've redone my notes here and we'll see how we go. But one thing I wanted to highlight, first of all, is that we are working on these issues, as you can tell from the discussion and from Professor Kerr's discussion, it is a very intricate area of the law, and I'll come back to that in a second.

And so the administration has put forward I think seven proposals on amending or changing ECPA, or at least areas that will be worthy of discussion that we've been able to come to a position on so far. But they are difficult issues; we've been working on them. Beyond those seven proposals, we don't have an administration position on some of the other ideas and concepts that have been discussed today, so I just want to make that clear at the outset.

As I said a second ago, I mean the law is very intricate, and we've been talking a lot about ECPA, ECPA is divided up in various parts in Title 18 of the United

States Code, but ECPA is not the only thing that somebody has to deal with if you're working in this area, and I think Al was sort of referencing that earlier, as well.

From the perspective of the government, you've got ECPA that you have to focus on, but you've also got, in certain circumstances, depending on what kind of investigation you're doing and what your activities are, you've got the Foreign Intelligence Surveillance Act that regulates government's activities with respect to electronic surveillance, you've got the Communications Act of 1934, which also is a regulatory statute both on the government's activities and on private sector activities. ECPA regulates private sector activities, as well as that of the government.

You've got also I think from the perspective of private industry, you've got to deal with state laws. All the states in the United States have a variety of different laws that are similar in some ways and very different in others that deal with this area, and so if you're a private sector entity, you're going to have to comply with those, and if your business is international in nature, you're gong to have to comply with foreign law. So it's a fairly intricate area of the law, and it is complex, there's no doubt about that.

As a result of that, it's really important, as I think Valerie was referencing, that whatever we do in this area, we need to think about carefully and try, to the extent we can, anticipate the consequences of making a change in one part of the stature or another. And both –- making changes that will have an impact both on privacy, which is obviously very important, as well as the kinds of practical things that Valerie was talking about a moment ago in terms of how agents and prosecutors and the folks at the various providers deal with these statutes on a day to day basis, because you're going to make changes in the law that is going to impact how huge groups of non-lawyers who are not steeped in all of this have to implement these statutes, and so have the folks have

referenced, that's very important.

Having been through a variety of different legislative efforts over the years, I mean I can tell you that when somebody comes up with an idea, you get a group of folks in a room trying to figure out exactly, okay, well, if we make that change in that one word, what are the implications across the board? Let's think about the national security investigative implications of that, think about standard law enforcement, kidnapping cases, all kinds of different things, and then what's the implications on privacy of all of that, what are the reactions going to be? It is very difficult to try to work through some of these questions, and it's very important that we do it carefully and thoughtfully, so that's one of the key things that I wanted to point out. As Valerie mentioned, I think it is important that we have this balance and that we have tools that are appropriate with respect to the investigative need and the stage of the investigation that you're at, as well as the interests that are being protected.

And as Valerie mentioned, I mean there's certain times, and the same content is not protected in the same way in all places. And so, for example, again, picking up on some things Valerie referenced, but your tax return, for example, that we're all familiar with, if you're working on filling out your tax return and let's say you're using a hard copy document, just take that example, sitting at your dining room table, working your way through your facts and figures, that's going to be protected by the Fourth Amendment if the government wants to come in and take that away from you without your consent.

If, however, the government thinks there might be some interest in your tax return, we don't have probable cause to get a warrant, we can serve a subpoena on you, and you have to give that to us, you have to give us those records. If you give your

records to your accountant, you have the means to have an accountant do your tax return, we can serve a subpoena on the accountant for that tax return information and get that information from him or her, it's not protected by the Fourth Amendment in the same way. And that's true across the board with respect to all of our affairs, all of the papers that we handle and how we handle them and who we give them to and who we expose them to, that's just the way it is, and it's been that way for a long, long time with respect to the Fourth Amendment.

You take something –- you take those tax returns and have a draft, and you don't want to send that to the IRS, you ball it up, throw it in the trash, put it out at the curb, that's not protected –- it's protected differently let's say, at least under the Fourth Amendment, than it was before.

So the expectations of privacy, the reasonable expectations of privacy that you have change over time depending on the facts and circumstances, they're not universal in all circumstances. Okay, I want to move quickly to the questions here. I want to throw out just a couple other things to think about as we go through here.

