REFORMING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

- - -

WEDNESDAY, SEPTEMBER 16, 2015

United States Senate,

Committee on the Judiciary,

Washington, D.C.

The Committee met, pursuant to notice, at 10:17 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley, Hatch, Sessions, Cornyn, Lee, Flake, Perdue, Tillis, Leahy, Whitehouse, Klobuchar, Franken, Coons, and Blumenthal.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman Grassley. Today's hearing is intended to help inform the Committee about the most recent views of a wide variety of stakeholders concerning the need to reform the Electronic Communications Privacy Act--or as we know it around here, "ECPA"--and various ways of fixing it. The Committee's last hearing on the topic was 4-1/2 years ago. Since then, numerous proposals have been advanced by members of the Committee.

In 1986, Congress enacted ECPA to both protect the privacy of Americans' electronic communications and to provide the Government with a means to access these

communications and related records in certain circumstances. However, dramatic changes in the use of communication technology have occurred since 1986.

Americans now depend on email, text messages, social networking websites, web-based apps, and countless other electronic communication methods on a daily basis. And more than ever, these communications are being retained in some form due to the dramatic reduction in the cost of storing data in the cloud.

These communication technologies are enriching all of our lives. They are of great help to me in keeping in touch with my constituents in Iowa. And for the most part, we have American technology companies to thank for this digital revolution. These companies are now a significant engine of growth for our economy by creating an increasingly global market for these communication technologies.

But, of course, these technologies are also being used every day by those who intend to do our society great harm--terrorists, violent drug dealers, child predators, environmental criminals, and you can go on and on. These technologies create a digital trail that is often essential to bringing these offenders to justice.

In light of these changes, there is a growing consensus that ECPA must be modernized to adapt to this new landscape. And whatever updates to the law we make, of course, must be

consistent with people's protections under the Fourth Amendment.

The privacy and technology communities have criticized ECPA for failing to provide sufficient privacy safeguards for individuals' stored electronic communications. Indeed, given the way Americans use email today, it hardly makes sense that the privacy protections for an email should turn on whether it is more than 180 days old or whether it has been opened.

At the same time, law enforcement officials have expressed concern with certain aspects of the current ECPA framework and how it currently works in practice. And they are concerned that reform efforts to a statute they use every day do not unduly hamper their ability to investigate violations of the law.

For example, the Department of Justice has expressed concern about efforts to change the ECPA notice requirements to provide targets with unprecedented amounts of information that could compromise ongoing investigations.

Both the Department and civil law enforcement agencies have expressed the need to address an emerging gap in their authorities if the target of an investigation fails to respond to lawful civil process for email evidence in the target's possession. They contend that this gap could allow offenses such as civil rights violations, securities fraud,

and consumer fraud to go unpunished.

In addition, many State and local law enforcement officials are frustrated with the current timeliness and quality of responses by providers. Unlike traditional search warrants, law enforcement agents cannot control how quickly they obtain evidence through ECPA warrants; they rely on the providers to conduct the searches for them. To these officials, any heightening of ECPA's legal standards should be accompanied by changes to the law that ensure that they receive the information they need timely.

In addition, some officials have expressed concern that the voluntary nature of ECPA's emergency exception can result in unacceptable delay in important cases--for example, when a child is abducted.

Closely related to these concerns is the ongoing issue of encryption and the "Going Dark" problem, which the Committee recently held a hearing on. This is another example of a situation where agents may meet the legal standard to obtain critical evidence--but then are not able to access it quickly enough, or even at all.

As I said at our last hearing on ECPA reform that we discussed in 2011, if we are considering changing the legal standards under ECPA, we should also, as I said, "be working to ensure that these same providers are granting law enforcement the necessary access" to address the "Going

Dark" issue. I sent a letter to the Deputy Attorney General last week to get an update from the Department about how that process is proceeding.

Reforming ECPA's treatment of stored electronic communications, therefore, is a complicated and potentially far-reaching endeavor that sits at the intersection of the privacy rights of the public, the investigative needs of law enforcement professionals, society's interest in encouraging and expanding commerce, and the dictates of our important Constitution.

The key is to strike the right balance between these interests. As Ranking Member Leahy declared at our last hearing on this topic in 2011, "meaningful ECPA reform must carefully balance privacy rights, public safety, and security." I agree.

I am grateful for the presence of all the witnesses today, and I now recognize Senator Leahy.

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

Senator Leahy. Well, thank you, Mr. Chairman. You know, I remember when the Electronic Communications Act was passed 29 years ago. In fact, I was talking with a former Director of the FBI last month in Vermont about when we worked out the very final parts of it my Capitol office about 10 or 11 o'clock at night and tried to bring law

enforcement and everybody else together, and we passed it.

But keep in mind those calls were on landlines at that time. Call waiting was novel. Few had heard of email. But we did figure there would be new electronic communications, and we thought ECPA could provide that.

But there are now many ways that nobody could have anticipated of communicating, and the privacy rules concerning this are simply outdated. As the statute reads today, Government agencies can obtain the contents of an email without a warrant if that email is more than 180 days old.

Well, we do not expect our private letters or photos stored at home to lose Fourth Amendment protection simply because they are more than 6 months old. Neither should our emails, our texts, or other documents.

Now, tomorrow is a major historical date in Iowa. It is Senator Grassley's birthday. I think they declare it as a day of public rejoicing. But if I sent him a note, which I have actually written, and he puts that note in his desk, a handwritten note in his desk, somebody is going to have to have a warrant to go and get it. I did not put anything in there to justify a warrant, I should say, but if I send him a text and that is stored in the cloud, why should it be any different? Why should somebody be able to just take it out?

Now, Senator Lee and I have introduced the ECPA

Amendments Act to bring privacy protections for the digital world in line with those in the physical world. Our bill has 22 other cosponsors in the Senate, nine of them on this Committee. In the House, even more, 300 cosponsors in both parties support the bill. An extraordinary coalition of industry and civil society supports this bill: Americans for Tax Reform, the Center for Democracy and Technology, Heritage Action, and the ACLU. Now, usually representatives of those people have to have an arbitrator get on an elevator with them if they are all in there together. But they all agree with this. The bill has been reported from the Judiciary Committee by voice vote in each of the last two Congresses. I think, to use a technical term, passing this is a no-brainer.

Five years ago, the U.S. Court of Appeals for the Sixth Circuit found that the contents of email was fully protected by the Fourth Amendment, regardless of its age. And that has effectively become the rule nationwide. Major service providers no longer turn over the contents of emails or texts without a warrant or a legitimate warrant exception. The ECPA Amendments Act simply, as Senator Lee knows, codifies that current practice.

Some have raised concerns that the bill would hamper civil regulatory agencies, such as the SEC. We want these agencies to be effective, but there is nothing in our

Constitution that says only certain agencies have to follow the Constitution and others do not have to. The SEC has not been able to obtain emails without a warrant because of the 2010 Federal court ruling, and our bill does not change that.

I am disappointed that the Commerce Department was not asked to join the administration panel, given its important perspective, but I thank the Chairman for having this. The number of Senators and House Members that have joined on this tells us that this is an important issue.

Thank you, and happy birthday a day early.

Chairman Grassley. Thank you.

Before I introduce the panel, I would want to put in the record some letters that we received outlining concerns of the current ECPA reform proposals from law enforcement agencies, so five I will name: the National Association of Assistant U.S. Attorneys, the Federal Law Enforcement Officers Association, the Major County Sheriffs Association, the National District Attorneys Association, the Iowa County Attorneys Association. So I would ask, without objection, that these and additional letters be entered into the record.

[The information follows:]

/ COMMITTEE INSERT

Chairman Grassley. Our first witness is Principal Deputy Assistant Attorney General Elana Tyrangiel. Ms. Tyrangiel also serves as head of the Department of Justice Office of Legal Policy. Prior to joining Justice, she worked in the Office of White House Counsel and served as Assistant U.S. Attorney in D.C. Before that she was a policy counsel for the National Partnership for Women and Families. She has an undergraduate degree from Brown and a law degree from the University of Michigan.

Our second witness, Andrew Ceresney, currently serves as Director of the Division of Enforcement, Securities and Exchange Commission. Before joining SEC, he was a partner at Debevoise & Plimpton where his practice included white-collar crime and SEC investigations. Prior to that, he served as Assistant U.S. Attorney, Southern District of New York. He received his undergraduate degree from Columbia and his law degree from Yale.

The third witness, Daniel Salsburg, is Chief Counsel, Office of Technology, Research, and Investigation, Bureau of Consumer Protection at the FTC. Previously he served as Assistant Director, Bureau of Consumer Protection, and before that senior trial attorney for the CFTC Division of Enforcement. Mr. Salsburg received his undergraduate and law degrees from the University of Pennsylvania.

I want to thank all three of you for testifying, and we

will do it in that order, so proceed, Elana.

STATEMENT OF ELANA TYRANGIEL, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL POLICY, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Ms. Tyrangiel. Thank you. Chairman Grassley, Ranking Member Leahy, and members of the Committee, thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act, or ECPA. We appreciate the opportunity to engage with the Committee on this topic, which is of particular importance to the Department. I look forward to discussing with the Committee how the Department uses ECPA and how the statute might be updated and improved.

ECPA has always sought to ensure that the Government can perform its crucial public safety and civil and criminal enforcement missions while safeguarding individual privacy. It is important that ECPA reform efforts remain focused on maintaining both goals.

Electronic communications play a vital role in Government investigations. Indeed, as technology has advanced and as electronic communications and electronic data storage have augmented traditional means of communicating and storing information, appropriate governmental access to data has become even more important to upholding our law enforcement and national security

responsibilities.

ECPA is critical to tracking down criminals and investigations into murder, kidnapping, organized crime, child exploitation, identity theft, terrorism, and more. But criminal investigations are only a subset of the circumstances in which ECPA applies. This statute also applies when the Government acts as a civil regulator or even as an ordinary civil litigant. ECPA reform efforts should account for the breadth of the statute's applications.

We agree that, notwithstanding several updates to ECPA since its enactment in 1986, the statute draws some lines that do not account for the development of technology and the ways in which we use electronic and stored communications today. For example, there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, there is no reason for the statute to give lesser protection to emails that have been opened than to emails that remain unopened. How to account for changes in technology while maintaining privacy protections and providing for public safety and law enforcement imperatives remains a central challenge of ECPA reform efforts.

Personal privacy is critically important to everyone. All of us use email and other technologies to share personal

information, and we want it to be appropriately protected. And many discussions about enhancing privacy focus on a proposal that would require law enforcement to obtain a criminal search warrant based on probable cause to compel disclosure of stored email and similar stored content from a public service provider. This is a sensible approach provided that Congress consider crafting limited alternatives for certain investigative functions.

For example, civil regulators and litigators typically investigate conduct that, while unlawful, is not a crime. But criminal search warrants are only available if an investigator can show probable cause that a crime has occurred. Lacking warrant authority, civil investigators enforcing civil rights, environmental, antitrust, and a host of other laws would be left unable to obtain stored contents of communications from providers. As information is increasingly stored electronically, and as wrongdoers take new steps to shield that information from civil investigators, the amount of critical information that is off limits to Government regulators and litigators will only increase.

Efforts to update ECPA can reflect these considerations and, at the same time, incorporate strong mechanisms that protect individual privacy and ensure appropriate judicial oversight of Government access to individual's

communications. Any proposed changes to ECPA should address the ability of civil litigators and regulators to ask a court to compel disclosure of information from providers.

The Department also has several more technical yet important concerns that we believe merit consideration, and although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are other parts of the statute, as noted in my SFR, that would benefit from further examination.

I would also like to speak briefly about Government access to data stored abroad, which some proposals to amend ECPA would significantly alter. The administration is studying these proposals, but the Department has significant concerns about aspects of these proposals.

The Department of Justice appreciates the opportunity to discuss all of these issues with the Committee, and I look forward to your questions today.

[The prepared statement of Ms. Tyrangiel follows:]

Chairman Grassley. Thank you.

Andrew?

STATEMENT OF ANDREW CERESNEY, DIRECTOR, DIVISION OF ENFORCEMENT, U.S. SECURITIES EXCHANGE COMMISSION, WASHINGTON, D.C.

Mr. Ceresney. Thank you, Chairman Grassley, Ranking Member Leahy, and members of the Committee. Good morning, and thank you for inviting me to testify today on behalf of the SEC concerning the Electronic Communications Privacy Amendments Act pending before your Committee.

