

**REFORMING THE ELECTRONIC
COMMUNICATIONS PRIVACY ACT**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED FOURTEENTH CONGRESS
FIRST SESSION

SEPTEMBER 16, 2015

Serial No. J-114-29

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

| | |
|---|--|
| ORRIN G. HATCH, Utah | PATRICK J. LEAHY, Vermont, <i>Ranking Member</i> |
| JEFF SESSIONS, Alabama | DIANNE FEINSTEIN, California |
| LINDSEY O. GRAHAM, South Carolina | CHARLES E. SCHUMER, New York |
| JOHN CORNYN, Texas | RICHARD J. DURBIN, Illinois |
| MICHAEL S. LEE, Utah | SHELDON WHITEHOUSE, Rhode Island |
| TED CRUZ, Texas | AMY KLOBUCHAR, Minnesota |
| JEFF FLAKE, Arizona | AL FRANKEN, Minnesota |
| DAVID VITTER, Louisiana | CHRISTOPHER A. COONS, Delaware |
| DAVID PERDUE, Georgia | RICHARD BLUMENTHAL, Connecticut |
| THOM TILLIS, North Carolina | |
| KOLAN L. DAVIS, <i>Republican Chief Counsel and Staff Director</i> | |
| KRISTINE LUCIUS, <i>Democratic Chief Counsel and Staff Director</i> | |

CONTENTS

OPENING STATEMENTS

| | Page |
|--------------------------------|------|
| Grassley, Hon. Charles E. | 1 |
| Prepared statement | 114 |
| Leahy, Hon. Patrick J. | 3 |
| Prepared statement | 116 |

WITNESSES

| | |
|---|-----|
| Calabrese, Chris | 30 |
| Prepared statement | 93 |
| Responses to written questions | 120 |
| Ceresney, Andrew | 6 |
| Prepared statement | 55 |
| Responses to written questions | 125 |
| Espinel, Victoria | 31 |
| Prepared statement | 106 |
| Responses to written questions | 141 |
| Littlehale, Richard | 26 |
| Prepared statement | 75 |
| Responses to written questions | 142 |
| Salgado, Richard | 28 |
| Prepared statement | 82 |
| Responses to written questions | 151 |
| Salsburg, Daniel | 8 |
| Prepared statement | 64 |
| Responses to written questions | 161 |
| Tyrangiel, Elana | 5 |
| Prepared statement | 46 |
| Questions submitted with no response returned | 117 |

APPENDIX

| | |
|--------------------------------------|----|
| Items submitted for the record | 45 |
|--------------------------------------|----|

REFORMING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

WEDNESDAY, SEPTEMBER 16, 2015

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

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

Present: Senators Grassley [presiding], 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 4½ 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. 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. 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.

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. 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. 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, quote "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, soci-

ety'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, quote, "meaningful ECPA reform must carefully balance privacy rights, public safety, and security", end of quote. 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. 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.

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

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.

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.

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. If I sent him a note, which I have actually written to him, 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?

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 Co-Sponsors in the Senate, 9 of them on this Committee. In the House, even more, 300 Co-Sponsors 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. Usually representatives of those people have to have an arbitrator get on an elevator with them if they are all in there together. 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. 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 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. I would ask, without objection, that these and additional letters be entered into the record.

[The information appears as a submission for the record.]

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 Council. Prior to joining Justice, she worked in the Office of White House Counsel and served as assistant U.S. attorney in DC. 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, he 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 criminal 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, DC**

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. 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. 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 appears as a submission for the record.]

Chairman GRASSLEY. Thank you. Andrew.

**STATEMENT OF ANDREW CERESNEY, DIRECTOR,
DIVISION OF ENFORCEMENT, U.S. SECURITIES
EXCHANGE COMMISSION, WASHINGTON, DC**

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. 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. 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 noncooperative 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. 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 appears as a submission for the record.]

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, DC**

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 protect 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 has

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. 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 law enforcement 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 appears as a submission for the record.]

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. We have been told that the SEC has not provided any examples of cases where access to electronic communications has been cutoff 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, quote, "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. 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 quote, "ECPA so that agencies can ultimately bypass the target of or even potential witnesses in civil investigations", end of quote.

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. 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. 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. 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 information appears as a submission for the record.]

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. 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. 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. 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. 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 2½ years I have been Director of Enforcement. We have had discussions with the staff throughout that period of time.

Senator LEAHY. 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. 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. 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. Thank you.

Senator LEAHY. Thank you, Mr. Chairman.

Chairman GRASSLEY. Thank you, Senator Leahy.

Senator Hatch. Let me read here it will be Hatch, Whitehouse, Lee, who were here at the fall of the gavel. 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, am I pronouncing your name right?

Ms. TYRANGIEL. Yes.

Senator HATCH. 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. 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. 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. 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. 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, quote, “should be of some concern,” unquote.

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. 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. 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. 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. 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. 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. 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. 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. 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. Why are you talking about the—why did you use that example of the importance of it?

Mr. SALSBURG. 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. 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 [continuing]. 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. 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.

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

Chairman GRASSLEY. Thank you. 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. That I have been here for about 4½ years, I appreciate more fully how difficult it can be to bring about a change of law that basically everyone agrees on.

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.

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. I do think that while there are a few people in Washington, DC, 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.

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. 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. 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. What we are talking about on the civil side is a process protection.

Senator LEE. 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. 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. Senator Franken.

Senator FRANKEN. Since Senator Leahy asked me to be here as Ranking Member, I have to be here. 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. 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. 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. 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. SALSBERG. Right.

Senator BLUMENTHAL. Under which?

Mr. SALSBERG. Under the——

Senator BLUMENTHAL. 356?

Mr. SALSBERG. 356, yes.

Senator BLUMENTHAL. Okay. That is a suggestion that you have for improving it.

Mr. SALSBERG. Yes. 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. SALSBERG. 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. I welcome your suggestions for improving this legislation. As you know, I am one of the original Co-Sponsors 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. 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 noncitizen 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. It would—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. Our subpoenas are not self-executing, so, in other words, we need to—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. The caselaw essentially says that if we show a proper purpose and if the subpoena is properly tailored, it will be upheld. 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. 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. When you have to go to the second step of actually trying to get the information.

Mr. CERESNEY. Yes, 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. 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 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, 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. I applaud Senators Lee and Leahy for their efforts—I guess more Senator Leahy because he is my Ranking Member.

[Laughter.]

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. Then this morning we received Commissioner Brill's statement expressing her concern about this proposal. Commissioner Brill notes that it is quote, "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. 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.

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. 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.

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. 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 32d 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. In order to be able to get something, there needs to be a basis for jurisdiction. 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. SALSBERG. 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. 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. 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 that's—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. 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 in-

dividual has deleted the emails, we are able to obtain it. 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. 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. 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. I had ordered a publication not long ago, and within a few weeks, I get—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 is 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 protecting us from fraudsters and sex abuse and child kidnappers and terrorists. I just really think we have got to be careful about it. 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.

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. 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. 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.

What about getting an email address? It seems to me that is quite a lot—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? 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. 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. 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. 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. 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 nondisclosure 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. 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 has 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 investigator 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 two-fold 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. Nontechnical 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, governing law access to emergency records should be revised. Everyone agrees that law enforcement should have rapid access to communications evidence in a life-threatening emergency, 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 nontechnical 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 hears 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 appears as a submission for the record.]

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 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 Co-Sponsors. The House companion measure, the Email Privacy Act, now has 292 Co-Sponsors, 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 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 quote, "contravenes our general preference to provide clear guidance to law enforcement through categorical rules", end quote.

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", close quote.

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 appears as a submission for the record.]

Chairman GRASSLEY. Mr. Calabrese.

**STATEMENT OF CHRIS CALABRESE, VICE
PRESIDENT, POLICY CENTER FOR DEMOCRACY
& TECHNOLOGY, WASHINGTON, DC**

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, non-profit 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 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. 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. 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, 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 Co-Sponsors, 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 appears as a submission for the record.]

Chairman GRASSLEY. Ms. Espinel.

**STATEMENT OF VICTORIA ESPINEL, PRESIDENT
AND CHIEF EXECUTIVE OFFICER, BSA, THE
SOFTWARE ALLIANCE, WASHINGTON, DC**

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 customer’s 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 Co-Sponsors, 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.