It is very difficult, I think, to really understand and say what are the expectations of privacy that individual have and that society is prepared to recognize as reasonable in this area as technology evolves. I think folks, and it may be generational, as well, but I think there's a variety of different interpretations of what is private, what should be private, and I think that's why courts and Congress have thought carefully about these things, and in some instances, especially with the courts, held back from making pronouncements in this area until things evolve more.

The Supreme Court refrained from making broad pronouncements; I think it was in a case last year in this area. So I think there's something to be said for

that, and that, again, we need to move carefully in this area.

A couple final thoughts, it's important to remember, I mean this may be stating the obvious, but I'm not sure that folks always focus on this, at least in the discussions that I've had, it's important to remember, when we're talking about the internet, that the internet is a physical thing, it's not -– I was watching the Matrix last night -- you know, it's not the Matrix where we go into some alternate reality and disappear into the bits and bites of a technological world or tron or something like that. The internet is a physical thing. It's a series of devices that exist in the world, that have data on them or that transmit data via a wireless connection to another physical thing, that then puts it on a wire and takes it to other physical devices that are located around the world, or it's any number of different things that exist.

The data, the mechanisms, the routers, the wires, it's all connected in a variety of different ways, and it is all under the jurisdiction of somebody in the old fashioned legal world that we know.

So, for example, data that goes to a foreign country, data that resides on a server in India, for example, is going to be –- the data does exist somewhere, right, it is going to physically exist on let's say stored data, it's going to physically exist on a computer, on a server somewhere in the world, and when it is in some part of the world, it's going to be subject to the laws of that jurisdiction, that is just the way it is, and it's important to remember that, I think, as we work our way through this issue, the ECPA issues, and a whole range of cyber issues that we're confronting.

Another quick thought, with respect to email, I mean email is a difficult area, and it's difficult to figure out exactly what to do in that area. A lot of analogies have been drawn to the physical mail. And I will just say that physical mail or phone calls, the

analogy is not perfect, and I guess I would say it's a cautionary note to folks as you work through some of these issues and try to come up with the appropriate analogy. It's pretty tough sometimes because, for example, with the mail, I think most people would be shocked if the U.S. Postal Service, when you gave them the envelope that Jim Dempsey was talking about a little while ago -- if you gave them the envelope, and somehow they could scan through the contents of it, highlight terms in the mail, so that when it got delivered, they'd be highlighted with a little typed out link to a web site somewhere that might have some interesting related -– a feature that you'd - look at, and then send you junk mail that's related to the content of your actual mail that's sealed in an envelope.

I think we don't actually treat email the same way that we treat the physical mail. And so that doesn't mean we should come out one way or the other in terms of protecting email differently than regular mail. It may be that at the end of the day, that that's the right decision and that's what everybody decides to do, but the point is that, as you think about these things, it's important not to draw analogies that are not actually accurate and that really reflect what it is that we do in the physical world and how we handle these. So with that, again, thank you very much, Ben, and I look forward to some of the questions.

MR. WITTES: Thank you. I'm going to start off with one question, and then we're a little bit behind where I thought we were going to be time-wise, so I'm going to go directly from there to questions from the audience.

The question -- every single speaker, starting with me, and then Orin, and then all the members of the panel have emphasized at one point or another in their remarks that the statute is very complex.

And the question that you run into this with FISA discussions, as well, and the

question that I always sort of circle back to is, is it inevitably complex or is it needlessly complex? Is there a simpler architecture that one can imagine that is helpful here or does a simpler architecture inevitably result in sort of reductionism in treating unlike things similarly?

And so I'd like to just very briefly, if the members of the panel could, starting from left to right, just give some very brief thoughts on that. Are we inevitably faded to a very complicated architecture here or is there some simpler mechanism that would be helpful rather than hurtful?

MR. GIDARI: Well, look, it is complex, because technology is complex, and old rules don't apply very well to innovation, and so inevitably it's going to be complex. But at the same time, content is content, your communications are your communications. It isn't really difficult to fashion a rule that says when you speak, whatever it is that you're speaking, unless there is some loss of expectation of privacy or we're not willing to recognize it, it's protected, and you need probable cause to obtain those communications.