I share the bill's goal of updating ECPA's evidence collection procedures and privacy protections to account for the Digital Age. But the bill in its current form poses significant risks to the American public by impeding the ability of the SEC and other civil law enforcement agencies to investigate and uncover financial fraud and other unlawful conduct. I firmly believe there are ways to update ECPA that offer stronger privacy protections and observe constitutional boundaries without frustrating the legitimate ends of civil law enforcement.

The SEC's tripartite mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. Our Division of Enforcement furthers this mission by investigating potential violations of the Federal securities laws, recommending that the Commission bring actions against alleged fraudsters and other wrongdoers, and litigating the SEC's enforcement

actions. A strong enforcement program is critical to the SEC's efforts to protect investors from fraudulent schemes and promotes investor trust and confidence in the integrity of our securities markets.

Electronic communications often provide critical evidence in SEC investigations, as email and other message content can establish timing, knowledge, or relationships, or awareness that certain statements to investors were false or misleading. When we conduct an investigation, we generally will seek emails or other electronic communications from the key actors through an administrative subpoena. In some cases, the person whose emails are sought will respond to that request. But in others, the subpoena recipient may have erased emails, tendered only some emails, asserted damaged hardware, or refused to respond. Unsurprisingly, individuals who violate the law are often reluctant to produce evidence of their own misconduct. In still other cases, email account holders cannot be subpoenaed because they are beyond our jurisdiction.

It is at this point in an investigation that we may need to seek information from an Internet service provider, or ISP. The bill at issue would require Government entities to procure a criminal warrant when they seek the content of emails or other electronic communications from ISPs. Because the SEC and other civil law enforcement agencies

cannot obtain criminal warrants, we would effectively not be able to gather electronic evidence directly from an ISP, regardless of the circumstances, even in instances where a subscriber deleted his emails, asserted his hardware was lost or damaged, or fled to another jurisdiction.

Depriving the SEC of authority to obtain email content from an ISP would also incentivize subpoena recipients to be less forthcoming in responding to investigatory requests because an individual who knows that the SEC lacks the authority to obtain his emails may be emboldened to destroy or not produce them.

These are not abstract concerns for the SEC or the investors we protect. Among the type of scams we investigate are Ponzi and "pump and dump" market manipulation schemes, as well as insider trading violations. In these types of frauds, illegal acts are particularly likely to be communicated via personal email accounts, and parties are more likely to be non-cooperative in their document productions.

Technology has evolved since ECPA's passage, and there is no question that the law should evolve to take account of advances in technology and protect privacy interests, even when significant law enforcement interests are also implicated. But there are various ways to strike an appropriate balance between these interests as the Committee

considers advancing this important legislation.

As part of that balance, any ECPA reform can and should afford a party whose information is sought from an ISP in a civil investigation notice and an opportunity to participate in judicial proceedings before the ISP is compelled to produce the information. Indeed, when seeking email content from ISPs in the past, the Division provided notice to email account holders in keeping with longstanding, and recently reaffirmed, Supreme Court precedent.

If the legislation were so structured, an individual would have the ability to raise with a court any privilege, relevancy, or other concern before the communications are provided by an ISP, while civil law enforcement would maintain a limited avenue to access existing electronic communications in appropriate circumstances from ISPs. Such a judicial proceeding would offer greater protection to subscribers than a criminal warrant, in which subscribers receive no opportunity to be heard before communications are provided.

Thank you again for the opportunity to be here today. We look forward to working with the Committee on ways to modernize ECPA without putting investors at risk and impairing the SEC from enforcing the Federal securities laws. I am happy to answer any questions that you have.

[The prepared statement of Mr. Ceresney follows:]

Chairman Grassley. Thank you, Andrew.

Daniel?

STATEMENT OF DANIEL SALSBURG, CHIEF COUNSEL, OFFICE OF TECHNOLOGY, RESEARCH, AND INVESTIGATION, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, D.C.

Mr. Salsburg. Chairman Grassley, Ranking Member Leahy, and members of the Committee, I am Dan Salsburg, the Chief Counsel in the Office of Technology, Research, and Investigation in the FTC's Bureau of Consumer Protection.

Let me begin by noting that my oral statements and responses to questions are my own and they do not necessarily reflect the views of the Commission or any Commissioner. Having said that, I very much appreciate the opportunity to present the FTC's testimony and explain how proposals to amend ECPA could impact the Commission's civil law enforcement mission.

The FTC supports the objectives of ECPA reform and understands the need to update ECPA to account for technological advances and to protection consumers' privacy. In bringing civil law enforcement actions to protect consumers, we rely heavily on our ability to conduct thorough investigations of companies' business practices.

As a civil law enforcement agency, the FTC is concerned that recent legislative proposals to update ECPA could impede our ability to obtain certain information from ECPA service providers in future cases. Under recent legislative

proposals, to obtain content from an ECPA service provider the Government would need to obtain a criminal warrant, which is not available to the FTC. The proposals would require a warrant for all forms of content even those in which a target has no reasonable expectation of privacy. We are concerned that requiring a criminal warrant in three situations could impede the Commission's future effectiveness.

The first of these situations concerns previously public commercial content that advertises or promotes a product or service. We are talking about things like no longer running advertisements, old versions of websites, previously sent spam, and fleeting ads that may appear on a mobile device. This class of content is critical to many FTC investigations. Before determining whether a target ha made a false representation, we need to find the advertising or promotional material that contains the representation.

In many instances, especially fraud cases, the scam artists change websites and electronic marketing materials frequently. When Commission staff investigates complaints about a website, the website currently viewable to the public may be different from the one that the consumer complained about.

Current ECPA allows us to compel a provider to produce marketing materials in some circumstances. We have not used

this tool often. Most of the time, our investigators are able to track down a target's old marketing materials without needing to seek the materials from the provider. But the increasingly fleeting nature of advertisements--an ad on a mobile device may only appear for a few seconds, for instance--makes it quite likely that we will need to compel old advertising and promotional materials from a provider more often.

An exception from the criminal warrant requirement in proposed legislation for previously public commercial content that advertises or promotes a product or service would enable the Commission to obtain such commercial content. At the same time, such an exception would have no impact on privacy rights because the materials would be purely commercial and have been affirmatively published by the target. As a result, the target would not have a reasonable expectation of privacy with respect to Government access.

The second situation which should be exempted from the criminal warrant requirement contained in recent ECPA reform proposals is content with the consent of the customer. As cloud computing becomes more widespread, it will be increasingly important for a civil law enforcement agency to be able to compel an ECPA provider to disclose content to civil eliminate with the customer's consent. For example, a

defendant may want to authorize the FTC to obtain documents directly from its cloud computing account if the records are voluminous, or a consumer victim who deleted a message from a scam may want the FTC to obtain the message from the consumer's email service provider. Under current legislative proposals, however, even if the customer or subscriber has consented, we could not compel the cloud computing service to release the customer's content. When a customer consents to disclosure to the Government, the customer has no reasonable expectation of privacy with respect to the Government's access.

Third, a criminal warrant should not be needed when the FTC has compelled a target to produce content that is held by a cloud service provider and the target has refused or failed to comply with the FTC's demand. Under these circumstances, the FTC should be able to seek a court order directing the target's provider to produce the content.

In conclusion, thank you for giving the Commission an opportunity to describe the importance of electronic communications in our investigations and the ways in which proposed updates to ECPA, while extremely important, could hinder our law enforcement actions. The FTC looks forward to working with the Committee to address the Commission's concerns as legislation advances.

[The prepared statement of Mr. Salsburg follows:]

Chairman Grassley. Thank you all for your testimony. I will start and then Senator Leahy will be next with our questions.

Andrew, I am going to start with you. Chairwoman White has told us that the SEC's ability to carry out enforcement responsibilities and conduct investigations has been significantly curtailed as a result of the Warshak decision. But we have been told that the SEC has not provided any examples of cases where access to electronic communications has been cut off due to that decision or would be impacted if the pending reform bills were enacted.

Can you provide any examples of the type of cases or investigations that have been affected since that case decision due to providers requiring a warrant when the Government seeks electronic content in a civil investigation?

Mr. Ceresney. Yes, Senator. Obviously, I cannot talk about the details of ongoing investigations, but I can say that there are number of investigations in which, if we were exercising our authority under ECPA to obtain emails from ISPs, we would do that in furtherance of the investigation, for example, manipulation schemes, touting schemes, FCPA cases where, if we had the authority, we would certainly do that. I cannot necessarily say it would produce emails that would dramatically further the investigation because right

now I am not able to know what it is, emails we would obtain through that kind of process, but I can definitively say that there are investigations that are ongoing, and there were investigations even prior to the Warshak case where we were exercising the authority that were significantly advanced by obtaining ISP emails.

Chairman Grassley. Okay. Daniel, along those same lines, in your written testimony you suggest that a warrant-only requirement for obtaining electronic communications from an Internet service provider "could create some obstacles in future civil law enforcement cases..." Would you provide us examples of the type of cases and situations the FTC is concerned about that would create obstacles to future civil law enforcement cases?

Mr. Salsburg. Of course, Senator. The types of cases that we are talking about are those instances where the target or the defendant is trying to be evasive, is not responding to discovery or to our civil investigative demands. So that is one class of cases where we cannot get the information directly from the target.

The other class of cases are where the target is an outright fraud, a fly-by-night scam, and we do not want to contact them directly. You know, if we contact them directly, they may flee; they may destroy evidence, destroy records, and hide assets, and keep us from being able to get

money back for consumers.

Chairman Grassley. Okay. This would be to any or all of you. There is a perception from the privacy and tech community that what you are really asking for is a mechanism that lacks judicial oversight and sidesteps the target of a civil investigation without any notice or hearing. In fact, the written testimony provided to us from Google states that you are proposing to amend "ECPA so that agencies can ultimately bypass the target of or even potential witnesses in civil investigations."

For any or all of you, is this a fair characterization of what you are really proposing?

Ms. Tyrangiel. Senator, no, it is not. We are asking for a mechanism to allow courts to compel this information from providers where necessary, and as has been mentioned, this is information that we try to get from subscribers. Where we cannot get it from subscribers, we really do need it, and there are ways of protecting privacy and of ensuring that there is appropriate processes of safeguard for civil liberties and privacy.

Chairman Grassley. Andrew?

Mr. Ceresney. And I would just add that the mechanism that we are proposing, which is a judicial proceeding where we would make some showing, whatever the showing that Congress dictates would be, we would give notice to the

subscriber and allow them to come in and offer objections. And from our perspective, that is more protection than a warrant proceeding where it is ex parte, where the subscriber is not present.

Chairman Grassley. Do you have anything to add?

Mr. Salsburg. I would agree that the judicial mechanism that we are proposing would require two things: one is we would have to go to the subscriber first, and only when we are unable to get the information from the subscriber could we then go and seek a court order. So it is two additional protections. We would have to first try to get it from the subscriber, and then there would be the judicial intervention.

Chairman Grassley. Senator Leahy.

Senator Leahy. Thank you, Mr. Chairman.

First off, we are putting things in the record, and there is a great deal of consensus around the need to update ECPA, and I ask consent that these letters be placed in the record in support.

Chairman Grassley. Yes.

Senator Leahy. Thank you. They range from the Chamber of Commerce, former FBI Director Sessions, Leadership Conference on Civil Rights, and many others.

[The letters follow:]

/ COMMITTEE INSERT

Senator Leahy. Ms. Tyrangiel, let me ask you a question. The FBI now uses warrants when it seeks the contents of email communications in criminal investigations, regardless of the age of the email. Is that correct?

Ms. Tyrangiel. That is correct.

Senator Leahy. So this bill that Senator Lee and I have would not change the FBI procedure in that regard?

Ms. Tyrangiel. The bill would not change the procedure for criminal--obtaining disclosure through a third-party provider of stored email, regardless of the age.

Senator Leahy. Thank you. So the privacy protection is afforded to email or text messages. Should that change if they are older than 6 months or if they have been opened?

Ms. Tyrangiel. No, we do not think there is a principled reason to treat email differently--we do not think there is a reason to treat email differently depending on the age.

Senator Leahy. Mr. Ceresney?

Mr. Ceresney. No, I do not think that we see any distinction there.

Senator Leahy. Mr. Salsburg?

Mr. Salsburg. We agree with that.

Senator Leahy. Thank you.

You know, we talked about United States v. Warshak. I will ask the same question of both Mr. Ceresney and Mr.

Salsburg. Since that ruling, has the SEC or the FTC obtained email content through a subpoena issued to a third-party provider?