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.

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 appears as a submission for the record.]

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.

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, quote, “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”, close quote. 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.

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 emails. I do not know that that is required by the Constitution. Maybe the Supreme Court says it is. 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? 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. 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. 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. 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? 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. 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. 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. 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. I thank you for that.

Finally, to what extent does this preempt State law? 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. 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. 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. I would not want to imply that our companies are not willing to comply with any type of appropriate legal—

Senator WHITEHOUSE. From a legislative point of view, they are opposed to being asked to comply with a court order.

Ms. ESPINEL. 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. 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. 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. 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. 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. 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. 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. 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. 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. 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 the 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 [continuing]. But not order the provider to do it on behalf of the agent, if that is what—

Senator WHITEHOUSE. 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 [continuing]. To law enforcement.

Mr. SALGADO. That is right.

Senator WHITEHOUSE. 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. 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. How has our Government's position affected the global competitiveness of the companies you represent? Are they losing business? 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.

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. 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. 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. 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. 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. 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. 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. 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. 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. 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. 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.

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. 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. 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. 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. While that decision is binding law technically only in the Sixth Circuit, DOJ and Federal agencies have testified that they are following it nationwide.

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

Mr. SALGADO. 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. What we have on our books right now is an unconstitutional provision, and we can fix that. 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. 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.

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. 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 Co-Sponsors to introduce the LEADS Act which clarifies that ECPA warrants, like other warrants, cannot be used to compel searches abroad. I think this commonsense rule, were we to advance it, would enhance trust and transparency and our competitiveness. 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.

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. You raise an important point, that MLATs are not the only way that U.S. law enforcement can work with foreign law enforcement.

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. 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.

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? 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 toward 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. 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 inves-

tigative 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. 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. 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. Do you know—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 1 week for questions and other submissions. Thank you all very much. Thank you.

[Whereupon, at 12:36 p.m., the hearing was adjourned.]
[Additional material submitted for the record follows.]

A P P E N D I X

Submitted by Chair Grassley:

| | |
|---|-----|
| Federal Bureau of Investigation | 167 |
| National Association of Assistant United States Attorneys | 171 |

Miscellaneous submissions:

| | |
|---|----|
| White, Mary Jo, statement | 61 |
| Federal Trade Commission, statement | 64 |
| Brill, Julie, statement | 73 |



Department of Justice

STATEMENT OF
ELANA TYRANGIEL
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

BEFORE THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"REFORMING THE ELECTRONIC
COMMUNICATIONS PRIVACY ACT"

PRESENTED
SEPTEMBER 16, 2015

**Statement of
Elana Tyrangiel
Principal Deputy Assistant Attorney General**

**Before the
Committee on the Judiciary
United States Senate**

**At a Hearing Entitled
“Reforming the Electronic Communications Privacy Act”**

September 16, 2015

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 (ECPA). This topic is particularly important to the Department because of the wide-ranging impact the statute has on public safety and both criminal and civil law enforcement operations. We are pleased to engage with the Committee in discussions about how ECPA is used and how it might be updated and improved.

ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, ECPA has been updated several times since, with significant revisions occurring in both 1994 and 2001.

I intend to focus the majority of my testimony on the SCA, which contains three primary components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications: anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates the government’s ability to compel disclosure of both stored content and non-content information from a service provider; it creates a set of rules that governmental entities generally must follow in order to compel disclosure of stored communications and other records.

Since its inception, the SCA has served multiple purposes. It provides rules governing how providers of communications services disclose stored information—including contents of communications, such as the body of an email, and non-content information—to a wide variety of government entities. In doing so, it imposes requirements on the government and providers to ensure that the privacy of individuals is protected. The statute thus seeks to ensure public safety

and other law enforcement imperatives, while at the same time ensuring individual privacy. It is important that efforts to amend the SCA remain focused on maintaining both of these goals.

I. The Stored Communications Act Plays an Important Role in Government Investigations

Any consideration of the SCA must begin with an understanding of the statute's extremely broad scope. The paradigm that generally comes to mind in discussions of the SCA is a law enforcement agency conducting a criminal investigation and seeking a target's email from a service provider that makes its services available to the public. And, indeed, the SCA is critical to all sorts of criminal investigations into murder, kidnapping, organized crime, sexual abuse or exploitation of children, financial fraud, and more. As technology has advanced, electronic communications and electronic data storage have augmented traditional means of communicating and storing information. Appropriate governmental access to electronic communications and stored data, including both content and non-content information, has thus become even more important to upholding our law enforcement and national security responsibilities.

Even within these criminal investigations, it is important to understand the kind of information that the government obtains under the SCA as well as how that information is used. Under the SCA, the government may use legal process to compel service providers to produce both content and non-content information related to electronic communications. It is clear that the contents of a communication—for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography—can be important evidence in a criminal case. But non-content information can also be essential to building a case.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Non-content information about a communication may include, for example, information about the identity of the parties to the communication, and the time and duration of the communication. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without a mechanism to obtain non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant.

For example, the SCA has been critical to tracking down violent criminals. In one case, law enforcement obtained graphic photographs of a man sexually abusing his prepubescent son. Because of the offender's careful protection of his true identity, including the use of an anonymous online network, investigators needed to engage in a number of steps to ascertain the offender's location. Using information obtained from undercover chat sessions, officers identified a "proxy computer" – an intermediate computer used to obscure the offender's communication. Law

enforcement obtained computer routing information from the proxy computer, and from that routing information, identified an IP address from which the offender's internet traffic appeared to originate. After taking additional steps to confirm that the IP address was associated with the unlawful conduct, pursuant to ECPA agents served a subpoena on the offender's Internet service provider to obtain his physical address, leading to the eventual arrest of three individuals involved in the offense and the rescue of a minor victim from extreme, ongoing abuse.

Similarly, agents used evidence gathered using a process under ECPA in the investigation of the Boston Marathon bombing. Subpoenas to phone companies provided subscriber information and call detail records, which were critical during the investigation to help identify the bombers and their associates, and some of which were used at trial to show the communications between the bombers at critical times.

The SCA has broad effect in other ways as well. The statute applies not only to public and widely accessible service providers but also to non-public providers, such as companies or governments that provide email to their employees. Moreover, federal criminal investigations are only a subset of the circumstances in which the SCA applies. The statute applies to the federal government in civil contexts as well as to state and local governments when they seek to obtain content or non-content information from a service provider. This means that the statute also applies when the government is acting as a civil regulator—or even as an ordinary civil litigant. For instance, the SCA applies in all of the following circumstances that could arise, just within the Department of Justice:

- Civil Rights Enforcement: DOJ's Civil Rights Division brings a civil suit against a landlord who is sending racially harassing text messages to tenants. The target of the messages deletes them, and the landlord denies ownership of the account from which they were sent. The SCA governs the Division's ability to obtain those messages from the provider during civil discovery.
- False Claims Act: The DOJ Civil Division investigates a business for submitting false claims to the Federal government. The Division has reason to believe that the defendant's employees used email messages sent via the business's customer service email accounts to orchestrate the fraud. However, the defendant claims that it did not use email for business purposes. The SCA governs the ability of the Division to compel the internet service provider that hosted the company's website to disclose the contents of the business's email account.
- Environmental Litigation: The Department's Environment and Natural Resources Division brings a civil enforcement suit under the Superfund statute, a company relevant to the litigation has gone bankrupt, and the company's cloud provider has the only copies of that company's relevant corporate email. The SCA governs the Division's ability to obtain that email during civil discovery.

- Antitrust Investigations: The Department's Antitrust Division is conducting a civil investigation of several companies for engaging in an unlawful agreement to restrain trade. During the course of the investigation, DOJ attorneys discover that executives of those companies are using their personal email accounts to continue communications about the agreement. The SCA governs the Division's ability to obtain that email from the service provider.
- Tax Enforcement: The DOJ Tax Division investigates a tax preparation service that advertises via social networking sites. The company fraudulently inflates the amount of refunds due to the taxpayer and profits from taking a significant share of the fraudulent refund. Based on complaints about the preparer, the social networking site closes the company's account. The SCA governs the Tax Division's ability to obtain the posts advertising the company's tax preparation services.