I don't think it's hard to say that in 20 words or less, and I think you can debate about what's reasonable in terms of an expectation of privacy, but the fundamental principal ought to be the same.

MR. WITTES: Valerie.

MS. CAPRONI: I think it inevitably is going to be complicated because of the very difficult balancing that goes into a statute like this. But not to ignore your question and deal with what Al just said, but I'm going to do that anyway, actually you said a couple of times, content is content, but that followed, I believe, a discussion where he talked about location being content. So I don't think we can say everybody

understands content is content is content, because I would say that your location is not "content" that needs a search warrant to obtain.

I see all of you, you're exposing yourself to public now, so we know that you're here, that is not a private fact about you. It doesn't become more private if you – in the words of one of the judges in the Jones case, zero multiplied by infinity is still zero in terms of your expectation of privacy and where you are, so I don't see that as content.

And I think going down that track takes you down to a very difficult position. So, for example, are your bank records content, which, if you think about it, what your bank record is is you saying to the bank, here's a little piece of paper, will you please give me money, or you're saying to a credit card company, I have a little piece of plastic, if you pay today, I'll pay you tomorrow. So it is a communication, we know what's happened there; we have a very good sense of what the transaction is.

Is it really different that we get your bank record that shows that you spent $1,000 at the Kitty Cat Club versus getting your email that says meet me at the Kitty Cat Club, let's go spend $1,000? Really, is that really different to the extent that we're going to say there's a difference of such magnitude that one requires a search warrant, which is like the gold standard, probable cause to a neutral and detached magistrate that will specifically state what you can take and what you can't take versus a subpoena, which, not being as cynical as Jim, it's still -- it's an order that's issued by an Assistant U.S. Attorney to say turn over the records.

MR. WITTES: Jim.

MR. DEMPSEY: Well, I think the statute is currently unnecessarily complex, and the treatment of content, open versus unopen, 180 days, 181 days, those are distinctions that no longer comport I think with the way people use the technology. If

we do go down the road of ECPA reform, I can guarantee that the statute will end up more complex than it is now, that's the nature of things. Although on the location piece of it, which is currently very complicated, I think the overall trend of the technology is going to be towards simplification of the issue. In my mind, there's no doubt that the location information is becoming more precise. Forget about GPS, GPS is almost irrelevant to this.

Remember, what was Google doing driving those cars around snooping on wifi networks? They were mapping the location of the wifi networks. Those wifi networks are – many of them specific to a house, that's as Fourth Amendment as you can get. But again, the legislative process produces complexity, so there you are.

MR. WITTES: Other Jim.

MR. BAKER: Okay, so a couple points. In theory, could you start today with a blank sheet of paper and write a statute that would cover all of this area that I described earlier in a way that is simple, straight forward and easily understood in theory? Yes.

But again, you're going to have to deal with all of the different statutes that I mentioned, state law, foreign law, and figure out a way to make those not apply to the private sector entities, because the private sector entities are the ones that have the data, in most instances, and you're going to have to deal with the fact that technology will change anyway, so you're going to have to be able to project into the future as much as you possibly can and write a statute that's going to endure for 20 – 30 years, so that we don't have to go back and do this again, because at some point in time, you will not have thought of everything, so your nice, new statute you're going to have to amend as technology evolves, and you're going to end up with kind of a structure like we have

today, which is really a series of statutes that have been enacted, and rulings by courts that have been decided based on a variety of different facts and circumstances and changes in technology over time.

So in theory you could do it. I think it would be very hard, and I think you would have a hard time figuring out what technology would be in the future and also making sure that you don't inadvertently mess up something that law enforcement does or expose something that you wanted to make private and then all of a sudden is no longer private.

MR. WITTES: So I'm going to go to questions from the audience. Please wait for the microphone before you start asking questions. Please frame questions as questions, say who you are when you get the microphone, and please keep questions brief so that others can have a chance, as well. Let's start with the gentleman in the orange shirt here.