Mr. Ceresney. We have not, Senator Leahy, but we have done so in an excess of caution, and I think in deference to the reform discussions that have been ongoing in Congress. Our view--

Senator Leahy. And in deference to a 5-year-old Sixth Circuit case which has not been overturned?

Mr. Ceresney. No. Our view is actually that Warshak does not deny us the authority to obtain emails through an administrative subpoena. From our perspective, Warshak involved a grand jury subpoena with no notice to the subscriber. We always have given notice to subscribers, and there is a long line of Supreme Court and other circuit cases that say that an administrative subpoena with notice to a subscriber complies with the Fourth Amendment.

Senator Leahy. Mr. Salsburg?

Mr. Salsburg. We have not sought email content from a provider, either before the Warshak decision or since.

Senator Leahy. Okay. And you have affirmatively sought a legislative solution or change from Congress in the past 5 years?

Mr. Salsburg. No, we have not sought a solution until now.

Mr. Ceresney. We have obviously offered over the last few years to have ongoing discussions, and we have had discussions with the Committee.

Senator Leahy. Have you made a proposal?

Mr. Ceresney. We have. We have had discussions back and forth with various constituents.

Senator Leahy. Could you give me a copy of the proposal you made? I do not seem to recall that.

Mr. Ceresney. We have had discussions with staff about this issue over time.

Senator Leahy. Beginning 5 years ago, or just since Senator Lee and I looked like we might actually get something passed here?

Mr. Ceresney. No, I can only speak to the 2-1/2 years I have been Director of Enforcement. We have had discussions with the staff throughout that period of time.

Senator Leahy. And you have sent up a concrete proposal?

Mr. Ceresney. We have been discussing proposals with the staff for--

Senator Leahy. You have not sent up a concrete proposal from your agency?

Mr. Ceresney. Well, our view is we want to be responsive to proposals that Congress is providing, and so to the extent that staff for particular Senators or

Congressmen have offered us what they are thinking about, we have offered them our thoughts on those proposals.

Senator Leahy. Are you seeking wiretap authority for your civil investigations?

Mr. Ceresney. No, we are not.

Senator Leahy. But you do want to be able to read emails without a warrant?

Mr. Ceresney. What we are proposing, Senator, is some sort of judicial proceeding that would find some sort of standard, whether it be some sort of standard that would allow us then to obtain emails with notice to the subscriber as part of the proceeding so that the subscriber can raise any concerns that they have.

Senator Leahy. What about listening to your targets' phone calls?

Mr. Ceresney. No, we are not proposing that.

Senator Leahy. Would that not be more efficient, more effective?

Mr. Ceresney. Senator, we are not seeking wiretap authority. That is something that the criminal authorities have that we do not. That is not something we are seeking.

Senator Leahy. All right. Ms. Tyrangiel, how many Federal, State, and local agencies have civil regulatory authority that allows them to issue subpoenas for records?

Ms. Tyrangiel. Thank you for that question. Certainly

at the Department of Justice, there are a number of civil enforcement functions, including antitrust, tax, environment, civil rights. Since Warshak, they have been unable to get stored content from providers, and this has hurt their investigations and inserted delay and made it difficult in instances where they could not obtain information from subscribers.

Senator Leahy. My time is up. I am going to have a couple questions for the record on that.

[The questions of Senator Leahy follow:]

/ COMMITTEE INSERT

Senator Leahy. Thank you, Mr. Chairman.

Chairman Grassley. Thank you, Senator Leahy.

Now, Senator Hatch. Let me read here it will be Hatch, Whitehouse, Lee, who were here at the fall of the gavel. And then it would be Perdue, and then I assume we would go to the Democrat, Senator Franken, and then it would be Cornyn, Flake, and Tillis, of those who are here now. I guess Cornyn in not here, but, anyway, that is the way it will be.

Senator Hatch?

Senator Hatch. Ms. Tyrangiel, in your written testimony you stated that the Department had concerns about legislative proposals aimed at safeguarding data stored abroad from improper Government access. As you know, the Electronic Communications Privacy Act is silent on the privacy standard U.S. officials must satisfy in order to access data stored abroad. And yet the Federal Government has taken advantage of this statutory silence to apply its own standard.

What is the legal basis for law enforcement agents to use ECPA warrants to obtain data stored overseas?

Ms. Tyrangiel. Thank you for that question, Senator. There is a longstanding legal framework that allows the Government to serve compulsory legal process on United States companies to require them to bring back information

that is stored abroad. And the concern with proposals that would change that framework is that it would take away an option that has long been available under that framework and would replace it with international cooperation, which is not an adequate solution because those agreements that--that kind of cooperation does not exist everywhere. Only about half the countries we have agreements with. And because even when we can use those agreements, it takes a really long time and can delay investigations in times when we really need it to be fast.

Senator Hatch. Well, I do not agree with you on that point, and that is why I introduced the LEADS Act, to establish a legal framework for law enforcement to access data stored abroad or overseas. My bill is trying to help your efforts, and I would appreciate any suggestions you have that might make it a more workable bill or that might improve it or help you in your work.

Ms. Tyrangiel. We look forward to working with you.

Senator Hatch. Thank you. If Federal officials can obtain emails stored anywhere in the world simply by serving a warrant on a provider subject to U.S. process, nothing stops governments in other countries, including China and Russia, from seeking emails of Americans stored in the U.S. from providers subject to Chinese and Russian process. In fact, the lawyer who is litigating the Microsoft case on

behalf of the Government acknowledged last week that the ability for a foreign government to require disclosures of a U.S. provider "should be of some concern."

Now, are you concerned about the far-reaching or reciprocal consequences of the Government's current position on the extraterritorial reach of U.S. warrants?

Ms. Tyrangiel. Thank you for that question. This is a challenging issue, one that the Department is actively considering. Whatever the solution is, we do not think that the solution should involve deciding conflicts of laws in a way that always works against the United States. Historically, courts have been able to weigh sovereignty interests, the interests of U.S. victims, governmental interests, and other factors in coming to decisions on these issues, and the concern is any regime that would decide all matters of conflicts of law against the U.S. in every case.

Senator Hatch. Well, the Mutual Legal Assistance Treaty, or MLAT, process facilitates formal agreements for sharing evidence between the United States and foreign countries. Do you agree the process has proven slow and cumbersome to use?

Ms. Tyrangiel. It certainly is slow and cumbersome for us to get information from other countries, which is part of our concern. In the incoming process for MLATs, we agree that there needs to be progress made, and we are working on

progress, both technological and otherwise, and I know the administration has requested resources in aid of that effort to improve things further.

Senator Hatch. In your view, what can Congress do to improve the process? And how does another country access data stored here in the United States?

Ms. Tyrangiel. So, again, these are really challenging issues, and we look forward to working with you on them. One thing that is clear with the MLAT process is that it is not a one-size-fits-all kind of issue, and people work differently all around the world. And because it is so complicated, it requires an approach that takes into account the way that it is operating now, and we very much look forward to working with you to streamline the process.

Senator Hatch. Well, I look forward to working with you as well, and I hope we can streamline this process and make it work not only for you but for businesses and others as well.

Thank you.

Chairman Grassley. Senator Whitehouse.

Senator Whitehouse. Thank you, Chairman.

In evaluating this question of civil access to content maintained by the service provider, I take a step back to the question of a criminal warrant. A criminal warrant is obtained by a Government official going before a Federal

judge on an ex parte basis and getting the judge's consent to get access to the material involved. That protection is there, as I understand it, because of the immense power that criminal law enforcement gives to the Government, power of, for instance, incarceration. We even have a Federal death penalty. So from the very beginning, the Founders constructed a process that limited arbitrary access to information on the part of the Government when it had those terrible powers in its hands.

Ms. Tyrangiel, does the Government have any such powers with respect to civil enforcement?

Ms. Tyrangiel. It does not. Civil enforcement lacks warrant authority.

Senator Whitehouse. And what you are proposing is that, just like a warrant, the Government would have to go before a Federal judge in order to get access to the data for civil enforcement purposes.

Ms. Tyrangiel. There are a number of ways to do it, but, yes, having a court be able to compel that evidence.

Senator Whitehouse. A court order would satisfy you?

Ms. Tyrangiel. Yes.

Senator Whitehouse. And in a number of circumstances, your colleagues here on the panel have suggested that the subject might actually be, the subscriber might actually be notified first, or that there might be notice to the

subscriber, so it would not be an ex parte proceeding; it would be a proceeding in which the individual whose privacy interest was involved had every right to appear, correct?

Ms. Tyrangiel. That is correct.

Senator Whitehouse. All right. Now, what happens, Mr. Salsburg, in the case that you talked about where, for a variety of reasons, you do not want to reveal to the misbehaving party that this investigation is under way because they are likely to abscond or hide assets or destroy evidence or whatever? Do you want some form of ex parte process like a warrant provides where the civil agency could say, look, these are extraordinary circumstances, this is why we need access ex parte to this information, and try to convince the judge of that?

Mr. Salsburg. We are not actually asking for that authority.

Senator Whitehouse. So why are you talking about the-- why did you use that example of the importance of it?

Mr. Salsburg. Well, I suppose I conflated the previously public content argument that we have, where we would still want to be able to get the content from a provider when we are talking about content where there is no reasonable expectation of privacy.

Senator Whitehouse. Do any of you seek a proposal under which the Government would be able to make a showing

that an ex parte provision is necessary and go forward without notice to the subscriber?

Mr. Ceresney. We are not. From our perspective, in fact, we typically will seek the email from the subscriber first, and if we are not able to obtain or do not believe we have obtained full emails, then we will go to the ISP.

Senator Whitehouse. So even though the Constitution allows the warrant requirement that we are relying so much on to be ex parte, you are not requesting that.

Mr. Ceresney. We are not. What we are looking for is a limited ability to obtain ISP emails in appropriate cases where we just cannot get them from--

Senator Whitehouse. Through a court order, from--

Mr. Ceresney. Through a court order.

Senator Whitehouse. --perhaps the very same judge who you might have to go before to get the warrant.

Mr. Ceresney. The very same judge, and that is why I say--

Senator Whitehouse. Only in this case, the party would be present and have every right to defend their privacy interests.

Mr. Ceresney. Exactly. And that is why I said in my oral testimony and in my written statement that that actually is more protection than a warrant provides.

Senator Whitehouse. It sure is. All right.

Thank you very much, Mr. Chairman--oh, may I ask--I have a minute left before I yield back my time.

Just to be clear, I think Chairman Grassley asked you this, but just in case it did not come through as clearly to you as it did to me, I would be interested in looking back at cases that have come to a conclusion and where there is a public disclosure of the case, where you can take a look at the case and say this piece of evidence actually helped make that case and we got it because we were able to have access through the service provider to that information--not an ongoing case, which I know is a very delicate circumstance for all of you, but closed cases, looking back, just so we can see whether or not this has made a difference in real life in the past.

And, with that, I will yield back my time, Mr. Chairman. Thank you for holding this hearing.

Chairman Grassley. Thank you.

Now, Senator Lee.

Senator Lee. Thank you, Mr. Chairman, and thanks to all of you for being here.

You know, updating the Electronic Communications Privacy Act has been a priority of mine ever since I arrived in the Senate. And now that I have been here for about 4-1/2 years, I appreciate more fully how difficult it can be to bring about a change of law that basically everyone

agrees on.

Now, the overwhelming majority of the American people--and by "overwhelming majority," I mean 99.9 percent of anyone you ask--can agree that the Government ought to have a warrant before it goes after your email, the content of your email.

Number two, the same number of people would agree, I think by about the same ratio, that it ought not make any difference whether that email is 179 days old or 181 days old, whether or not the Government has to get a warrant.

And so, you know, this is a very simple principle that ought not be all that difficult to legislate, but I have been honored to work on this legislation, and I introduced Senate bill 356, the ECPA Amendments Act, along with Ranking Member Leahy, to bring our laws into conformity both with expectations of members of the public and what seems to be widely followed practice today.

To start out with, I want to ask each of you a simple yes-or-no question. I want to ask you: Does your agency believe that it should under normal circumstances--meaning in the absence of a generally applicable, widely recognized exception to the warrant requirement, should it be required to get a warrant in order to get at the content of people's emails, regardless of the age of the email? We will start with you, Ms. Tyrangiel.

Ms. Tyrangiel. The Department has indicated that we do not oppose a warrant requirement for our criminal entities when they are obtaining information from a third-party provider to the public, but note some concerns about that rule where there is no warrant authority available like in our civil investigations.

Senator Lee. Okay.

Mr. Ceresney. If I understood your question correctly, the answer is no. We believe that a judicial proceeding, as we have been discussing, that has notice to the subscriber and allows the subscriber to object is an appropriate mechanism for obtaining emails.