During any discussions of possible changes to the SCA and ECPA more broadly, it is important to keep in mind its wide-ranging application and scope.

II. Modernizing the Rules for Compelled Disclosure of Email and Other Similar Stored Content Information

As I mentioned, ECPA was originally enacted in 1986—a time when the internet was still a nascent technology and landline telephones predominated. Although ECPA has been updated several times since its enactment, the statute—and specifically the portion of the SCA addressing law enforcement's ability to use legal process to compel disclosure of the stored contents of communications from a service provider—has been criticized for making outdated distinctions and failing to keep up with changes in technology and the way people use it today.

Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.

Acknowledging that the so-called “180-day rule” and other distinctions in the SCA no longer make sense is an important first step. The harder question is how to update those outdated rules and the statute in light of new and changing technologies while maintaining protections for privacy and adequately providing for public safety and other law enforcement imperatives.

Personal privacy is critically important to all Americans—including those of us who serve in the government. It is also of increasing importance to individuals around the world, many of whom use communications services provided by U.S. companies. All of us use email and other

technologies to share personal and private information, and we want it to be protected appropriately. We also know that companies in the United States and elsewhere depend on privacy as a driver of innovation and competitiveness. Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.

In the past several years, we have worked to help facilitate a better understanding of how the warrant requirement affects the Department of Justice's ability to enforce the law. And the Department appreciates, for example, that most recent proposals (*i.e.*, the "ECPA Amendments Act" (S. 356)), would not impose a warrant requirement in investigations involving corporate email. This type of provision would help preserve the manner in which corporate investigations have historically been conducted. Corporations often act as "electronic communications service providers" under the SCA when they provide email and internet service to their employees. It would be anomalous, however, for the SCA to afford greater protection to electronic corporate records than to the identical records in hard copy, and such a rule could be abused by organizations and individuals seeking to avoid accountability for violating the law. Retaining the current use of subpoenas in that context therefore makes sense.

The Department remains concerned, however, about the effect a blanket warrant requirement would have on its civil operations. Civil regulators and litigators do extremely important work. But they typically are investigating conduct that, while unlawful, is not a crime. 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 communications content 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 off-limits to government regulators and litigators will only increase. It is also not the case that these civil regulators and litigators can ask criminal law enforcement officers to obtain a warrant on their behalf, because such warrants can only be obtained in furtherance of a criminal investigation—a step that would be impermissible unless the underlying conduct appeared to be criminal in nature.

Nor could civil litigators and regulators reliably obtain email and other content information solely by serving a subpoena directly on a subscriber (rather than a provider). As several of the examples described above demonstrate, serving a subpoena on a provider may be the only way for civil law enforcement to obtain certain stored communications. For example, where the subscriber no longer exists—as in the case of a bankrupt corporation or a deceased individual—or a purported subscriber denies ownership of the communications and therefore refuses to comply with a subpoena, civil litigators and investigators without the ability to obtain

relevant evidence from a provider would be unable to obtain that evidence. Moreover, many individuals who violate the law may be tempted to destroy their communications rather than turn them over. Having the ability to seek records only from the individual, rather than the provider, could serve to encourage such illegal obstruction of justice. Thus, it is important that any proposed changes to ECPA take into account the ability of civil regulators and litigators 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, including ensuring that the definition of “remote computing service” is appropriately scoped.

Finally, given the increasing prevalence of electronic communications, critical investigations involving widespread or complex crimes – such as those involving terrorism, transnational crime, financial fraud, or child exploitation – can last years and involve hundreds of search warrants, court orders, and subpoenas issued pursuant to ECPA to a variety of providers. ECPA reform proposals should account for investigations of this type and avoid enacting new obstacles to investigations that are already among the most challenging and important ones that law enforcement undertakes.

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.

III. The Need for Additional Updates to the SCA and ECPA

Although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are a number of other parts of the statute that merit further examination during any process of updating and clarifying the statute.

(A) Clarifying Exceptions to the Pen Register Statute

First, Congress could consider clarifying the exceptions to the Pen Register statute. The Pen Register statute governs the real-time collection of non-content “dialing, routing, addressing, or signaling information” associated with wire or electronic communications. This information includes phone numbers dialed as well as the “to” and “from” fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are actually less extensive than the exceptions to the Wiretap Act. This makes little sense—if the government is authorized to intercept communications in real-time, it is reasonable that the government should also be permitted to acquire the accompanying non-content information. Congress could harmonize the exceptions in these two sections of the statute by amending the Pen Register Act to bring it into line with the Wiretap Act. Moreover, the Pen Register Act’s consent provision may be read so that a user can only consent to the use of a pen/trap device by

the provider as opposed to by the government or the user herself. The Pen Register Act's consent provision could be clarified to allow the user to provide direct consent for implementation of a pen/trap device by the government.

(B) Clarifying the Standard for Issuing 2703(d) Orders

Second, Congress could consider clarifying the standard for the issuance of a court order under § 2703(d) of the SCA, which can be used by criminal law enforcement authorities to compel disclosure of various types of stored records. According to that provision of the statute, “[a] court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the [records] sought are relevant and material to an ongoing criminal investigation.”

The Fifth Circuit has interpreted this provision to require a court to issue a 2703(d) order when the government makes the “specific and articulable facts” showing specified by § 2703(d). *See In re Application of the United States*, 724 F.3d 600 (5th Cir. 2013). However, the Third Circuit has held that because the statute says that a § 2703(d) order “may” be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit’s approach makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not.

(C) Making the Standard for Non-content Records Technology-Neutral

Third, Congress could consider modernizing the SCA so that the government can use the same legal process to compel disclosure of addressing information associated with modern communications, such as email addresses, as the government already uses to compel disclosure of telephone addressing information. Historically, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA endorsed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Therefore, while law enforcement can obtain records of calls made to and from a particular phone using a subpoena, the same officer can only obtain “to” and “from” addressing information associated with email using a court order or a warrant, both of which are only available in criminal investigations. This results in a different level of protection for the same kind of information (*e.g.*, addressing information) depending on the particular technology (*e.g.*, telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal and national security investigations. Congress could consider updating the SCA to set the same

standard for addressing information related to newer technologies as that which applies in traditional telephony.

(D) Clarifying that Subscribers May Consent to Law Enforcement Access to Communications Content

Fourth, Congress could consider clarifying the consent provision of the SCA. Under section 2702, a provider *may* disclose the contents of communications with the consent of a user or customer, but the provider is not required to do so. This has the impact of allowing the provider to overrule its customer's direction to disclose content associated with the customer's account. Thus when the victim of a crime seeks to share his or her own emails or other messages that may provide evidence, providers can refuse to disclose that information to law enforcement, even when provided with a written release from the account owner or subscriber.

(E) Appellate Jurisdiction for Ex Parte Orders in Criminal Investigations

Fifth, Congress could consider clarifying that higher courts have appellate jurisdiction over denials of warrants or other ex parte court orders in criminal investigations. Under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact. Congress may wish to consider clarifying that these denials are appealable so that the disagreements among courts are resolved and the law becomes standardized.

IV. Obtaining Stored Information Abroad

Some discussion concerning ECPA has focused on changing the standards and protocols for law enforcement access to content that a provider has chosen for its own business reasons to store outside the United States. The Administration is studying these legislative proposals, but the Department has significant concerns about aspects of these proposals.

* * *

In conclusion, I would like to reemphasize that in discussing any efforts to modernize ECPA, it is important to take into account the statute's broad application. As technology continues to advance, ECPA's importance to both criminal and civil law enforcement will only increase.