MR. SEGOYAN: Hi, so my name is Chris Segoyan, (phonetic) I'm a graduate fellow at Indiana University, and I study privacy and the law enforcement access to this data. So there's two ways for the government to get your location information prospectively that's generated by a cell phone. First if for law enforcement to go directly to the phone company, and let's leave aside the prospective cell tower, signals cell tower information, but they can either triangulate your cell location from multiple towers or they can get the phone company to ping the GPS chip in your phone.

And Mr. Baker before the Senate just a few weeks ago said that, as a matter of policy, the DOJ sought a probable cause order to get that information, to compel the phone company to prospectively monitor the individual. But you didn't say whether your belief was that the law required you to do that or whether that was just

defensive lawyering on the part of the Office of Enforcement Operations.

And so the first quick part is whether, for the panel, whether you believe the law requires a probable cause order for prospective accurate location information either triangulated or GPS, and then the second part is that the other way for law enforcement to get someone's location information is to drive around the city with a device called a triggerfish, it's made by Harris Corporation, and in that case, law enforcement picks the signals out of the air, and so this is -– the communication between the phone and the tower, and law enforcement can then look at the individual with that information.

Prior to the Patriot Act, that could be obtained with no order at all. After the Patriot Act, you now need a pen register. And these devices let you locate someone to the home. And so the question for the panel is, should triggerfish require more than a pen register? Thank you.

MR. WITTES: Let's start with Jim Baker on that since the question is principally directed at you, I suppose.

MR. BAKER: So, again, I think as a couple of folks have pointed out, location information is not simple to define, but I think what I said in front of the Senate was that if you're looking prospectively with respect to information that you would get from a cell phone provider, the idea there is, we have to get a court order, but it's not a warrant, it is a combination, a hybrid order of 18 USA 2703D, plus a pen register order to get all these records going forward. If it's GPS information, I believe I said that we do need a warrant if you're asking for GPS information, which is still much more precise than the kind of cell phone information that you were talking about.

I mean I guess if we didn't have to do it, I don't think we would. If we

could get it with a subpoena somehow, prospective information, which would be easier to get than having to go to a court, I mean each time you wratch it up, this information, the requirements, you have to establish more facts and you have to go through a different process and so it becomes more cumbersome. So I would say that our interpretation is that we have to get it.

Now, with respect to the triggerfish, I guess I would say that it sounds like a pen register to me. I can't think of a case off the top of my head that ruled to that effect, but I believe I'll defer to Valerie right now if she has an answer on that, but I think that the triggerfish device would require a pen register order.

MR. WITTES: Valerie, do you have stuff to add to that?

MS. CAPRONI: I really don't, I agree it would be a pen register.

MR. WITTES: And, Jim Dempsey and Al, do you have senses of what should be required in those situations that the question asked about?

MR. GIDARI: Well, I think prospectively the notion that you can be tracked without constituting a search is -– seems just bizarre to me, I think it's just -– yes, you'd need a probable cause warrant to do that, I think it should be that simple.

MR. WITTES: Jim.

MR. DEMPSEY: Just quickly, I think the analogy is with wire tapping. So I would say that in the case of wire tapping, whether the wire tap is carried out with the cooperation of the service provider or whether the wire tap is done by the government on its own, let's say climbing the pole outside the suspect's house, which is not the preferred way, but is covered by the statute. So the statute says that a warrant is required whether the government acquires the information from the service provider doing the work, so to speak, and isolating the communications and delivering them to the government or

whether the government, through its own device, acquires the information, both are treated the same. And I would think in the location context, both should be treated the same.

MR. WITTES: Yes, in the second row here. Wait for the mic.

MR. SLOVER: George Slover, private citizen currently, recently retired from the House Judiciary Committee and the Department of Justice. And I was wondering -- we've got a whole different apparatus. This has been kind of a law enforcement discussion, but it's also the intelligence gathering, and I wonder if the law can be different for intelligence gathering and law enforcement or whether we need to have a situation where we just assume that whatever the intelligence community gathers is going to be accessible to law enforcement, and maybe should be accessible to law enforcement, and therefore, we need to have the same protections against intelligence gathering. Or whether there's some way to create a barrier that we can rely on to allow intelligence gathering without the risk that it will spill over to unauthorized gathering by law enforcement.