Senator Lee. Mr. Salsburg?

Mr. Salsburg. We agree with the SEC's position.

Senator Lee. Okay. So I do think that while there are a few people in Washington, D.C., who can understand what you are saying, I think the overwhelming majority of the American people would be very disturbed to hear that that question cannot be answered with a simple no, that the Government should not be able to get at people's emails, the content of their email, without a warrant.

Now, let me direct a question your way, Ms. Tyrangiel. I am concerned that the Department of Justice, once it has obtained emails, may use those emails for any investigation related to the initial reason for the acquisition or not.

So if you obtained emails on a mere subpoena in a civil investigation, what, if anything, would prevent those same emails that you obtained without a warrant in the context of a civil investigation with a subpoena, what would prevent the Department from using that in a criminal prosecution?

Ms. Tyrangiel. So certainly it would not be acceptable for things to be obtained on the civil side for the purposes of trying to use it on the criminal side. When things are in use, they should be done according to the authorities that are available.

However, when criminal evidence becomes apparent, that information can be shared, and we are not proposing a way to get around the warrant requirement without any privacy protections and that there should--there are ways of protecting privacy both by standard and by process. And so what we are talking about on the civil side is a process protection.

Senator Lee. And what kinds of safeguards would the DOJ propose in order to prevent a civil agency carveout from being used to avoid the warrant requirement? You can understand how that could easily be manipulated in order to avoid the warrant requirement.

Ms. Tyrangiel. Thank you for that question. I do not believe this instance is really any different than the other sorts of evidence that can be obtained in other ways. These

are issues that exist as to all investigations. Prosecutors and civil litigators and investigators are held to a standard to obey the rules and hold to those rules and follow the process that the law requires. But I am happy to get back to you if there are further questions or to talk-- to answer further questions.

Senator Lee. Okay. Thank you. I see my time has expired, Mr. Chairman.

Chairman Grassley. Thank you, Senator.

Now, Senator Franken.

Senator Franken. Well, since Senator Leahy asked me to be here as Ranking Member, I have to be here. So can Senator Blumenthal go next? Because I am forced to be here next to you. I am required.

[Laughter.]

Chairman Grassley. Go ahead, Senator Blumenthal.

Senator Blumenthal. Thank you. I want to thank Senator Franken for his courtesy.

I am curious, Mr. Salsburg. In your testimony you expressed concern about what would happen if a customer consents to having her service provider turn over emails, but the service provider nonetheless refuses. Can you give us some examples of how and when that might occur if a customer says okay but the service provider says no? When and how would that occur?

Mr. Salsburg. Sure. Let me give you two examples.

The first is, assuming that we are investigating a business and the business is ready and willing to turn over information to us, but it maintains it all in the cloud, and the cost of that customer, that target getting the information from the cloud provider is significant, where if they were just to authorize us to go to the cloud service provider and use our litigation support folks, they would rather have that happen.

You know, is that going to happen all the time that a target is willing to turn over its information en masse to the Government? No. But if that scenario arises, the Commission should be able to take that consent and use compulsory process to get that information from the provider.

The second scenario is the customer is a victim and the victim no longer has access to the content of the claim that has been made to them, and they want the Government to go get it.

Senator Blumenthal. Have those two scenarios actually occurred?

Mr. Salsburg. There have been a couple of instances where this has occurred, but it is not common. And what we are concerned about is as the move to cloud computing gets more ingrained and gets further along, these scenarios may

happen more frequently.

Senator Blumenthal. Does the FTC have any recourse against the target of a subpoena if that target fails to do everything in his or her power to get emails from his service provider and get the provider to turn them over?

Mr. Salsburg. It does. We can file a--if we are talking about an investigative demand, we can file an enforcement action. But at the end of the day, if the customer refuses to turn the information over, we would have no ability under the pending legislation to get that information.

Senator Blumenthal. Under the pending legislation.

Mr. Salsburg. Right.

Senator Blumenthal. Under which?

Mr. Salsburg. Under the--

Senator Blumenthal. 356?

Mr. Salsburg. 356, yeah.

Senator Blumenthal. Okay. So that is a suggestion that you have for improving it.

Mr. Salsburg. Yes. And, interestingly, the provision of ECPA that authorizes a provider to voluntarily provide information authorizes it to turn over the content with consent voluntarily to the Government, and we just want to make sure that there is a parallel provision that allows the Government to compel it in those circumstances.

Senator Blumenthal. If the target of an investigation has intentionally used an Internet provider that will not cooperate with the FTC so that target can pretend to consent but then, in effect, use the refusal of the Internet provider as the barrier, is there anything the FTC can do to penalize the target? If you understand my question.

Mr. Salsburg. Yes. You know, we can seek to compel if we are talking about an investigative demand, but ultimately we do not have the authority to penalize anybody.

Senator Blumenthal. Well, I welcome your suggestions for improving this legislation. As you know, I am one of the original cosponsors of S. 356. I think it is important to strike that balance between privacy and law enforcement, having been in law enforcement myself, having been a strong supporter of the work that all three of your agencies do, and very much welcome your suggestions here and any other thoughts that you may have.

Thank you, Mr. Chairman.

Chairman Grassley. Senator Perdue?

Senator Perdue. Thank you, Mr. Chairman, and thanks to the witnesses for your time today.

Obviously, this is--we have had similar conversations where we are trying to balance privacy and enforcement. It is ongoing, and I applaud your efforts and your leadership in that. I look forward to debating both ECPA and the LEADS

Act, and I want to applaud the Ranking Member and Senator Lee for their hard work on these bills.

Ms. Tyrangiel, I have a quick question related to LEADS. As we know, and I think you have just explained, LEADS would create a rule that Government may use ECPA warrants to obtain content data stored outside the U.S., but only if the account holder is a U.S. person. In all other cases involving content data stored abroad, it would require the Government to utilize the MLAT process, as I understand it.

I know that DOJ has concerns about the LEADS Act. What is your view on the provisions of the bill that seek to improve and streamline the MLAT process?

Ms. Tyrangiel. Thank you for that question. Improving the MLAT process on an incoming basis, which is what that proposal is talking about, is difficult and complicated, and we very much look forward to working with the Committee on that. We do think it is not a one-size-fits-all kind of solution, and having provisions that apply, for instance, to require sort of online intake when not all countries actually use government email to send in their requests is the sort of thing that makes this hard. So we very much look forward to working with you to address those issues.

Senator Perdue. Can you explain the DOJ's concerns that I think DOJ has expressed regarding the effect of the

LEADS Act on domestic investigations, particularly those involving a non-citizen who is physically in the U.S.?

Ms. Tyrangiel. Thank you. The Department would be concerned with any proposal that would unilaterally take away a tool that we have in order to be able to obtain information about a U.S. crime affecting U.S. victims that historically has been in place for a long time and replace it with something that would take a really long time through international cooperation alone. And proposals that would also make it more difficult to get information about non-U.S. persons committing crimes in the U.S. than it would U.S. persons is also a concern for us.

Senator Perdue. I see. Mr. Ceresney and Mr. Salsburg, one last quick question. I want to go to the subpoena issue that was raised just a minute ago about your agency's ability to enforce subpoenas directly on the target of a civil enforcement action. I ask that particularly because of the Federal court decisions holding that an individual can be required to comply with a subpoena to produce content data that is being maintained by a service provider.

Can you give me your views and let us clarify that just a little bit further, if you do not mind? Mr. Ceresney?

Mr. Ceresney. Sure. Well, our subpoenas are not self-executing, so, in other words, if somebody objects to our subpoena, we need to go to court and obtain a court order

compelling production of the materials. That person in that proceeding can raise whatever objections they have, whether it be privilege or other relevancy objections or the like. And the case law essentially says that if we show a proper purpose and if the subpoena is properly tailored, it will be upheld. And so in those circumstances, we can obtain the email from the subscriber, but the problem obviously, as we have been talking about, is the subscriber will often not provide you with full email because they are incentivized not to. And if they know we cannot obtain the email through the ISP, that further incentivizes them not to provide us with full email.

Senator Perdue. What is your actual experience there of targets who actually do provide that information versus the ones you have to go get the warrant?

Mr. Ceresney. When we have to get the warrant or when we have to--

Senator Perdue. Well, when you have to go to the second step of actually trying to get the information.

Mr. Ceresney. Yeah, well, we have frequently brought subpoena enforcement actions. Obviously, in many cases we make a judgment. There are resource constraints about bringing subpoena enforcement actions, and obviously, we make a judgment about whether to compel in a particular case.

I will say that our experience is that in certain cases subscribers provide full emails; in others, they don't. And that becomes clear because, as you subpoena others who were involved in the misconduct, you sometimes find that the other people supply you with emails that the original subscriber did not, and that tells you that the original production was not sufficient.

Senator Perdue. Mr. Salsburg?

Mr. Salsburg. We have a similar process to the SEC where our civil investigative demands are not self-executing. We do need to go to a court to enforce them as well.

In our experience, I think most targets usually comply with our CIDs. If they do not, we have to them make a resource judgment call. Is it worthwhile to pursue an enforcement action which is pretty lengthy and may not result in us being able to get recourse for consumers quickly? Or do we forgo the information and try to find the necessary information in another way?

Senator Perdue. Okay. Thank you.

Thank you, Mr. Chairman.

Chairman Grassley. Senator Franken.

Senator Franken. Thank you, Mr. Chairman.

Mr. Salsburg, the FTC plays a key role in protecting Americans' privacy, and Americans understandably care deeply

about the privacy of their emails and other online documents. Since the Warshak decision, their expectations have largely been met, and the ECPA Amendments Act would ensure that those expectations continue to be met. And I applaud Senators Lee and Leahy for their efforts--I guess more Senator Leahy because he is my Ranking Member.

[Laughter.]

Senator Franken. So I do find, Mr. Salsburg, the final portion of your testimony a little surprising. I did not expect to hear the FTC's Bureau of Consumer Protection suggesting that the ECPA Amendments Act be significantly rewritten to give FTC broad authority to obtain via simple court order Americans' email content from third-party service providers. And then this morning we received Commissioner Brill's statement expressing her concern about this proposal. Commissioner Brill notes that it is "exceedingly rare" that it would be useful for the FTC to seek content through ECPA, and she highlights the cost for Americans' privacy as well as the question of constitutionality or patient unconstitutionality of obtaining content with just such a court order--or with just a court order.

I realize your oral presentation today reflects only your views, but I am interested in your view and data that you may have. Setting aside potential constitutional

concerns for the moment, do you have any data, any case statistics to support your claim that a new expansion of FTC authority to obtain mail content is needed?

Mr. Salsburg. Let me first note that we have not sought email content in the past, and the question is whether the economy is changing in a way, with data moving to the cloud computing, that we can see it being foreseeable in the future. I do not have any empirical evidence of this, but I think one of the major drivers of ECPA reform is this very notion that data is being kept in the cloud with third-party service providers and no longer being maintained locally on people's computers.

Senator Franken. Okay. Thank you. I am sorry I was not here for the beginning, so is it "Ceresney"?

Mr. Ceresney. Yes.

Senator Franken. Very good--to me. Under ECPA, as it was written in 1986, subpoenas could be used to compel a third-party provider to disclose the contents of a customer's emails if the emails were relatively old, more than 180 days old. Now courts have taken issue with that, and personally I think that is not what the American people expect when it comes to the privacy of their emails. We have been discussing that.

But if I am understanding your testimony correctly, you are not satisfied with even the ECPA standard. You are

looking for new and broad authority for Federal regulatory agencies like SEC and IRS to be able to obtain content without a warrant, without regard to the age of the information.

In the last 5 years, has the SEC sought to challenge Warshak or to take action against providers who refuse to comply with requests because of Warshak?

Mr. Ceresney. Senator, we have not, in deference to the ongoing discussions in Congress about ECPA reform. But what I would say is what we are seeking is actually more protections than in the current ECPA; that is, the current ECPA allows an administrative subpoena with notice to the subscriber. What we are proposing is some sort of judicial proceeding where we would obtain a court order--and I think you use the term "just a court order," but a court order is essentially what a warrant is, which is a judge signing off on an order that allows us to obtain email, and in our case what we are proposing is with notice to the subscriber so that the subscriber, unlike a warrant, which is ex parte, the subscriber could come in and assert any objections that they have.

So I think what we are proposing is actually more protection, first of all, than in the current statute and, second, than in a warrant.

Senator Franken. So you take issue with my saying

"just a court order"?

Mr. Ceresney. Yes, I do, with all due respect.