The Department of Justice stands ready to work with the Committee as it considers potential changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

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

Testimony on Updating the Electronic Communications Privacy Act

by

**Andrew Ceresney
Director, Division of Enforcement**

U.S. Securities and Exchange Commission

**Before the
Committee on the Judiciary
United States Senate
September 16, 2015**

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

Thank you for inviting me to testify today on behalf of the Commission concerning the Electronic Communications Privacy Amendments Act (S. 356) pending before your Committee. The bill seeks to modernize portions of the Electronic Communications Privacy Act (ECPA), which became law in 1986. I share the goal of updating ECPA's evidence collection procedures and privacy protections to account for the digital age. But S. 356, 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. As described in more detail below, 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. The SEC's Division of Enforcement furthers this mission by, among other things, investigating potential violations of the federal securities laws, recommending that the Commission bring cases against alleged fraudsters and other securities law wrongdoers, and litigating the SEC's enforcement actions. A strong enforcement program is a critical piece of the Commission's efforts to protect investors from fraudulent schemes and

promotes investor trust and confidence in the integrity of the nation's securities markets. The Division is committed to the swift and vigorous pursuit of those who have broken the securities laws through the use of all lawful tools available to us.

Electronic communications often provide critical evidence in our investigations, as email and other message content (e.g., text and chat room messages) can establish timing, knowledge, or relationships in certain cases, or awareness that certain statements to investors were false or misleading. In fact, establishing fraudulent intent is one of the most challenging issues in our investigations, and emails and other electronic messages are often the only direct evidence of that state of mind. When we conduct an investigation, we generally will seek emails and other electronic communications from the key actors via an administrative subpoena – a statutorily authorized mechanism for gathering documents and other evidence in our investigations.¹ In certain instances, the person whose emails are sought will respond to our request. But in other instances, 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 to the government evidence of their own misconduct. In still other instances, email account holders cannot be subpoenaed because they are beyond our jurisdiction.

It is at this point in an investigation that we may in some instances, when other mechanisms for obtaining the evidence are unlikely to be successful, need to seek information from the internet service provider (ISP). S. 356 would require government entities to procure a criminal warrant when they seek the content of emails and 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 evidence, including communications such as

¹ See Section 21(b) of the Securities Exchange Act of 1934, Section 19(c) of the Securities Act, Section 209(b) of the Advisers Act, and Section 42(b) of the Investment Company Act.

emails, directly from an ISP, regardless of the circumstances.² Thus, if the bill becomes law without modifications, the SEC and other civil law enforcement agencies would be denied the ability to obtain critical evidence, including potentially inculpatory electronic communications from ISPs, even in instances where a subscriber deleted his emails, related hardware was lost or damaged, or the subscriber fled to another jurisdiction.³ 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 thus feel free to destroy or not produce them.

These are not abstract concerns for the SEC or for the investors we are charged with protecting. An effective enforcement program protects investors and the integrity of the capital markets by deterring securities law violations, punishing violators, returning money to injured investors, and preventing fraud. Among the types of scams we investigate where the ability to obtain content from ISPs would be most helpful include schemes – often perpetrated by individuals or small groups of actors – that target or victimize the elderly or other retail investors, including Ponzi schemes and “pump and dump” market manipulation schemes,⁴ as

² Our cases are often the sole actions against wrongdoers: while we often conduct investigations in parallel with criminal authorities, the vast majority of our investigations do not have any criminal involvement. For example, although the criminal authorities have brought a significant number of insider trading cases in recent years, we have charged than more than 650 defendants with insider trading violations in the last 6 years, most of whom were not charged criminally.

³ Chair White first raised these concerns in an April 2013 letter to Senator Leahy. A copy of that letter is attached.

⁴ “Pump-and-dump” schemes involve the touting of a company’s stock (typically microcap companies) through false and misleading statements to the marketplace. These false claims are often made on social media such as Facebook and Twitter, as well as on electronic bulletin boards and chat rooms. Often the promoters will claim to have “inside” information about an impending development or to use an “infallible” combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is “pumped” up by the buying frenzy they create. Once these fraudsters “dump” their shares and stop hyping the stock, the price typically falls, and investors lose their money.

well as insider trading activity that provides insiders with an unfair trading advantage over average investors and undermines our markets.

In these types of frauds, illegal acts are particularly likely to be communicated via personal accounts and parties are more likely to be non-cooperative in their document productions. For example, in an insider trading case, there appeared to be gaps in the emails the suspected tipper produced pursuant to the SEC's administrative subpoena. We were able to obtain the individual's personal emails from the ISP under ECPA and among the messages provided by the ISP was an email containing the alleged tip, which became a critical piece of evidence in our successful actions against the tipper and tippee. Similarly, in an investigation into a market manipulation scheme conducted by foreign stock promoters that used personal email for certain sensitive communications regarding the scheme, it was essential to obtain the emails from an ISP because the principals were in a foreign country, and we could not compel them to produce information. The resulting emails provided key evidence on multiple issues: the emails showed planning discussions for the illegal scheme and control by the defendants of the companies that proved to be central to the manipulation.

Technology has evolved since ECPA's passage, and there is no question that the law ought to evolve to take account of advances in technology and protect privacy interests, even when significant law enforcement interests are also implicated. There are various ways to strike an appropriate balance between those interests as the Committee considers the best way to advance this important legislation. Any reform to ECPA can and should afford a party whose information is sought from an ISP in a civil investigation 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 has provided notice to email account holders in

keeping with longstanding (and just recently reaffirmed) Supreme Court precedent.⁵ Thus, in contemplating potential solutions, the Committee could consider language that would (1) require civil law enforcement agencies to attempt, where possible, to seek electronic communications directly from a subscriber before seeking them from an ISP; and (2) should seeking them from an ISP be necessary, give the subscriber or customer the opportunity to challenge the request in a judicial proceeding. If the legislation were so structured, an individual would have the ability to raise with a court any privilege, relevancy, or other concerns before the communications are provided by an ISP, while civil law enforcement would still maintain a limited avenue to access existing electronic communications in appropriate circumstances from ISPs. Such a proceeding would offer even greater protection to subscribers than a criminal warrant, in which subscribers receive no opportunity to be heard before communications are provided.

Some have asserted that providing civil law enforcement with an ability to obtain electronic communications from ISPs in limited circumstances would mean electronic documents enjoy less protection than paper documents. That is not accurate. Indeed, as currently drafted, S. 356 would create an unprecedented digital shelter – unavailable for paper materials – that would enable wrongdoers to conceal an entire category of evidence from the SEC and civil law enforcement.

⁵ See *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2015) (“The Court has held that absent consent, exigent circumstances, or the like, in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker.”); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (holding subpoenas “provide protection for a subpoenaed employer by allowing him to question the reasonableness of the subpoena, before suffering any penalties for refusing to comply with it, by raising objections in an action in district court. . . . We hold only that the defenses available to an employer do not include the right to insist upon a judicial warrant as a condition precedent to a valid administrative subpoena.”); *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000) (stating issuance of a subpoena “commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. . . . As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process”).

This should not be the case. The bill in its current form would harm the ability of the SEC and other civil law enforcement agencies to protect those we are mandated to protect and to hold accountable those we are responsible for holding accountable. There are multiple ways to modernize ECPA consistent with the law that would not impede our ability to protect investors and the integrity of the markets. We look forward to discussing with the Committee ways to modernize ECPA without putting investors at risk and impairing the SEC from enforcing the federal securities laws.

Thank you again for the opportunity to appear here today, and I would be happy to answer any questions you may have.



THE CHAIRMAN

UNITED STATES
 SECURITIES AND EXCHANGE COMMISSION
 WASHINGTON, D.C. 20549

April 24, 2013

The Honorable Patrick J. Leahy
 Chairman
 Senate Judiciary Committee
 United States Senate
 224 Russell Senate Office Building
 Washington, DC 20510

Dear Chairman Leahy:

I write in connection with the Senate Judiciary Committee's upcoming consideration of S. 607, the Electronic Communications Privacy Act Amendments Act of 2013.¹ While I appreciate your efforts to update the privacy protections for e-mail and other electronic communications for the digital age, I am concerned that the bill as currently constituted could have a significant negative impact on the Securities and Exchange Commission's enforcement efforts. For the reasons set forth below, I respectfully ask you to consider the negative impact that the legislation in its current form could have on the Commission's ability to protect investors and to assist victims of securities fraud, and would be interested in discussing with you a modest change in your proposal that would continue to address privacy concerns while also providing the Commission the authority it needs to effectively discharge its critical functions.