MR. WITTES: I'd actually like to add to that question a second dimension of I think the same issue, which is, if one raises the bar under ECPA, does that compound the issues that we are already having with respect to public/private cooperations in the area of cyber security. But anybody who wants to address any component of this issue, the sort of relationship with intelligence, is –- do you want to start, Valerie?

MS. CAPRONI: Sure; I would say as a general matter, the rules have to be coordinated so they work well together. A wall between information that's gathered in an intelligence context and information that can then be used in a law enforcement

context is an extremely bad idea. That was one of the things the Patriot Act did and it's one of the things that I think, despite the number of people who hate the Patriot Act, that aspect of the Patriot Act people like.

I think it's been incredibly valuable in terms of our sharing of information within the intelligence community, but to erect a barrier between records that are obtained for purposes of a national security investigation, where the way we mitigate that national security risk may well be a criminal prosecution I think is not a good idea.

MR. BAKER: If I could just interject. I mean so the statutes are – I ran through this whole list of statutes before and they apply to different people differently, but generally Title 3, the prohibition on wire tapping, the pen register statute, I don't have copies in front of me, but they prohibit the conduct by anybody, so by you, by the government, by the government wearing a law enforcement hat, by the government wearing an intelligence hat.

And that's why they're so important, because they do prohibit or regulate activities in a lot of different ways across the board. Some statutes, for example, FISA, only regulates activity done under color of law, so it doesn't prohibit you from doing something.

So these laws do have import sort of across the spectrum of governmental activity, which is why it's really difficult sometimes to have a discussion in public about the implications of a change in ECPA that it might have on the intelligence side, so it's something we have to do carefully.

MR. WITTES: Do you want to add to that, Jim?

MR. DEMPSEY: Yeah, all I would say is, again, I fully appreciate your point on that one, Jim, but my motto here is, think comprehensively, act incrementally,

that we're not –- just the fact that it's a complicated structure and just the fact that we have two parallel systems, one for national security and one for law enforcement, it shouldn't be the excuse to do nothing, particularly if we can identify, and this is your criteria, and it's a good one, if we can identify specific changes that then do not have collateral implications.

And I think any reform process here has to -- you start from the do no harm principal, but I think we can accept the complexity, we can accept the bifurcation between national security and law enforcement authorities, and we can still, within those constraints or within that context, develop incremental improvements in the statute that do address that -– that move us somewhat in the direction of simplicity with the sort of constitutional standard as our guide.

MR. WITTES: Bill Banks in the front here.

MR. BANKS: Thanks, Bill Banks at Syracuse University. I'm told that there's some instances where location data is difficult to obtain either because the device is an unusual one or the provider is a foreign one or there's encryption of some type that makes it difficult to either learn location in real time or learn location at all. I wonder if that's the significant problem from the government's perspective, and if it is, whether you think Congress should deal with it in some way.

MR. GIDARI: Well, I'm not going to answer your specific question, but let me try to pull the counter back a little bit and address an issue that I think is raised by your question and I think it's a very important issue. All of the types of activities that Valerie was talking about, and when you think about investigators, it's all very difficult to do in real time.

A lot of this data, yes, copies of certain types of data exist and you can

get them later, but a lot of data is fleeting, and a lot of data -- if you're actually trying to find somebody, for example, location information that you may be able to get, if you're actually trying to find somebody, you want to find them when they're there, not three hours after they were there, right.

So there are a whole range of very practical difficulties that the government faces on a regular basis in terms of finding out what the right data is, what provider has it, how can we get it, have they done it before, can they collect this data, can we ingest this data, is it in a format that we can deal with, and do we get it on a timely enough basis that we can actually act upon it, especially in a national security case or some type of kidnapping case where somebody's life is on the line.

So the practical difficulties that the government faces in this area are huge. Even if we get authorization pursuant to whatever standard you want to set, that's only half the battle for us, we still have to go and actually get the data, and that's a subject for another day, but it's – they're very practical problems along these lines that you highlight.

MR. WITTES: Yes, in the third row here.

MR. MARGOLIS: Hi, the name is Joel Margolis with Subsentio. I have a question for Al Gidari. You described a popular kind of location ap where I can transmit my location to others, and you thought that should be regarded as content and deserving of the high level of privacy protection. But I wonder: why should the location that I voluntarily disclose to others deserve a higher level of privacy protection than the location I want to keep private?