Senator Franken. I appreciate the respect. Thank you.

Thank you, Mr. Chairman.

Chairman Grassley. Thank you, Senator Franken.

Senator Tillis?

Senator Tillis. Thank you, Mr. Chair and Mr. Acting Ranking Member.

Mr. Chair, I also want to wish you a happy birthday in advance. I think you are celebrating maybe the 32nd anniversary of your 50th birthday tomorrow.

[Laughter.]

Senator Franken. That would make you 82, I think.

Senator Tillis. Now that I am 55, I started celebrating anniversaries about 5 years ago.

I want to ask a question that may also be appropriate for the second panel. I have got to go back to the Armed Services Committee, so I will start the discussion here. I am concerned with your efforts when it involves an ISP that is not within U.S. jurisdiction and efforts that we would have here to strengthen our ability to get to information for U.S.-domiciled ISPs and the potential risks that that could have for people who may intend to use this for the kinds of purposes that you are going after; some may or may not be.

What risks do we have going beyond just the 180-day retention requirement, dealing with that, and clarifying the obligations of the ISPs with respect to their warrant requirements, what risks do we have of just having the snakes go to another pasture and still be able to do what they want to accomplish or still be able to fall under that veil, and then put our ISPs at risk? I will open that up to the panel. We will start down there.

Ms. Tyrangiel. Thank you for that question. When there are providers that are doing business in the U.S., historically the courts have exercised jurisdiction over those individuals, and--

Senator Tillis. What is the variability if you go outside, or what has your experience been?

Ms. Tyrangiel. Well, in order to be able to get something, there needs to be a basis for jurisdiction. And so one of the things that concerns us about proposals that talk about data stored abroad is making that data where there are people even in the U.S. unable to use traditional legal process to compel that information that they may store elsewhere to come back to the United States.

Mr. Salsburg. This is a very challenging question, and the Commission has not taken any position on the LEADS Act, and I think it is fair to say that we would have difficulties on the civil side, as the law is now, if we

were trying to compel information from a foreign ISP that did not have presence in the United States.

Senator Tillis. So, again--and I do want you to respond--a concern that I have is making sure that whatever we do, as long as there is some other place on the globe, you know, the Internet infrastructure is a global infrastructure subject to several different jurisdictions, how we balance policy to make sure that we are not just tying the hands of businesses here to the benefit and to your detriment to ISPs abroad, and, Mr. Ceresney, we will let you comment.

Mr. Ceresney. I would just say we share some of the same concerns that the Department of Justice has about the LEADS Act. And, obviously, it is a thorny issue and one that needs to be worked carefully.

Senator Tillis. Mr. Ceresney, I think you mentioned--it may have been in your opening comments; I apologize for not being here for it--that subpoenas frequently fall short of getting the evidence they want because oftentimes the targets have either deleted the information or they absconded. What is at least working through Congress right now that you think helps you address that issue? Or what kinds of things do we have to look at to help you have that tool available?

Mr. Ceresney. Yes, well, what we are seeking is some

limited authority to obtain, in circumstances like the ones that you just cited where individuals have deleted emails or otherwise not produced to us, some ability to obtain those emails from the ISPs, and what we have proposed is some sort of court order under some standard that we would need to meet, with notice to the subscribers so that they could come in and object. And that is the limited authority that we are seeking here, and the idea is in circumstances like the one that you have just suggested where the individual has deleted the emails, we are able to obtain it. And what that would also do is incentivize people who are producing emails pursuant to our subpoenas to comply fully, because if they know that we can go to the ISP, it further incentivizes them to provide us with their full email.

Senator Tillis. Thank you. And because I have only got 25 seconds, I will just make a comment. I know that, on the one hand, we want to provide you all and the next panel, which will have law enforcement on it, with all the tools that you need to get after people that may be doing things that we do not want them to do.

On the other hand, we are talking about extending some of these capabilities to agencies who right now, such as the IRS--I do not think that was mentioned, but I think that would extend to agencies like the IRS that give us some pause to give them more capabilities than they already have.

So we have got to work on making sure that we have got the right kinds of controls in place as we move forward with the policy. Thank you all for being here.

Thank you, Mr. Chair.

Chairman Grassley. Senator Sessions.

Senator Sessions. Thank you, Chairman Grassley, for your leadership on this and for asking the appropriate questions and having an opportunity to discuss this. It is a very big issue. Those of us who have been involved in law enforcement for a long time are very well aware of what sounds like some good, theoretical idea can have a major and detrimental impact on the ability of the people of the United States to have order, to avoid multiple frauds and thefts and computer abuses and violations of their privacy, and things of that kind. And I had ordered a publication not long ago, and within a few weeks, I got I do not know how many more selling me different kinds of publications of a similar nature. So somebody is sharing information all over. President Obama was widely congratulated for his brilliant ability to target voters because they knew all kinds of things about him, where they went fishing, all these things somehow are available to private sectors, political candidates, and we have to be sure that we are not placing too much of a burden on law enforcement as they try to do their duty to protection us from fraudsters and sex

abuse and child kidnappers and terrorists. I just really think we have got to be careful about it. So I am glad that the Chairman is looking at this and we are asking it.

The law enforcement that I have talked to indicate that they have certain problems that we ought to deal with in the legislation. One is that there is often very long delays between the issue of a request to subpoena or an order to the actual production of the documents.

Two, we ought to consider what happens if you have erasure of these documents within hours even, or a few days. Is that appropriate? We do not allow that in phone company records, as I understand it.

And, third, I think it is critical--anybody who has been involved in law enforcement, I can imagine in a terrorist investigation particularly, you have got to be able to effectively not tell the suspect that you are on to him and have somebody call him and say, "The FBI just subpoenaed your toll records," and, boom, they flee the country or they hide other evidence that may be available. So I just think those are law enforcement requests that need to be considered.

Ms. Tyrangiel, so you can issue a subpoena for a telephone toll record that has the person's name, address, the link to their phone calls, the numbers that they called, without any content. You can get that with a subpoena. Is

that correct?

Ms. Tyrangiel. Yes, that is correct.

Senator Sessions. And, actually, DEA can get it with an administrative subpoena, and so can the IRS, without even asking a prosecutor's approval. Prosecutors issue them routinely also.

Well, what about getting an email address? It seems to me that is quite a huge difference between just getting who the person has been emailing, just like you want to know who they called on a telephone, as opposed to the contents of that email. Can that be obtained? And why should we enhance significantly the ability to get that information?

Ms. Tyrangiel. Thank you for that question. The standard is currently different. As I note in my SFR, the Department does support equalizing those standards and bringing them in so that you can actually use the same standard that we have been using for traditional telecommunications like telephone records to obtain the to-from material as well.

Senator Sessions. Well, that is a huge thing in a lot of investigations. Somebody says, "I never met this person." Then they have got 50 emails to them or 25 phone calls. "I did not talk to them on the day of the killing," and then there are 25 phone calls that day. This is hugely important in actually protecting the American people from

criminals.

Then you have got the standard for content. Mr. Ceresney mentioned that a court order is not much different from a search warrant. So you have a little less standard to get the older email contents. Is that correct? Is that email contents you first get through the 120 days and older?

Mr. Ceresney. Under the current statute, for more than 180 days, we can obtain them through an administrative subpoena with notice to the subscriber. But as I have said, in terms of an amendment to the statute, what we would support is some sort of judicial proceeding with notice to the subscriber that allows us to obtain those emails, contents.

Senator Sessions. And you can request the confidentiality and no notice?

Mr. Ceresney. We are not seeking that authority to obtain them with no notice. In fact, our general practice is to first seek them from the subscriber, and if we do not obtain emails, then to go to this mechanism. We recognize there are important privacy interests here, and we are trying to accommodate those while at the same time preserving some ability for us to obtain in appropriate circumstances the contents of emails.

Senator Sessions. My time is up. I really think we have got to be careful about not having an ability to

protect against disclosure to the person, because I do not--that is not true in other areas, that you can get a non-disclosure order, and it can be critical--if you are investigating a terrorist and they know you are on to them, this could be a life-and-death issue.

Thank you.

Chairman Grassley. I thank this panel. I appreciate it very much, and we will probably be in touch with you with some follow-up questions.

Chairman Grassley. I would like to call the second panel now, and while they are coming, if I can have your attention, I want to introduce them to be efficient.

Richard Littlehale is Assistant Special Agent in Charge, Tennessee Bureau of Investigation's Technical Services Unit. Special Agent Littlehale is responsible for coordinating the use of a wide range of technology in support of law enforcement operations, including using communication records in support of criminal investigations. He testifies on behalf of the Association of State Criminal Investigative Agencies. He received his bachelor's degree from Bowdoin College and his law degree from Vanderbilt.

Second is Richard Salgado. He serves as Google's director of law enforcement and information security. Before working at Google, Mr. Salgado worked at Yahoo! and prior to that served as special counsel in the Computer Crime and Intellectual Property Section at DOJ. He has also been a law professor at Stanford, Georgetown, and George Mason. He received his undergraduate degree from the University of New Mexico and law degree from Yale.

Next is Chris Calabrese, who is vice president of policy for the Center for Democracy & Technology. Before joining CDT, he worked as legislative counsel, American Civil Liberties Union, Washington office. Before that, he was legal counsel to Massachusetts Senate Majority Leader.

Mr. Calabrese graduated from Harvard and has a law degree from Georgetown.

Finally, Victoria Espinel is president and CEO of BSA | The Software Alliance, which advocates on behalf of software industry before governments. She previously served for over a decade in the White House under both Republican and Democrat administrations, including being nominated to be the first U.S. Intellectual Property Enforcement Coordinator. She graduated from Georgetown School of Foreign Service, has an LLM from the London School of Economics, and a law degree from Georgetown.

I want to thank all of you for appearing, and let us do it in the order that you are seated there left to right, my left to right.

STATEMENT OF RICHARD LITTLEHALE, ASSISTANT SPECIAL AGENT IN CHARGE, TECHNICAL SERVICES UNIT, TENNESSEE BUREAU OF INVESTIGATION, NASHVILLE, TENNESSEE

Mr. Littlehale. Chairman Grassley, Ranking Member Leahy, Senator Franken, and members of the Committee, thank you for inviting me to testify. I am a technical investigation in Tennessee, and I serve on the Technology Committee of the Association of State Criminal Investigative Agencies. I am pleased to speak on behalf of the State and local enforcement officers who work the majority of investigations in this country and to share a criminal investigator's perspective on the challenges that law enforcement faces when working today's digital crime scenes.

The challenge of lawful access to electronic evidence is top of mind every day for those of us in the trenches, and while we agree that the law should be updated, any effort to reform ECPA should also reflect its twofold aim of protecting privacy and assuring law enforcement's ability to obtain digital evidence when lawfully authorized to do so.

I have three points for your consideration this morning.

First, we have some concerns about the pending legislation, Senate bill 356. It might well be time to protect additional stored content with a probable cause

standard, but this bill creates greater protection for stored digital content than for a letter in someone's house. Bringing ECPA into balance should put the physical and digital worlds on the same plane, not favor digital evidence over physical evidence.

The notice provisions in the bill also seem one-sided. It is hard for investigators to understand why there are no requirements for how quickly service providers must respond to our legal demands for evidence, but we should be required to notify customers that their records have been obtained as quickly as 3 to 10 days from service of process. We urge the Committee to carefully balance the need for notification against the resource burden it places on us. Time spent complying with arbitrary timelines for notice means less time investigating crimes in an era where digital evidence is a factor in most investigations.

We also have grave concerns about challenges that we have been very vocal about and which the legislation does not address. Whatever legal standard Congress decides to impose for Government access to electronic content, the public has a powerful interest in law enforcement's ability to actually get that information once we comply with the law.

The reality is that legal barriers are not the only barriers to obtaining communications records. Non-technical

barriers and lack of a consistent legal framework governing service provider response slow our efforts as much or more than a change in the standard of proof. I urge you to ensure that whatever standard of proof you decide is appropriate, you also ensure that law enforcement can access the evidence we need reliably and quickly. There is no requirement in ECPA or in the bill before the Committee today imposing any structure on how service providers respond to our legal demands. Some respond quickly; others do not. This is clearly problematic in emergencies, and it also can prevent us from efficiently processing large volumes of leads. Consider a pool of cyber tips from the National Center for Missing and Exploited Children that might contain clues to the location of a child being victimized or pages and pages of online ads that could hide sex-trafficking victims. There may well be an emergency in there somewhere, but we cannot know about it until we get routine response back from the service providers. Speed is important in all investigations. A requirement for automated exchange of legal process and response from service providers should be considered. Not only would this help speed access to evidence, it could provide a great deal of transparency around Government entities' access to records, companies, law enforcement, and Congress.