In carrying out its mandate to investigate violations of the federal securities laws, the Commission frequently seeks to obtain the contents of e-mail and other electronic communications. Such communications can provide direct and powerful evidence of wrongdoing. Because persons who violate the law frequently do not retain copies of incriminating communications or may choose not to provide the e-mails in response to Commission subpoenas, the SEC often has sought the contents of electronic communications directly from internet service providers (ISPs). Historically, the Commission has relied for this purpose on Section 2703(b) of the Electronic Communications Privacy Act (ECPA), which currently provides that a governmental entity may require from service providers pursuant to an administrative subpoena the disclosure of wire or electronic communications that are more than 180 days old.

A 2010 opinion from the Sixth Circuit Court of Appeals (*U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010)) has greatly impeded the SEC's ability to serve administrative subpoenas on ISPs absent the consent of the subscriber. In *Warshak*, a case involving the Department of Justice, the court held that the use of a Section 2703(b) subpoena or court order to obtain the contents of e-mails violated the Fourth Amendment's prohibition against warrantless searches. The ECPA amendments being proposed essentially would codify *Warshak*, permitting

¹ The views expressed in this letter are my own and do not necessarily reflect the views of the full Commission.

The Honorable Patrick J. Leahy
Page 2

federal governmental entities to obtain the content of e-mails from ISPs only if it were to obtain a warrant pursuant to the Federal Rules of Criminal Procedure. Such a structure essentially would foreclose the Commission – a civil federal agency – from gaining access to this information directly from ISPs absent consent of the entity being investigated.

Some have asserted that the Commission could avoid the negative consequences of the Act by simply subpoenaing the e-mails directly from the individuals being investigated. Unfortunately, individual account holders sometimes delete responsive e-mails, or otherwise fail to provide them, notwithstanding subpoenas that call for their complete production. Indeed, it is not surprising that individuals who violate the law are often reluctant to produce evidence of their own misconduct. Subpoenas to individuals also can be more effective if the subpoena recipient knows the Commission has the ability to go to an ISP and test whether they have fully responded to the subpoena. If individuals being investigated know the Commission lacks that ability, it could encourage them to be less forthcoming in their productions. In order for the Commission to obtain this important evidence and create a complete investigative record, it needs to preserve the authority to subpoena the ISPs to obtain any deleted or otherwise not available – or not produced – e-mails.

A case filed last year against two individuals demonstrates the importance of the authority. The civil action against these individuals alleged that over a period of years they engaged in a scheme to artificially inflate the financial results of a publicly owned retailer by engaging in a series of fraudulent “round-trip transactions.” As alleged in the complaint, one of the individuals had sent himself an e-mail describing the publicly owned company’s commitment to buy certain products and services at inflated prices, and stating “the fake credits that were negotiated with” the company were being used “to hit certain quarterly numbers.” During the Commission’s investigation (and pre-*Warshak*), the Commission obtained this key e-mail through an ECPA subpoena to the individual’s ISP. This evidence was particularly important because, as alleged in the complaint, the defendants had carefully concealed their scheme. At the time the Commission subpoenaed the ISP, the individual had failed to produce his personal e-mail in response to a document subpoena the SEC had issued him almost a year earlier. Thus, absent ECPA authority to subpoena the ISP directly, the Commission would not have had in its possession this critical piece of evidence.

Others have asserted that the Commission can simply work with the Department of Justice (DOJ) to get criminal search warrants. The reality is that to force the Commission to rely on DOJ to obtain search warrants in this context is impractical in most cases and ignores the significant differences in our respective jurisdictions. First, DOJ only has authority to seek search warrants to advance its own investigations, not SEC investigations. Thus, the Commission cannot request that the DOJ apply for a search warrant on the SEC’s behalf. Second, many SEC investigations of potential civil securities law violations do not involve a parallel criminal investigation, and thus there is no practical potential avenue for obtaining a search warrant in those cases. The large category of cases handled by the SEC without criminal involvement, however, have real investor impact, and are vital to our ability to protect – and, where feasible, make whole – harmed investors.

The Honorable Patrick J. Leahy
Page 3

Instead of effectively foreclosing the Commission from obtaining these electronic communications from the ISP, it would strike a better balance between privacy interests and the protection of investors to provide federal civil law enforcement agencies a viable avenue for obtaining the information in appropriate circumstances upon the approval of a federal district court. Specifically, a mechanism could be included in the proposed ECPA amendments to enable a federal civil agency to obtain electronic communications from an ISP for use in a civil enforcement investigation upon satisfying a judicial standard comparable to the one that governs receipt of a criminal warrant. I believe this approach would continue to address the privacy concerns animating your proposal while at the same time preserving a legitimate mechanism for the SEC, in appropriate circumstances and with court approval, to obtain much needed electronic communications from the ISPs.

I would be happy to discuss these issues with you in more detail or to provide you or your staff with legislative language for your consideration. Thank you in advance for your consideration of the impact S. 607 would have on the Commission's enforcement program. Should you wish to discuss these issues further, please do not hesitate to contact me at (202) 551-2100 or have your staff contact Tim Henseler, Acting Director of the SEC's Office of Legislative and Intergovernmental Affairs, at (202) 551-2015.

Sincerely,



Mary Jo White
Chair

cc: Members of the Senate Judiciary Committee

64

**Prepared Statement of
The Federal Trade Commission
Before the
United States Senate
Committee on the Judiciary
On
Reforming the Electronic Communications Privacy Act
Washington, DC
September 16, 2015**

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 Bureau of Consumer Protection at the Federal Trade Commission (“Commission” or “FTC”).¹ I appreciate the opportunity to appear before you today to discuss the FTC’s work and how proposals to amend the Electronic Communications Privacy Act (“ECPA”)² could impact the Commission’s civil law enforcement mission.

I. FTC Background

The FTC is an independent agency with an important dual mission to protect consumers and promote competition. The FTC is the only federal agency with jurisdiction to protect consumers and maintain competition in broad sectors of the economy. Although the Commission has important education, research, and advocacy functions, it is first and foremost a civil law enforcement agency. The agency enforces laws that prohibit business practices that are anticompetitive, deceptive, or unfair to consumers, and seeks to do so without impeding legitimate business activity.³

The impact of the FTC’s consumer protection work is significant. Between July 2013 and June 2015 alone, the FTC returned over \$154 million to consumers and sent over \$50 million in civil penalties to the Department of Treasury. The Commission’s consumer protection enforcement actions cover a broad range of activities, including fraud. For example, in recent years, the FTC’s actions have: (1) stopped fraudsters’ efforts to collect “phantom” debts from

¹ The written statement represents the views of the Federal Trade Commission. Commissioner Brill issued a concurring statement with respect to Part II.C. The oral presentation and responses to questions reflect the views of the witness, and do not necessarily reflect the views of the Commission or any Commissioner.

² 18 U.S.C. § 2701 *et seq.*

³ The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.*, and enforces a wide variety of other laws ranging from the Clayton Act to the Fair Credit Reporting Act. In total, the Commission has enforcement or administrative responsibilities under more than 70 laws. *See* <https://www.ftc.gov/enforcement/statutes>.

financially strapped consumers that the consumers did not actually owe;⁴ (2) taken aggressive enforcement actions to stop illegal robocalls;⁵ (3) sued companies that made false or unsubstantiated health claims;⁶ and (4) stopped foreclosure rescue scams and deceptive payday lending practices.⁷

In bringing these actions, we rely heavily on our ability to conduct thorough investigations of companies' business practices. Targets of FTC enforcement actions

⁴ See, e.g., *FTC v. K.I.P., LLC*, No. 1:15-cv-02985 (N.D. Ill. Apr. 6, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/152-3048/kip-llc-payday-loan-recovery-group>; *FTC v. 4 Star Resolution, LLC*, No. 1:15-cv-0112-WMS (W.D.N.Y. Feb. 9, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/122-32024-star-resolution-llc>.

⁵ See, e.g., *FTC v. Caribbean Cruise Line, Inc. et al.*, No. 0:15-cv-60423 (S.D. Fla. Mar. 4, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3196/caribbean-cruise-line-inc>; *FTC v. Worldwide Info Servs., Inc.*, No. 6:14-cv-8-ORL-28DAB (M.D. Fla. Nov. 13, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3175/worldwide-info-services-inc>; *FTC v. All Us Marketing LLC*, No. 6:15CV1016-ORL-28GJK (M.D. Fla. June 29, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-pavless-solutions-llc>; *FTC v. Lifewatch, Inc.*, No. 1:15-cv-05781 (N.D. Ill. June 30, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc>.