MR. GIDARI: First, there should be no hard questions for the rest of the period, Joel, so thank you. Why do you assume that I don't want to keep that private just

because I conveyed it? I made a decision to talk to somebody when I've enabled my smart phone to convey that location.

What the providers typically do on the other end is anonymize that, they promise to you that they'll take that data, eliminate the identities surrounding it, really to the question the gentleman asked a second ago, and only store that data for purposes of future use to identify location when another person is in the vicinity and wants to know where the nearest Starbucks is.

So the mere fact of conveyance of my communication to a person of my choice doesn't render that a public communication. So I think any time anybody uses their device -– let me just substitute something for location.

Let me just take weather and put a temperature gauge on that. If I were to just convey the temperature to somebody, why does that make it public? Because I'm using a network and conveying it. It is content, it is my communication, and I've made that choice, so I don't see a distinction in that case.

MR. WITTES: I've been horrifically discriminating against people in the back of the room, which is actually hard for me to see because of lights. But if there are people back there who have questions, put your hands high up. Yes, over there.

MR. DE PIAZZA: Hi, my name is Fabri de Piazza; I'm the editor of GOVERNINGWorks. I'm wondering a sort of larger, general question, which is, to what extent do you think reasonable expectation of privacy is a viable constitutional standard given where we are?

MR. WITTES: This is a huge question that is, in some ways, subsumes the entire event. Does anybody want to address it?

MR. BAKER: I was going to suggest Orin gets this one.

MR. WITTES: Yeah, this is like a classic Orin question. Orin, do you have thoughts on it?

MR. KERR: Sure.

MR. WITTES: Somebody bring Orin the mic.

MR. KERR: I think the answer is that reasonable expectation of privacy is a constitutional term of art like due process. So just like we don't think, well, we can figure out due process based on just what process seems to be due, we can't think about reasonable expectation of privacy as what a reasonable person would expect. So it's a constitutional term of art that actually is separate from the desirability of a particular rule at social policy, and we shouldn't confuse them, and can actually kind of think of them as two separate questions.

So I would think about the Fourth Amendment issues as being just an issue up to the courts as to what issues are outside of the realm of legislative zones of where Congress can legislate and just focus on the areas that are left open from the standpoint of policy. So I would essentially say just ignore the Fourth Amendment issues to the extent that the courts have not said you can't do this and try to do what's been left open.

MR. BAKER: If I could just amplify one quick point. And others have made this point I think, and Orin, in some of his articles, as well. The Fourth Amendment does not protect you against all searches and seizures by the government; it protects you against unreasonable searches and seizures by the government. And so I actually think that it is a reasonable expectation of privacy related to the Fourth Amendment's terms right out of the text. I think it's a useful way to keep thinking about these things, and it's something that it does -- I'm sorry to say, it kind of changes over time in terms of what

people's reasonable expectations of privacy are. But I think it's a useful concept and sort of a -– you've got to have some kind of agreed principal in this area to try to figure out what to do, and I think that's as good a one as any.

MR. WITTES: We've got time for one more question, and the gentleman in the back has been very patient.

SPEAKER: (inaudible) with the State Department.

MR. WITTES: Speak up, please.

SPEAKER: (inaudible) with the State Department. This might be another question for Professor Kerr. But I've been thinking more and more about how, practically speaking, the courts might be uniquely situated in resolving a lot of these questions with respect to Cloud location and other information.

I know that Chairman Leahy and the Congress have been working hard, but it seems like there's been a lot more progress as far as at least litigation goes. And I wonder, ideally, would we all be better off if the courts simply weighed in and decided these questions, and practically speaking, is there a chance that Congress might weigh in given the fact that it is a Senate/House divided control, so I just kind of am curious to hear your thoughts on those two kind of questions.