Third, law governing access to emergency records should

be revised. Everyone agrees that law enforcement should have rapid access to communications evidence in a life-threatening energy, but that is not always the reality. The emergency provision in today's ECPA is voluntary for the providers, not mandatory. Even when emergency access is granted, there is no guarantee we will get the records immediately. In some cases, we cannot even get someone on the phone, and in other cases, the provider has chosen never to provide evidence in the absence of legal process, no matter the circumstances. Neither ECPA nor the reform bill fix this issue.

In an effort to better inform the Committee, I solicited feedback on these non-technical barriers from a wide range of law enforcement agencies, specialties, and investigative focuses. The replies underscored the frustrations of investigators regarding routine turnaround times from some providers that are measured in months, the inability to speak to a human being about a case in a timely manner, and uneven access to records and emergencies. They talked about service providers who routinely pre-litigate the legal process instead of leaving that to the courts or who return legal documents without complying because the demand failed to use the specific terms that the provider prefers, regardless of whether or not those terms are legally required.

We appreciate the current bill's requirement for GAO to look at those issues, and we hope they find a way to tell our stories. These are the day-to-day realities of professionals working the digital crime scene. The public never heard about these things, but those of us who spend our days and many of our nights gathering digital evidence to find criminals and investigate their crimes need Congress to understand and think about the implications and possible solutions.

In closing, I want to reemphasize how important both aspects of ECPA are to our Nation's criminal investigators. We are well aware of ECPA's role in balancing privacy and public safety. We also depend on it as a critical tool and set of rules that guides how we obtain the digital evidence that is a key to an ever-increasing number of cases. We urge the Committee to balance both these ECPA bills as we all work to get ECPA reform right for the 21st century.

Thank you for having me, and I look forward to your questions.

[The prepared statement of Mr. Littlehale follows:]

Chairman Grassley. Thank you.

Mr. Salgado?

STATEMENT OF RICHARD SALGADO, DIRECTOR, LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE, INC., MOUNTAIN VIEW, CALIFORNIA

Mr. Salgado. Chairman Grassley, Ranking Member Leahy, and members of the Committee, thank you for the opportunity to appear before you today. My name is Richard Salgado. As director for law enforcement and information security for Google, I oversee the company's compliance with Government requests for users' data, including requests made to pursuant to the Electronic Communications Privacy Act of 1986, otherwise known as ECPA. In the past, I have worked on ECPA issues as senior counsel in the Computer Crime and Intellectual Property Section in the Department of Justice.

Google strongly supports S. 356, the ECPA Amendments Act of 2015, which currently has 23 cosponsors. The House companion measure, the Email Privacy Act, now has 292 cosponsors, more than any other bill that is pending in Congress. It is undeniable, it is unsurprising that there is strong interest in aligning ECPA with the Fourth Amendment and users' reasonable expectations of privacy.

The original disclosure rules set out in ECPA back in 1986 were foresighted given the technology that existed at the time. In 2015, however, those rules no longer make any sense. Users expect, as they should, that the documents they store online have the same Fourth Amendment protections

as they do when the Government wants to enter the home to seize the documents stored in a desk drawer. There is no compelling policy, there is no compelling legal rationale for there to be different rules.

In 2010, the Sixth Circuit opined in United States v. Warshak that ECPA violates the Fourth Amendment to the extent that it does not require law enforcement to obtain a warrant for email content. In doing so, the Sixth Circuit effectively struck down ECPA's 180-day rule and the distinction between opened and unopened emails as irreconcilable with the protections afforded by the Fourth Amendment. Google believes the Sixth Circuit's interpretation in Warshak is correct, and we require a search warrant in all instances when law enforcement seeks to compel us to disclose the contents of Gmail accounts and other Google services. Warshak lays bare the constitutional infirmities with the statute and underscores the importance of updating ECPA to ensure that a warrant is uniformly required when governmental entities seek to compel third-party service providers to produce the content of electronic communications.

Warshak is effectively the law of the land today. It is observed by governmental entities and companies alike. In many ways, S. 356 is a modest codification of the status quo and the implementation of the Sixth Circuit's conclusion

in Warshak.

Between the last time I testified in support of updating ECPA in March of 2013 and now, the Supreme Court issued a landmark decision in Riley v. California, where it unanimously held that generally officers must obtain a warrant before searching the contents of a cell phone incident to an arrest. Chief Justice Roberts noted that a regime with various exceptions and carveouts "contravenes our general preference to provide clear guidance to law enforcement through categorical rules."

To reinforce the constitutional imperative for clear rules in this area, Chief Justice Roberts concluded his opinion with unambiguous direction to law enforcement. He wrote: "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple--get a warrant."

Notably, this Committee is being asked by some today to jettison precisely the type of categorical rules that the Supreme Court held were imperative in Riley. Doing so would undermine users' reasonable expectations of privacy and encroach upon the core privacy protections afforded by the Fourth Amendment. We urge the Committee to reject such

please and to codify the bright-line, warrant-for-content standard that is reflected in the bill sponsored by Senators Lee and Leahy.

ECPA no longer reflects users' reasonable expectations of privacy and no longer comports with the Fourth Amendment. S. 356 represents an overdue update to ECPA that would ensure electronic communications content is treated in a manner commensurate with other papers and effects that are protecting by the Fourth Amendment. It is long past time for Congress to pass a clean version of S. 356.

Thank you for your time and consideration, and I would be happy to answer any questions you have.

[The prepared statement of Mr. Salgado follows:]

Chairman Grassley. Mr. Calabrese?

STATEMENT OF CHRIS CALABRESE, VICE PRESIDENT,
POLICY CENTER FOR DEMOCRACY & TECHNOLOGY,
WASHINGTON, D.C.

Mr. Calabrese. Thank you, Chairman Grassley, Ranking Member Leahy, Ranking Member Franken, and members of the Committee. Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology. CDT is a nonpartisan, nonprofit policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech, and access to information. We applaud the Committee for holding a hearing on the Electronic Communications Privacy Act and urge the Committee to speedily approve S. 356, Senator Lee and Leahy's Electronic Communications Privacy Amendments Act.

Every day, whistleblowers reach out to journalists--and members of this Committee--advocates plan protests against injustice, and ordinary citizens complain about their Government. All of these activities are crucial to our democracy. They also all rely on our long-held constitutional guarantee of private communications, secure from arbitrary access by the Government. This is true whether the communication happens in the form of a letter, a phone call, or, increasingly, an email, text message, or over a social network. But as our technology has changed, the legal underpinnings that protect our privacy have not

kept up.

When ECPA was enacted in 1986, it relied on balancing three policy pillars: individual privacy, the legitimate needs of law enforcement, and support for innovation. Changes in technology have eroded this balance. The reliance on trusted third parties for long-term storage of our communications have left those communications with limited statutory protection. This void has created legal uncertainty for cloud computing, one of the major business innovations of the 21st century and one at which U.S. companies excel.

At the same time, information accessible to the Government has increased dramatically. Emails and text messages provide invaluable leads, insight into criminal activities and plans, and demonstrate motive and intent. Most, if not all, of this information would not have been available in 1986. In combination with the vast new stores of meta data, it is clear that for law enforcement this is a golden age of surveillance.

In the face of an outdated statute, courts have acted, recognizing in cases like U.S. v. Warshak that people have a reasonable expectation of privacy in their email and at the same time invalidating key parts of ECPA. But that patchwork is not enough on its own. It continues to lag behind technological change and harms smaller businesses

that lack an army of lawyers. It also creates uncertainty around new technologies that rely on the use and storage of the contents of communication.

Reform efforts also face a concerted assault from civil agencies that seek to gain new powers and blow a huge privacy hole in the bill. Agencies have blocked reform in spite of the fact that the SEC has confessed to never using subpoena powers post-Warshak. No less than FBI Director Comey told the House Judiciary Committee that, in regard to ECPA, a change "would not have any effect on our practice."

Criminal investigators have also suggested that changes be enacted so that companies turn over the entire contents of user inboxes whenever an emergency is asserted. However, it is not clear this is a problem. Major companies report only a few hundred of these requests every year. More troubling, approximately 20 percent of them must be rejected because they failed to meet the emergency standard.

Support for privacy reform is deep and abiding. More than 100 technology companies, trade associations, and public interest groups have signed on to ECPA reform principles. Signatories include nearly the entire tech industry, span the political spectrum, and represent privacy rights, consumer interests, and free market values.

The companion bill in the House has more than 290 cosponsors, including a majority of Republicans and

Democrats. The Committee has consistently sought to solve these problems through strong reform measures, passing nearly identical legislation to S. 356 in both 2012 and 2013. Post-Warshak, a warrant for content has become the status quo. Nonetheless, it is critical for the Committee to approve S. 356 in order to cure a constitutional defect in ECPA, protect individual privacy, and assure that new technologies continue to enjoy robust constitutional protections.

Thank you.

[The prepared statement of Mr. Calabrese follows:]

Chairman Grassley. Ms. Espinel.

STATEMENT OF VICTORIA ESPINEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BSA | THE SOFTWARE ALLIANCE, WASHINGTON, D.C.

Ms. Espinel. Thank you. Good morning, Chairman Grassley and members of the Committee. I want to thank the Chairman and Ranking Member Leahy for having the hearing on this important issue. My name is Victoria Espinel. I appreciate the opportunity to testify today on behalf of BSA | The Software Alliance. BSA is the leading advocate for the software industry in the United States and around the world.

BSA members have a keen interest in today's data privacy area. We support efforts to update ECPA, and we commend Senators Lee and Leahy for their leadership. We urge this Committee to advance legislation that would better protect privacy in the 21st century.

We have long worked with CDT, Google, and the many other members of the Digital Due Process Coalition in support of this reform. Furthermore, our board of directors sent a letter to congressional leadership this week highlighting a series of legislative efforts needed to address data policy issues, and at the top of that list is ECPA reform.

When ECPA was enacted in 1986, most people had no conception of the Internet or email. Congress, though, had

the foresight to create a framework for giving law enforcement access to data while protecting privacy. For reasons that made sense in 1986 but do not today, the law makes it easier for law enforcement to obtain access to your old emails than it is to obtain a letter in your desk. ECPA reform would close that loophole.

ECPA reform is important to us because customer trust is important to us. Ensuring that customers have faith in the security and privacy of their email and other online data is vital to ensuring their trust in digital services. Simply put, if consumers do not trust technology, they will not use it.

BSA supports the bipartisan ECPA Amendments Act because it will aid in restoring the balance and this trust equation. And to quote Ranking Member Leahy from earlier this morning, we believe "this is a no-brainer."

Today, in addition to the inconsistent work requirements of ECPA, the law also is unclear on how to govern data requests that cross international borders. The lack of clear rules creates unhelpful confusion and has opened the door to U.S. law enforcement demands that could undermine user trust around the world. A case argued last week in the Second Circuit Court of Appeals could set a significant and damaging precedent. In that case, the Department of Justice is seeking to compel Microsoft to turn

over the contents of one customer's inbox. The problem in the case is this: that the customers emails are stored in Ireland. In the same way that U.S. police cannot simply fly to Ireland and knock down a suspect's door to raid their home, law enforcement's jurisdiction online must be respectful of borders as well. Barging into an Irish data center, however it is done, would be an obvious invasion of Irish sovereignty, and imagine the uproar if foreign police tried such a move in the United States.

Law enforcement agencies from different countries must and do work together to provide mutual assistance. The bipartisan LEADS Act, led by Senators Hatch, Coons, and Heller, with 12 bipartisan cosponsors, provides a way of addressing this issue, and we commend them for their attention to these important questions.

In sum, BSA supports the ECPA Amendments Act and the LEADS Act because we believe it is critical to modernize U.S. privacy protections in order to address three important goals:

First, protecting global privacy by setting strong, consistent standards. We should require a warrant for all digital content, and we need to create a framework for international cross-board requests. We will be in a better position to protect the privacy of American citizens if we are not setting an example for foreign governments to reach

back into the United States.

Second, increasing transparency and predictability--for consumers, for companies, and for law enforcement. We should help bolster consumer trust by enabling companies to clearly communicate the rules around the privacy and the security of their data.

And, third, enhancing the ability of law enforcement to work together across international borders. We need a new forward-looking framework to address these cross-border requests, and we need to improve the MLAT system.