⁶ See, e.g., *FTC v. Lunada Biomedical, Inc.*, No. 2:15-cv-03380-MWF (PLAx) (C.D. Cal. filed May 12, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3067/lunada-biomedical-inc>; *FTC v. Leanspa, LLC*, No. 311-cv-01715 (D. Conn. Apr. 6, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/1123135/leanspa-llc-et-al>; *FTC v. New Consumer Solutions LLC et al.*, No. 15-C-1614 (N.D. Ill. filed Feb. 23, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3210/new-consumer-solutions-llc-mole-detective>. Commissioner Ohlhausen voted against issuing the initial complaint and accepting the related settlement orders and proposed consent agreement in this matter. See Dissenting Statements of Commissioner Ohlhausen, *FTC v. Lasarow* (August 13, 2015), available at <https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v-lasarow> and <https://www.ftc.gov/public-statements/2015/02/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-health>; *FTC v. NourishLife, LLC*, No. 1:15-cv-00093 (N.D. Ill. filed Jan. 7, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3152/nourishlife-llc>; *FTC v. NPB Advertising, Inc.*, No. 8:14-cv-0155-SDM-TGW (M.D. Fla. filed May 15, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3116/npb-advertising-inc-et-al>; *Health Discovery Corp.*, No. C-4516 (Mar. 13, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3211/health-discovery-corporation-melapp-matter>; *FTC v. Genesis Today, Inc.*, No. 1:15-cv-00062 (W.D. Tex. filed Jan. 26, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3283/genesis-today-pure-health-lindsey-duncan>. Commissioner Ohlhausen voted against accepting the proposed consent agreement. See Dissenting Statement of Commissioners Ohlhausen and Wright, *FTC v. Genesis Today, Inc.* (January 26, 2015), available at <https://www.ftc.gov/public-statements/2015/01/dissenting-statement-commissioners-maureen-k-ohlhausen-joshua-d-wright>.

⁷ See, e.g., *FTC v. Sameer Lakhany*, No. 8:12-cv-00337-CJC-JPR (C.D. Cal. Apr. 29, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/112-3136/lakhany-sameer-credit-shop-llc-fidelity-legal-services-llc>; *FTC v. C.C. Enterprises, Inc.*, No. 8:15-cv-00585-CJC-JPR (C.D. Cal. Apr. 16, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/112-3136-x120014/householdrelief>; *FTC v. Wealth Educators Inc.*, No. cv15-2357 (C.D. Cal. Apr. 10, 2015), available at <https://www.ftc.gov/enforcement/cases-proceedings/1523004/wealth-educators-inc>.

increasingly use electronic media and the Internet to reach consumers, transact business, and retain records. Although the Commission currently does not seek content of e-mails and other electronic communications covered by ECPA from ECPA service providers, we believe that in the future, as more electronic communication moves to the cloud, the effectiveness of our fraud prevention program may be hampered if proposed legislation is not appropriately modified.

II. FTC Views on ECPA Legislative Proposals

The FTC supports the objectives of ECPA reform. Technology has evolved considerably since ECPA's passage in 1986, transforming the way consumers and businesses function. The FTC appreciates Congress's efforts to update ECPA to account for these technological advances and to protect consumers' privacy. And, the FTC appreciates the Committee's continued interest in hearing the agency's views on current ECPA reform proposals.

As a civil law enforcement agency, the FTC is concerned that recent proposals could impede its ability to obtain certain information from ECPA service providers in future cases. Under current law, the Commission could compel an ECPA service provider to produce a customer or subscriber's content with notice or delayed notice to the customer or subscriber under 18 U.S.C. Section 2703(b)(1)(B). The Sixth Circuit, in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), however, held that the Fourth Amendment bars warrantless access to email content held by an ECPA service provider. We currently forebear from employing the authority under 2703(b)(1)(B) to compel production of a customer or subscriber's content. Under recent legislative proposals, however, to compel content from an ECPA service provider, the government would have to obtain a criminal warrant, which is not available to the FTC. The proposals would require a warrant for content even when it is previously public commercial content advertising or promoting a product or service or the customer or subscriber has consented

to the provider releasing the content to the FTC. The proposals also would prohibit agencies such as the FTC from obtaining content when the customer or subscriber is a scam artist who refuses to produce the content to civil law enforcement. As a result, these proposals appear to prohibit civil law enforcement from compelling the content of electronic communications from an ECPA service provider under all circumstances.

The Commission believes that Congress can and should modernize ECPA in order to protect customer or subscriber's privacy interests in electronic communications while also ensuring the effectiveness of civil law enforcement agencies by authorizing such agencies to: (1) obtain previously public commercial content that advertises or promotes a product or service, such as websites and marketing materials; (2) compel an ECPA service provider to disclose content with the customer or subscriber's consent; and (3) when efforts to obtain information directly from a target fail, seek a court order compelling the provider to produce electronic content.

A. Law Enforcement Access to Previously Public Commercial Content that Advertises or Promotes a Product or Service

Previously public commercial content that advertises or promotes a product or service is critical to many FTC investigations. Indeed, most of the agency's consumer protection investigations involve advertising or other marketing claims made through electronic media. These deceptive claims may appear on the companies' websites or classified ad sites. 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 about which consumers

complained. In other instances, the marketing materials may no longer be readily available due to an ECPA service provider's policy.⁸

Where the target is a fraudulent marketer, obtaining the advertisements through a civil investigative demand ("CID") to the marketer is often not a viable option for several reasons. First, the marketer may have no incentive to cooperate with the request. It may claim that it no longer has, or never itself retained, a copy. Or, it may simply deny that it ever posted the material. Second, any attempt to contact the marketer may cause it to flee, destroy evidence, or hide assets. In these circumstances, when a marketer refuses to cooperate or is unavailable, it is essential that the Commission retain the ability to use other appropriate mechanisms to obtain the information. If legislation impedes the Commission's ability to do so, it would frustrate the agency's ability to obtain evidence against the marketer and obtain relief for consumers.

Accordingly, the Commission is concerned that its robust anti-fraud program will suffer if copies of previously public commercial content that advertises or promotes a product or service cannot be obtained directly from the service provider. Under current law, Commission staff can work with ECPA service providers to obtain such previously public content in certain circumstances.⁹ Without further clarification to recent legislative proposals, however, updates to ECPA would appear to prevent the FTC from compelling ECPA service providers to produce such previously public material.¹⁰ Commission staff might then be unable to obtain

⁸ For instance, on some bulletin boards, postings expire automatically, but copies may be maintained by the service provider.

⁹ The Commission can compel an ECPA service provider to produce a customer's previously public commercial content that advertises or promotes a product or service so long as the provider is maintaining a copy for an independent business reason, rather than solely for the subscriber. Cf. 18 U.S.C. § 2703(b)(2)(B) (covering content held "solely for the purpose of providing storage or computer processing services to such subscriber or customer. . .").

¹⁰ The Commission does not believe that all previously public content should be exempt from ECPA. But, a marketer has no reasonable expectation of privacy in its previously public commercial content that advertises or promotes a product or service.

advertisements that ran on a social media site from the site operator, or old versions of web sites from a scam's web site host.

Consequently, we urge Congress to ensure that any legislation updating ECPA preserve the ability to obtain previously public commercial content that advertises or promotes a product or service. This would enable the Commission to obtain such commercial content -- a narrow, well-defined category of content. At the same time, because such materials are purely commercial and were affirmatively published by a target, the target does not have a reasonable expectation of privacy in them with respect to law enforcement access.

B. Law Enforcement Access to Contents of Records with the Customer or Subscriber's Consent

Proposed amendments to ECPA permit civil law enforcement agencies to require an ECPA service provider to produce non-content information "pertaining to" the subscriber, if the customer or subscriber has consented. Under these proposals, however, this authority does not extend to the "content" of any other records of the customer or subscriber, including its business records, Web pages, or other stored communications, even if the customer or subscriber has consented to disclosure.¹¹

As cloud computing becomes more widespread, it is increasingly important for a civil law enforcement agency to be able to compel an ECPA service provider to disclose such electronic content 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 the defendant's only copies of the records are maintained on that service. Indeed,

¹¹ Under current ECPA, there is no separate provision that permits a civil agency to demand content from a provider when it has the consent of the customer or subscriber. Instead, the law's general provisions regarding government access to content would apply. *See* 18 U.S.C. § 2703.