MR. WITTES: So this is actually a terrific question on which to end, and what I'd like to do is to give all the panelists and Orin a chance to address it. And if I can just add my own sort of lilt to it, given the seriousness of the disagreements here, are we kind of faded to wait for higher level judicial guidance as to what the parameters of the debate here are, or wait until the modern version of Katz before we can adopt the modern version of Title 3, right? Or is the scenario where we can really expect to try to do what Congress did in '86 and which so many of the panelists have been enthusiastic about as

an exercise, a sort of forward looking exercise for Congress to have engaged in at the time, can we expect reasonably to replicate that sort of an effort at this point? So I'd like -- let's have Orin kick us off with his stab at an answer here and then just go down this time from right to left. And so are we faded to do this judicially or can we expect to reform legislatively realistically, and then we'll close?

MR. KERR: My own take is I have more confidence in Congress to do a better job with these issues than I do in the courts. The judges don't understand the technology, they struggle to understand the difference among the different forms of technology, the different context, and typically the courts are lagging indicators of these issues.

So the courts step in 20 or 30 years after everybody else has kind of figured these issues out, and they say, yeah, this is what we think the answer is, whereas Congress can think about the latest technology.

And I think the history here is, when Congress acts, it actually does a pretty good job on the whole, and the difficulty is making sure that Congress revisits the issues. So I would focus more on Congress here than on the courts.

MR. BAKER: I guess I don't know exactly who the best decision-maker is on these at the end of the day. But I will say, to pick up on a point that Al made earlier, the law is going on every day, people are making decisions every day in a whole range of different areas. Back to the providers that he mentioned, FBI agents, lawyers in different agencies, lawyers of the Justice Department, lawyers in the interagency, we're all making decisions every day trying to figure out what the law is.

You've got some guideposts out there in terms of –- well, you've got the law out there in terms of statute from Congress, you've got some guideposts in terms of

judicial decisions that may or may not fit to exactly the problem that you're confronting, and a lot of it is very -- it's difficult to interpret sometimes, but that is going to go on, and so you're going to have all things moving forward I think simultaneously.

You're going to have things that end up in courts and in litigation, you're going to have Congress changing statutes and so on, and you're going to have the Executive Branch and the private sector interpreting it and doing things about it and acting on a day to day basis.

MR. WITTES: Yeah, I guess I agree with both Orin and Jim Baker, that –- I really just quote -– Justice Breyer wrote a book after he retired called Active Liberty, and he talked about the evolution of the law, and he even specifically mentioned that through conferences like this, events like this is how you sort of develop that sort of understanding of what is the reasonable expectation of privacy and what should policy be, and it's going to go back and forth between the courts and Congress. What each does obviously influences the other, as well.

It was 40 years between Olmstead and Katz. It took 40 years for the court, the Supreme Court, to catch up with technology, so to speak, so I'm not sure we want to wait 40 more years.

MS. CAPRONI: I'm not sure where the right place to decide this is, I think it's inevitably going to be decided both places. I would say the one thing that is useful, though, that the courts give us is a clear expectation that might change over time, but a clear expectation of where the constitutional floor is.

And I think one of the things that I see in this discussion is, there's not agreement about where does the Fourth Amendment lie in these issues so that what Congress is working with is some level of -– sort of a cushion above the floor. So I think

both branches have a role to play, from my personal perspective, knowing where that floor is would be a useful thing to know.

MR. GIDARI: You know, inevitably when you're talking about a court deciding something, the party on the other side of the V is one of my clients, and they don't really like to be there, so the providers are really the people in the middle in all of this.

There really is a common law that is developing, and because of all of the uncertainty about how the law applies, many of the providers take the most conservative view, and so the person most likely to sue them over their interpretation of ECPA tends to be to my right here as the government seeks to compel them to do something that they really think they should have decided to do with a rationale understanding of the law.

But the irrationality comes from the fourth stakeholder then who doesn't like the decision you make and sues you on privacy grounds in a class action lawsuit. So the providers really are in the middle, and they've taken the most conservative view, many of them take the most conservative view.

And as a result, I think you end up with less case law because the government is loathed to sue the providers, and you don't actually end up with the kind of reported decisions that would crystallize the issue more, sooner, if, in fact, those issues did get litigated. So I think in the end, it's a long way of saying the courts are painfully slow and generally have the wrong issue before them when it comes time to decide.

MR. WITTES: On that cheerful note, we are going to close. Thank you all for coming, and please join us for future such events. Thank you.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012