There is a misperception that U.S. law enforcement has unfettered access to data stored by U.S. companies. It is only a misperception, but that misperception is doing real harm to user trust. The effort to fix that should begin here with the legislation pending before this Committee.

And if I may, I would like to close by wishing an early happy birthday to the Chairman as well.

Thank you very much, and I look forward to your questions.

[The prepared statement of Ms. Espinel follows:]

Chairman Grassley. Thank you very much.

I am going to ask my questions last because I want to accommodate Senator Sessions. Then after that, it would be Whitehouse and then Hatch and then the Senator from Minnesota.

Senator Klobuchar. I think I will put mine in the record, Mr. Chairman, but thank you.

Chairman Grassley. Okay.

[The prepared statement of Senator Klobuchar follows:]

Chairman Grassley. Go ahead, Senator Sessions.

Senator Sessions. Thank you very much, Mr. Chairman. I do have a commitment at lunch.

You introduced the Federal Law Enforcement Officers Association letter, which notes that law enforcement relies on electronic information "to generate leads, identify suspects, exonerate the innocent, obtain justice for the victims of crime who often suffer violations of their civil rights and privacy by individuals and terrorists." So I would offer that and note that many others are sharing the same comments, including the FBI Agents Association, Fraternal Order of Police, the National Sheriffs Association, the National District Attorneys Association, and the Major Cities Chiefs Association, to name a few.

Well, I do believe that if you obtain a subpoena to an individual file in a bank and there is a letter in that file from the customer, then you can obtain that, I believe, under current law based on a subpoena, and that has been part of the history of the country.

However, I will acknowledge that the ability to obtain all e-mail traffic goes to another level, and so I think it is right for us to consider how to restrict that and to be consistent with the Supreme Court and the reality that people are entitled to a degree of privacy, an expectation of privacy in the contents of those e-mails. So I do not

know that that is required by the Constitution. Maybe the Supreme Court says it is. But as a practical matter, I can understand that, and I think we can work with that.

Mr. Littlehale, you are on this panel I believe the only law enforcement strong advocate, but let me ask you: Is there a problem, a realistic problem, briefly, with computer companies and so forth delaying answers to legitimate requests from law enforcement? And does that at times place people at risk?

Mr. Littlehale. Thank you for the question, Senator. Yes, indeed. An example that Mr. Salgado offered was the Riley decision requiring a search warrant for a cell phone. But if I get a search warrant for a cell phone, I determine how quickly I execute it. Once I have the warrant, under the Riley decision, I can execute the search right away.

In the instance of a search warrant for a service provider, we are dependent on the service provider to process that warrant as they see fit under existing law, and we suggest that that should change.

Senator Sessions. And as in practical experience, you have had what you consider--law enforcement, what they consider inordinate delay in responses on occasions?

Mr. Littlehale. That is the sense of us that do this every day for a living, Senator, yes.

Senator Sessions. And you have worked with child

exploitation experiences and the need oftentimes for the most swift response.

Are you concerned that we may be moving into a world where everything is erased very quickly from the time it is happening? And what impact would that have?

Mr. Littlehale. The concern that even when we get the process that is required the records are no longer there is a concern, partially just because of the limits of the technology and the absence of requirements that govern how long those records live on those servers. They may disappear. And there is also in some instances now a commercial incentive for providers of service to remove those records in a timely fashion to assure their customers that the records are private.

Senator Sessions. And so the legislation as written has nothing on either one of those two issues to improve them?

Mr. Littlehale. That is correct, Senator. It does not.

Senator Sessions. And, briefly, are you concerned about the ramifications of customer notification and the dangers and problems that could pose for law enforcement?

Mr. Littlehale. We are indeed, Senator, both because of the dangers that it may pose to our investigation and also because of the administrative burden that a scheme

whereby we must go every 90 or 180 days and obtain delay and notification order after delay and notification order in a world where a unit like mine has tens or hundreds of legal demands outstanding at any given time.

Senator Sessions. Cases, and some of them are life-and-death investigations. Well, I thank you for that.

And, finally, to what extent does this preempt State law? And are we dealing with just with Federal law enforcement or are we impacting every police officer, sheriff, and prosecutor in America?

Mr. Littlehale. You are indeed. Federal law will set a bar. Certainly, States are free to offer more protection, but we must conform with Federal law where it supersedes State law.

Senator Sessions. Well, thank you all. This is an important issue. We need to wrestle through it and try not to do any damage, because people should not treat lightly the difficulties of investigating criminal activity and how you prove a case, and the idea that you can just get it by more police officer shoe leather has always been false, and some of this information so gathered could be critical in saving lives and stopping crime.

Thank you, Mr. Chairman.

Chairman Grassley. Senator Whitehouse and then Senator Hatch.

Senator Whitehouse. Thank you, Chairman.

Ms. Espinel, you have done a terrific job for the administration. You have always been a great witness before this Committee. Why a warrant requirement and not a court order requirement when a warrant is a court order, and it is actually a court order of a particularly pro-government kind because it is ex parte and has quite a low standard, relevancy standard likely to lead to the production of information?

Ms. Espinel. So just to be clear, I assume your question is not about 180-day distinction, but in terms of--

Senator Whitehouse. No. It is a question about getting access. Wouldn't the companies you represent, if they are willing to comply with a warrant, why would they not be willing to comply with a court order?

Ms. Espinel. So I would not want to imply that our companies are not willing to comply with any type of appropriate legal--

Senator Whitehouse. Well, from a legislative point of view, they are opposed to being asked to comply with a court order.

Ms. Espinel. But I think in this case, I think we believe that the civil agencies have other tools at their disposal, and we do not believe it is appropriate to extend either an expectation to the warrant, as you know, or this

type of court order to them.

Senator Whitehouse. You realize that that puts you in the position of saying that if the Department of Justice goes before a judge and in a very pro-government ex parte proceeding gets a warrant, you are okay with that. If the same DOJ goes before the same judge and in a contested proceeding where the subscriber actually has the right to be present and litigate the matter and then they obtain a court order, you are opposed to that. That is the position you are left with, are you not?

Ms. Espinel. I think our position is that the civil agencies have the tools that they have. We very much appreciate the job that they do every day, so I should be clear about saying that. But we do not believe--

Senator Whitehouse. Except that it makes civil frauds and civil racketeering and things like that potentially uninvestigable if the target has done a good enough job of hiding his other traces.

Ms. Espinel. I think if we believe that to be the case, we would not take the position that we have. Our belief is that the civil agencies with the tools that they have can investigate, and it is our belief that the type of court order--

Senator Whitehouse. So you have to be arguing then, in order for that to be the case, you would have to be arguing

that there is no case in which access to information by direct request to the service provider contributed in a material way to an investigation.

Ms. Espinel. I think it is difficult to be categorical in a hypothetical situation, so I would not want to say that. But I will say I think we think on balance, balancing the needs of law enforcement with privacy here, we believe that the best outcome to this is that the civil agencies work with the tools they have rather than extending this new power to them.

Senator Whitehouse. But you do agree and accept that a contested court proceeding in open court with the target of the investigation present is a more rigorous judicial safeguard than a warrant application rendered ex parte. You have got to agree with that.

Ms. Espinel. I would agree that it has different types of protection than a warrant does. I do not necessarily say that I would agree that it is a more rigorous standard.

Senator Whitehouse. Really? That would be a novelty. Okay.

Ms. Espinel. But I believe--I would agree with you that there are different implications for privacy involved in the different kind of court order.

Senator Whitehouse. Mr. Salgado, who has a reasonable expectation of privacy against court-ordered disclosure of

information?

Mr. Salgado. Well, we think that the user certainly, when issued a court order, is going to have the obligation to enter the account, pull the data out, and produce it. In that context, the user's expectation of privacy has been satisfied, can control the entry--

Senator Whitehouse. You do not think anybody has a reasonable expectation of privacy in this country against a court order divulging information. Nobody thinks that they have a right to ignore court orders, do they, in terms of the reasonable expectation of privacy?

Mr. Salgado. Make sure we are talking about who has got the right here. If the court order is issued to the user compelling the user to take action, and the user has an opportunity, notice and opportunity, that is classic rule of law, good process, and put--

Senator Whitehouse. So you think the reasonable expectation of privacy on the part of a person with respect to their own information depends on where the request for the information is made?

Mr. Salgado. I think in part it does. Where you have got--

Senator Whitehouse. That is an interesting and novel view of reasonable expectation of privacy.

Mr. Salgado. I am not sure it is. You can think about

the SEC's proposal here in a slightly different way in the physical world and see how it works out. If you had a situation where a user had records secreted in their home and was refusing to comply with a court order, but it was clear they had these documents or there was at least some reasonable suspicion, whatever the standard would be for this civil order, what the SEC would have us do is issue an order to allow the SEC to enter the home to go get the records. And, in fact, it is slightly different than that. The order would be issued not to the SEC to go into the home but perhaps a landlord or somebody else who could go into this protected area and go get the records and produce it to the SEC. I do not think we would stand for this in the physical world. We would say to the user or, in this case, the homeowner, "You have the obligation to comply with this order. Your failure to comply with this order will meet all sorts of enforcement sanctions"--some of which the FTC and SEC witnesses described. That is it. At no point are you going to have an IRS agent go into--

Senator Whitehouse. So just to follow your hypothetical through, you would be comfortable with a court order in which the owner of the information was present in the courtroom and the court directed that owner of the information to require you as the custodian of the information to provide it to law enforcement. You just have

to take that bank shot off the individual in order to solve the problem that you just described.

Mr. Salgado. It is not. Remember, we are talking about a protected area. The protected area, either the home or the account, should be entered only in the civil contest for civil infractions by the user. The court ought to order the user to enter the protected area--

Senator Whitehouse. That is what I said.

Mr. Salgado. --but not order the provider to do it on behalf of the agent, if that is what--

Senator Whitehouse. But they could order the user--so you would be comfortable with a court order as long as it directed the user to release the information maintained by your company--

Mr. Salgado. That is right, the user could--

Senator Whitehouse. --to law enforcement.

Mr. Salgado. That is right.

Senator Whitehouse. And as long as you have got the user right there in the courtroom, they could be subject to such an order.

Mr. Salgado. That is right. And the user--

Senator Whitehouse. Okay.

Mr. Salgado. And this is actually what is done now.

Senator Whitehouse. My time is long since over, and I have other Senators waiting, so my apologies for going over

my time, Mr. Chairman.

Chairman Grassley. I thought you asked good questions. Thank you.

Senator Hatch?

Senator Hatch. Thank you, Mr. Chairman.

Ms. Espinel, currently the U.S. Government takes the position that it can compel a technology company to turn over data located anywhere--anywhere in the world--belonging to a citizen of any country so long as the data can be accessed in the United States. Now, how has our Government's position affected the global competitiveness of the companies you represent? Are they losing business? And if so, how?

Ms. Espinel. Thank you. First, I will start off by saying that I am proud to say the U.S. leads in technology. That has been the case, and I believe it will continue to be the case, and that is the case in part because of policies and laws that our Congress has put in place.

But we do have concerns that the situation that exists right now is undermining customer trust around the world, and our ability to compete is undermined if customers around the world do not trust U.S. technology providers. So we do have real concerns that this case is going on and that the outcome of the case will risk customer trust and that that will have a negative impact on the ability of our companies

to compete overseas.

I will say I think the worst-case scenario for this is if we end up in a position where foreign governments are actually prohibiting companies--either their government agencies or their companies to use U.S. technology because of these concerns.

Senator Hatch. Do you agree that the Government's position on the extraterritorial reach of the U.S. warrants puts our privacy at greater risk of intrusion by foreign governments?

Ms. Espinel. Yes, we believe that there is a serious risk that this will create an example that other governments will use to reach back into the United States. And, in fact, in my testimony I refer to a case that was argued last week in the Second Circuit. This issue came up and played out in the arguments in that case. In that case, the Department of Justice took the position that the disclosure--that ECPA does not regulate the disclosure of contents of email as long as that disclosure takes place overseas. If you take that argument to its logical conclusion--and the Department of Justice acknowledged that this is the case--that means that U.S. law would not be able to stop any foreign government from reaching back into the United States and accessing or demanding the data or emails of anyone sitting in this room. We have real concerns about that. We

think that is an issue that should be addressed. We need to have some sort of framework to address that, and it needs to be a framework that is easy for companies, customers, and law enforcement to understand. It needs to be clear and transparent. We believe that Congress has a role to play there, that this is an issue that can be addressed. And we support the LEADS Act as a way to try to address that concern.

Senator Hatch. Some have questioned whether the LEADS Act would promote data localization. Do you agree?