ECPA already permits a service provider to divulge such content voluntarily with the customer or subscriber's consent (and this provision is not affected by proposed changes to ECPA).¹² Under current legislative proposals, however, even if the customer or subscriber has consented, the agency could not compel the cloud computing service to release that customer or subscriber's content. This disparity -- allowing ECPA service providers to disclose content voluntarily if the customer or subscriber consents, but denying law enforcement agencies the authority to compel such disclosures -- enables providers to deny the effect of a customer or subscriber's consent. Thus, the Commission recommends that the Committee ensure that civil law enforcement agencies have the authority to compel ECPA service providers to produce electronic content if the customer or subscriber has consented to its production.

C. Civil Law Enforcement Access to Content That Cannot Be Obtained from a Target

Although we do not currently obtain subscriber content from ECPA service providers pursuant to section 2703(b)(1)(B), we believe that recent legislative proposals requiring the use of a criminal warrant to obtain content from an ECPA service provider could create some obstacles in future *civil* law enforcement cases, including those against fly-by-night scammers and especially those based abroad, as well as cases against targets that refuse to respond to the agency's CIDs or discovery requests. Under these proposals, targets could simply refuse to produce content, and the FTC would be left with limited ability to obtain it. The Commission therefore suggests that Congress consider providing a judicial mechanism that would authorize the Commission to seek a court order directing the provider to produce the content if the Commission establishes it has sought to compel it directly from the target, but the target has failed to produce it.

¹² See 18 U.S.C. § 2702(b)(3).

III. Conclusion

Thank you for giving the Commission an opportunity to describe the important work of the agency, the critical 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 this Committee to address the Commission's concerns as legislation advances.

**Commissioner Julie Brill's Statement
About the Federal Trade Commission's Written Testimony
on "Reforming the Electronic Communications Privacy Act
Submitted to Senate Judiciary Committee
September 16, 2015**

I write separately to describe my views regarding Part II.C of the Commission's written statement for the Senate Judiciary Committee's hearing on ECPA reform legislation.

In this section, the Commission asks Congress to create a "judicial mechanism" through which the Commission and other civil law enforcement agencies could obtain the contents of online accounts from ECPA-covered entities in the course of their investigations. The testimony frames this recommendation as an alternative to legislation that would require a criminal warrant to obtain content from ECPA-covered providers. I am not convinced that this authority is necessary to maintain the Commission's effectiveness as a law enforcement agency now or in cases that we can presently foresee. On the other hand, I am concerned that a judicial mechanism for civil law enforcement agencies to obtain content from ECPA providers could entrench authority that has the potential to lead to invasions of individuals' privacy and, under some circumstances, may be unconstitutional in practice.

As the Commission's testimony states, the FTC currently has some authority under ECPA to obtain content from ECPA-covered entities. Although this authority exists on paper, the Commission rarely if ever uses it. One reason for our forbearance from seeking content through ECPA is that situations in which this authority is useful are exceedingly rare. The Commission is highly effective in uncovering the identities and finding the locations of fraudsters and other targets by seeking basic identifying information under other provisions of ECPA. We are also very often successful in tracing the flow of ill-gotten money and locating assets that may be used for consumer redress through authority that is entirely separate from ECPA. In addition, we routinely acquire the contents of relevant documents, including nonpublic emails and other messages, either directly from targets or from third parties who are not subject to ECPA.

Moreover, for the past five years, a major, additional factor in the Commission's forbearance from obtaining content under ECPA is the Sixth Circuit's decision in *United States v. Warshak*, which held that obtaining the content of email through a court order, rather than a warrant, violated the Fourth Amendment.

In the meantime, the Commission has built an extremely impressive record of shutting down a wide range of frauds and recovering hundreds of millions of dollars for consumers. In our investigations and in our efforts to enforce judgments, we encounter many obstacles – wasted assets and offshore defendants, for example – but an inability to obtain content from ECPA providers generally is not one of them.

The costs – in terms of privacy protections for consumers – of solidifying the

Commission's authority to obtain content through ECPA is real. Fundamentally, I believe that individuals' privacy interests extend to what they store and send online. I simply am not convinced that a judicial mechanism enabling civil law enforcement agencies to order ECPA-covered providers to turn over content will provide the safeguards against government intrusion to which individuals are entitled.

At the same time, I am not today endorsing proposals that would only allow law enforcement authorities to obtain ECPA-related content through a criminal warrant. I believe that the issues raised in today's hearing will benefit from further discussion and debate within the Commission and with Congress and all stakeholders.

Written Statement by

**Richard Littlehale
Assistant Special Agent in Charge
Tennessee Bureau of Investigation**

Before the United States Senate Committee on the Judiciary

**Hearing on
“Reforming the Electronic Communications Privacy Act”**

September 16, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to speak to you today. I am the Assistant Special Agent in Charge of the Technical Services Unit of the Tennessee Bureau of Investigation. We are the high-tech investigative unit of Tennessee’s statewide criminal investigation agency. One of my unit’s most important responsibilities is to help law enforcement agencies at all levels of government throughout Tennessee use communications records in support of their criminal investigations. I have used these techniques for twenty years in support of cases ranging from searches for violent fugitives to efforts to recover abducted children and victims of minor sex trafficking.

I am grateful to the Committee for the opportunity to share a criminal investigator’s perspective on the challenges that law enforcement faces when gathering digital evidence. The evidence regulated by ECPA can be invaluable in the most critical of law enforcement investigations, and improvements in the law can help my colleagues and I work faster and more efficiently to bring the guilty to justice and exonerate the innocent. My fellow practitioners and I especially appreciate the signal sent by your invitation to today’s hearing, because state and local law enforcement conducts the vast majority of criminal investigations in this country. Since the laws before the Committee today govern our access to much of the digital crime scene, any change in the law will impact us greatly. Our community appreciates your recognition that our expert perspective should be a central consideration of any update to ECPA.

I offer testimony here today as a representative of the Association of State Criminal Investigative Agencies (ASCIA). The Director of the Tennessee Bureau of Investigation, Mark Gwyn, is the current president of ASCIA.

Access to Evidence in the Digital Crime Scene

The crime scene of the 21st century is often replete with digital evidence. This digital crime scene, including electronic communications records in the possession of private companies, often holds the key to solving the case. It also holds the key to ruling out suspects and exonerating the in-

nocent. Investigators' ability to access that evidence quickly and reliably under the law is fundamental to our ability to carry out our sworn duties to protect the public and ensure justice for victims of crime.

To date, the lion's share of the scholarly, media, and advocacy attention given to the question of lawful access to stored content has focused on the level of proof required to obtain digital evidence. This narrow focus neglects a set of critical issues that impact law enforcement's ability to gather digital evidence from private companies every day across the country. I am referring to the quality and character of service provider responsiveness to law enforcement legal demands, as well as well-intentioned but overly burdensome accountability considerations like customer notification and reporting requirements. From the perspective of an investigator working the digital crime scene, these concerns impact our ability to gather the digital evidence we need as much or more than any other, and they have been noticeably absent from the ECPA reform debate.

The simple truth is that legal and technological barriers are not the only ones that keep communications records out of law enforcement hands. In many instances, we are unable to utilize evidence that would be of enormous value in protecting the public because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain. That may be because of technological problems, but just as frequently it is because of **non-technical barriers to access**. The companies that retain these records are often unable or unwilling to respond to law enforcement's lawful demands in a timely manner, and there are few consequences for an incomplete or inaccurate response. The primary emergency disclosure provision in the section of ECPA that we use to obtain stored content is **voluntary** for the providers, not mandatory, and even where emergency access is granted to law enforcement, in some instances, there is insufficient service provider compliance staff to process legitimate emergency requests quickly.