Ms. Espinel. So I should say that we, BSA | The Software Alliance, we are categorically opposed to data localization. We have been opposing governments--or discouraging governments from putting those policies in place around the world. So we would not support this legislation if we believed that it would lead to data localization.

Data localization happens for lots of reasons, many of which are straight up protectionist. It is foreign governments trying to keep U.S. technology companies out of the market. But we do not believe that the outcome of this bill would be to lead to greater data localization.

What we do think is a much greater risk is that failing to address this issue, failing to set up a clear framework for how to deal with these international cross-border

request will lead to a situation where U.S. companies are being locked out of markets or lead to a situation where other governments are seeing what is happening in the U.S. and using that as a road map to reach back into the United States to get the data of our citizens. We think that is a much greater risk.

Senator Hatch. I agree with you.

Mr. Salgado and Mr. Calabrese, do you agree that there is a need for legislation that creates a legal framework for how and when law enforcement can access data stored abroad?

Mr. Salgado. I can speak for Google on this. We think that there is a need for legislation that addresses the access by U.S. law enforcement of users who are not in the United States, who are not U.S. citizens. The focus on where the data is stored does not make sense to us. We think it would lead to some bad results. But putting aside that one feature of the LEADS Act, we think there are ways to structure this that do not take into account and are not so wed to data localization as the feature that would still satisfy the spirit and aims of the proposal.

Senator Hatch. Do you agree with that, Mr. Calabrese?

Mr. Calabrese. Well, first, I appreciate your support for the Lee-Leahy bill as underlying and being added to by your LEADS Act.

Certainly this is a complicated area. CDT believes

that you have started an incredibly important conversation. You have created some tools in terms of MLAT reform that would be invaluable in speeding law enforcement investigations. And we believe that we can find an answer that gives everyone appropriate access to information overseas, and we worry about allowing the Chinas and the Russias of the world to have access to the information held by U.S. companies, and we appreciate your efforts to avoid that.

Senator Hatch. Well, thank you.

Mr. Chairman, could I ask one more question?

Chairman Grassley. Yes, go ahead.

Senator Hatch. I do not mean to hold you up.

To the both of you again, the Mutual Legal Assistance Treaty, or MLAT, process facilitates formal agreements for sharing evidence between the United States and foreign countries. Unfortunately, the process has proven slow and cumbersome to use.

Now, how important is it that Congress improve the MLAT process to make it more transparent and streamlined, if you will?

Mr. Salgado. Thank you, Senator, for that. Yes, I think MLAT has proven to be a very valuable mechanism. It is critical for keeping good rule of law and a sanity on international cooperation around data collection. It has

also proven to be very slow, and it is hindering legitimate investigations overseas. It has caused non-U.S. governments to take aggressive legislative action because they do not have good mechanisms to be able to get information they need from U.S. companies, data that is stored in the United States or held by U.S. people in an effective way. So I certainly agree with you that we have got to find a way to improve the cross-border exchange of evidence. It is going to be good for users. It will be good for the Internet. It will be good for rule of law.

The actual steps that we need to take, I think there are some things we can do around the Mutual Legal Assistance Treaty process itself to streamline it. Some of them are rather obvious things to do--to do more training on how to use the treaty process outside of the United States. Certainly the funding being provided to the Office of International Affairs in the Department of Justice is going to go a long way. The Bureau is setting up an MLAT unit. So there are many very practical steps that can be taken to help improve the treaty process.

We also think it might be time to take a look at alternatives to the treaty process, situations where it may not be necessary for the U.S. to exert quite so much control over data disclosure in situations where it may not actually have equities in the behavior of a U.S. company around a

disclosure. Lots of discussion to be had there. But we appreciate the leadership, sir, on your part in trying to find ways to make this quicker.

Senator Hatch. Thank you.

Chairman Grassley. Senator Coons.

Senator Coons. Thank you, Senator Grassley, and thank you for this hearing, and to Senator Hatch for your questions as well, and to the panel and the first panel.

Mr. Salgado, if I might start, we have heard some discussion about the Warshak case in 2010. It essentially vindicated your position that the Digital Due Process Coalition also shares that warrants are required whenever law enforcement seeks subscriber content under ECPA. And while that decision is binding law technically only in the Sixth Circuit, DOJ and Federal agencies have testified that they are following it nationwide.

So could you just for my benefit speak to why is statutory reform still necessary?

Mr. Salgado. Well, it is true that the law right now, the constitutional law and the way we are behaving I think does reflect that a warrant is required by the agencies, be they civil agencies or criminal agencies, in order to get the content of communications. We think that is right. But what we have on our books right now is an unconstitutional provision, and we can fix that. And we have got a very

elegant way in the current bill that takes care of this quickly, easily, does not actually change the way that agencies are going to be responding and the way they have been for the last 5 years.

We certainly appreciate the concerns that have been raised in the rather long debate over this provision, but I am afraid these may really just be some distractions around what this Committee can do, and can do the right thing and pass this bill without further delay to deal with some of these other issues that are worthy of discussion, need not hold up a change that everybody agrees is needed.

Senator Coons. Thank you. Thank you for that answer.

Mr. Calabrese, what should Congress be aware of when it considers the international application of ECPA warrants in terms of privacy, human rights, reciprocity, or any other relevant concerns you would have us--hold right in front of us when we move forward?

Mr. Calabrese. Senator, I am going to apologize up front. There is something that has been discussed a great deal but I feel like it needs to be corrected on the record. I promise to answer your question, but if I can have 30 seconds to just--what has been said here, we have conflated two really important and very different things in this Committee today. One is some kind of court order based on a subpoena, and one is a probable cause warrant. These are

not the same thing.

A subpoena gives you access to all information that is relevant, as pursuant relevant to a civil investigation, a civil infraction. So, you know, if you make a mistake on your taxes, that is a potential civil infraction. Nothing that has been put forward by the SEC would do anything but be a dramatic expansion of their authority to get at ordinary people's inboxes--not just the subjects of investigation, but ordinary folks who may be witnesses. Those people would have their--everything in their inbox that was relevant to an investigation, so a dramatic amount of information as opposed to probable cause of evidence of a crime. That is a really troubling privacy invasion, and it is one that has nothing to do with the underlying bill.

So I apologize for hijacking your question. I just felt like it was really important for this Committee to understand that we would be talking about a huge power grab by civil agencies, no matter how they frame it.

It is incredibly important that we update the MLAT process and update ECPA because we have the strongest, I believe--and I will be paternalistic here. We have the strongest privacy protections in the world with a warrant based on probable cause by a neutral magistrate. Right now we are seeing companies come to our--excuse me, other countries come to us and essentially meet that standard. It

is really important that we keep that and that they continue to meet that standard. And one of the best ways we can do that is by having a quick, streamlined MLAT process so they can give us the information we need and we can have everybody around the world perhaps bring their standard up to that important probable cause standard.

Senator Coons. Thank you.

Ms. Espinel, it is terrific to see you again. I am glad you were able to testify today. I greatly enjoyed working with you when you were leading IPEC and now in your current role at BSA, and I am grateful for your long and effective leadership on intellectual property issues and now on the difficult issues in front of us.

I have worked with Senator Hatch and 11 other bipartisan cosponsors to introduce the LEADS Act which clarifies that ECPA warrants, like other warrants, cannot be used to compel searches abroad. And I think this common-sense rule, were we to advance it, would enhance trust and transparency and our competitiveness. But some in law enforcement have argued that an extraterritorial ECPA is needed because other investigative processes like the MLAT are too slow.

Can you speak to that concern and how your members strive to be good partners to law enforcement, often without the need to obtain a warrant or to go through the MLAT

process?

Ms. Espinel. Yes, I would be happy to, and thank you for your leadership on the LEADS Act.

So, first, I want to be clear that we do not want to make the job of law enforcement any harder. We very much support what law enforcement does and the critical mission that they have, and our companies work every day both in what they do themselves and with law enforcement to help support that mission.

We have talked a lot about MLATs today. We also very much support MLAT reform, and I would be happy to elaborate on the reasons why we do and the things that we think could be done to help improve the MLAT system. But you raise an important point, that MLATs are not the only way that U.S. law enforcement can work with foreign law enforcement.

So to give a practical example of that, on January 7th of this year, the horrific attacks on the Charlie Hebdo office took place in Paris, and in that case U.S. law enforcement, working with French law enforcement, went to one of the companies I represent--they went to Microsoft--and they asked for email information relevant to the manhunt that was taking place in Paris at that time. It was the middle of the night on the west coast, and notwithstanding that, within 45 minutes the emails relevant to the investigation were in the hands of French law enforcement.

I raise this as an example of the fact that MLATs are an important tool. They are a tool that we think should be improved, but they are not the only tool that law enforcement has to work with foreign law enforcement. We believe that it is important both for us to improve the MLAT system, but for us to be looking for as many ways as possible to try to enhance the cooperation between U.S. law enforcement and foreign law enforcement.

Senator Coons. Well, thank you, Ms. Espinel. Thank you to the entire panel, and thank you, Mr. Chairman, for convening this important hearing today.

Chairman Grassley. Mr. Salgado, advocates for ECPA seek word for content rule, but as you know, earlier this summer our Judiciary Committee held a hearing on the "Going Dark" issue where we heard from the FBI Director and others that some of the technology companies are employing sophisticated encryption technology that makes them unable to turn over customer content information, including emails and text messages. In effect, this technology made court-authorized warrants not worth the paper that they are printed on.

Now, I know that Google is one of the leading technology companies in the world. Does Google employ this kind of encryption technology that effectively prevents it from responding to court-authorized wiretaps or search

warrants for the content of emails or text messages or photographs? And if not, do you believe your systems are fundamentally insecure or fatally flawed?

Mr. Salgado. We do not--thank you, Mr. Chairman. We are working towards more encryption on our products and our services as part of a larger plan to make sure the data services we provide to our users are secure and that users can use our services knowing that the information that they entrust to us is safe. This is an effort we have been taking on over many years, and as the technology improves and processing power increases, it is our intention to continue improving the security of our systems in many different ways. Encryption is just one technique to make sure that the data that is stored with us is in a secured state.

There are lots of different ways to secure data besides encryption, but I think there is pretty much a consensus in the security community that encryption is a fundamental and critical way to protect users' data from the very thieves--identity theft cases, privacy intrusions that law enforcement is interested in investigating. The encryption actually prevents those crimes from happening in the first instance, and we think as a net result it is a positive thing to implement encryption where the products make sense to include encryption.

Chairman Grassley. Agent Littlehale, as you know, when the police search a home or a business, officers will provide a copy of a warrant authorizing the search. This might reveal the basic type of investigations, whether it involves terrorism or drugs or Medicare fraud. But the police do not have to say anything more. I am told law enforcement has serious concerns about a provision in the Lee-Leahy bill that changes the notice provisions to require law enforcement to go beyond that, potentially divulging specific investigative detail to a target. Do you share these concerns about this bill's notice provisions? Why or why not?

Mr. Littlehale. We do, Mr. Chairman, because we are both concerned that providing greater protection for evidence because it is in digital form is, in fact, not bringing digital evidence in line with evidence in the physical world, and also because when a search warrant is executed in the physical world, we control the access to that warrant. And so notification provisions are one concern.

The other concern is that we need to gather access to that evidence in a manner that approximates the time that we would if they were in the physical world.

Chairman Grassley. Also for you--and this will be my last question--this country is facing a crisis involving

undocumented workers. I am deeply concerned that the LEADS Act puts a real burden on law enforcement's ability to investigate crimes committed by undocumented workers. As you know, this bill would limit the enforcement of U.S. warrants obtained to obtain the information of U.S. persons unless the information is stored in the United States, so it could act as a get-out-of-jail-free card for some undocumented immigrants.

Do you share my concerns about this aspect of the LEADS Act? Should we prevent our local police from searching emails of undocumented workers with a U.S. search warrant if an email provider happens to store those emails in another country?

Mr. Littlehale. I certainly share your concern, Mr. Chairman, that if we are to depend on the MLAT process, it is going to take a lot of streamlining. Just to offer an example of the realities of a practitioner's perspective in the golden age of surveillance, there was a case in Texas where they were investigating a homicide, and they sought records from a Canadian app provider, and just last year it took about 9 months for those records to be returned through the MLAT process in a friendly neighbor country. So, yes, we have deep concerns about that, Mr. Chairman.

Chairman Grassley. The record will remain open for one week for questions and other submissions. Thank you all

very much. Thank you.

[Whereupon, at 12:36 p.m., the Committee was adjourned.]

C O N T E N T S