As Congress considers simplifying the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to obtain those records, the full range of non-technical barriers to access must have a place in the discussion. I would urge Congress ensure that regardless of the level of process it ultimately decides is appropriate, that steps are taken to guarantee that law enforcement will be able to access the digital evidence that we need to do our jobs reliably and quickly once that process is obtained.

In an effort to better inform the committee, I solicited feedback on these non-technical barriers to access from a wide range of law enforcement agencies, specialties, and investigative focuses. More often than not, the responses were along the lines of "oh, you mean beyond the usual?" Beyond routine turnaround times measured in months, the inability to speak to a human being about your case in a timely manner, uneven access to records in emergencies? Beyond service providers who routinely pre-litigate the legal process instead of leaving that to the courts, who return legal demands without complying because the demand failed to use the magic language of the moment that the provider prefers, regardless of whether or not it is statutorily or constitutionally compelled? These are the day-to-day realities of professionals working the digital crime scene, not isolated and unfortunate bumps in the road.

Consider a case a few years ago regarding the stranger abduction of a 4-day-old infant in Nashville where my unit was tasked to work the digital crime scene. Over the course of an intensive

four-day investigation, my unit processed and explored leads on hundreds of telephone numbers, social media accounts, computers and mobile devices. At a time when every second counts, my fellow agents and I spent a significant amount of time simply trying to make contact with various providers to declare an emergency, calling and recalling to make sure that our process was received and expedited as necessary. In one instance, a voice mail that contained potentially critical evidence for the prosecution of the kidnapper was lost because a cellular provider mishandled a preservation request. In another, we had to spend precious time trying to get a service provider on the phone to figure out the time stamps of phone records, because it was unclear on the face of the records when the critical calls were made. All while processing hundreds of electronic leads, any one of which could be the one that holds the key to rescuing the victim. These issues are obviously problematic, but this is a routine part of a criminal investigator's day working the digital crime scene.

Another example that highlights a need for reform of current law started with a threat of a mass casualty attack on a high school in a large Texas city. An unknown party threatened a high school and responding police in March of 2015 on a popular social media platform, and backed it up with a picture of an assault rifle; this caused the school to go into lockdown. Law enforcement issued a subpoena and a judicial non-disclosure order (to keep the provider from notifying the user) to attempt to identify the user who posted the threat. Even though the threats were posted on the social media provider for everyone to see, the provider still would not turn over records under the emergency exception and required law enforcement to get a search warrant before they would release content. Fortunately, the attack did not materialize that day, and investigation continued. By late April, investigators had determined that the sender used a free virtual private network (VPN) service to mask their Internet Protocol address while posting the threats, and issued a court order to the VPN provider. Two and a half weeks later, they received a response stating that the provider found no responsive records, and indicated that "unfortunately due to limited resources our logs are purged at the latest every 48 hours." Was the threat real, or a hoax? Was the sender serious about the attack but deterred by the lockdown, or simply wasting resources and scaring children for their own amusement? Texas authorities may never know.

The Leahy-Lee ECPA Amendments Act, as introduced, could have the effect of providing more protection for digital evidence than evidence in the physical world, and does nothing to address the range of concerns that the above examples illustrate. That is a major concern, and if the intent is to bring the law into balance for the 21st Century, we strongly believe legislation should not create higher protections for a particular piece of evidence that is stored electronically rather than in a filing cabinet, nor should it elevate burdens on law enforcement without providing assistance with long-standing problems like the ones outlined below.

Non-Technical Barriers to Access

As we consider non-technical barriers to access in more detail, we should be mindful of a simple fact that is often overlooked in the public discourse on this topic: we are talking about law enforcement's ability to gather **evidence**. Not "information" or "content" or "communications records," but **evidence**. All hammers are tools; a hammer only becomes evidence if it is relevant to a criminal investigation. Similarly, law enforcement has no interest in communications records unless they advance a criminal investigation, whether to prove guilt or exonerate the innocent.

Timeliness and quality of service provider response. The importance of the timeliness and quality of service provider responses to lawful demands from criminal investigators for digital evidence cannot be overstated. Of all the issues that we are concerned about in this ECPA reform discussion that could increase the safety of the American citizens we serve without negatively impacting their privacy, this is the most significant. When we get the legal process that we need, let's make sure we get the records quickly, and make sure that they are complete and responsive. Let's minimize administrative latency in the compliance process. That is what would help us solve crimes more effectively.

There is no requirement in current law – including the service and execution of search warrants based upon probable cause – for providers to respond in a timely fashion to lawful process requests by governmental entities. Voluntary compliance has not worked as effectively as we need, because a truly efficient compliance operation might put a provider at a competitive disadvantage, because their competitors aren't required to spend the same resources. Any contemplated change in the law that would result in a lengthening of the investigative timeline – including moving some evidence to a probable cause standard that can currently be obtained on a lesser showing – should be accompanied by provisions that ensure accountability and prompt response by service providers to legitimate law enforcement requests.

It is worth considering the traditional legal framework surrounding search warrants as we consider these questions. We should keep in mind that in a traditional context, when law enforcement demonstrates probable cause to a neutral magistrate and the magistrate issues a warrant, it then becomes the law enforcement officer's decision about when to execute the warrant, how hard to search, and so on, based on the facts and circumstances of the case. In the digital space, it is the providers who actually conduct the search. Law enforcement typically has no visibility into the process of conducting the search or how thorough the search is. This results in sometimes haphazard diligence with respect to compliance, incomplete responses, and turnaround times measured in weeks and months.

Further, service providers often “pre-litigate” search warrants, returning them without being executed because of some perceived defect in language in the warrant. That is unheard of in other contexts; law enforcement gathers the evidence that they feel is responsive to the warrant, and then the defendant has an opportunity to challenge that collection later. The only option to really explore this would be to ask the prosecutor to seek a show cause hearing, and it is difficult to find the time for that when you are looking for a missing child or dangerous fugitive. As a result, this practice on the part of service providers goes largely unchallenged. This would be unheard of outside the digital space: when law enforcement demonstrates probable cause to a neutral magistrate and obtains a search warrant, we decide what evidence to gather and when we gather it, and any aggrieved party has the ability to object later through the courts. By creating a statutory requirement for responsiveness that looks more like response to legal demands in the physical world, this Committee would give law enforcement and industry a benchmark to ensure fairness across the industry, transparency for citizens, and adequate safeguards for public safety.

I have heard some service providers cite the high volume of law enforcement requests as a reason for response times that stretch into months, threatening the underlying investigation. We

have heard they do not have the staff necessary to process the volume of requests quickly. While staffing levels are obviously the prerogative of the company, we understand the difficulty of assigning new resources to an activity that is not a profit center. But the consequences of these decisions in world of criminal investigations is significant. Further, many of these providers are in the business of finding technological solutions to just this kinds of problem - automating processes to enhance efficiency and accountability and share information effectively. They are well acquainted with monitoring customer service centers and determining adequate staffing levels. The people on the other end of the line when we call providers are often very knowledgeable and helpful, and they often demonstrate significant interest and investment in our cases. It is not a matter of their willingness, but rather the resource allocation decisions made at different levels.

Since providers have little economic incentive to innovate or increase staffing levels in their compliance shops, a reasonable legal requirement for responsiveness may be part of the solution to these problems. Such a solution need not be overly costly or burdensome. Congress can protect citizens' privacy and at the same time ensure that victims of crime see justice done thanks to the persistent work of investigators who have timely and reliable access to evidence. Any reform of ECPA should take this issue into consideration.

Notification provisions may put a significantly greater and more costly administrative burden on law enforcement. Several ECPA reform proposals have borrowed language from wiretap law requiring notification of customers of legal demands, or securing a series of separate court orders delaying notification. These provisions risk diverting critical law enforcement resources from investigations simply to comply with burdensome notification provisions or delay orders. We would urge the committee to carefully balance the need for notification and reporting against the resources it will drain away from a range of investigative priorities. In addition, due to the nature of investigations today and the way people create accounts, there is no way to clearly understand - within the timeframes specified in pending ECPA reform legislation - who exactly is to be notified. How much time must investigators spend chasing down parties to notify, rather than working their investigations?

Concerns about the volume of law enforcement legal demands. As I address the issue of volume of legal process and its effect on timeliness of service provider response, I must also address a common talking point about those who would further restrict law enforcement access to stored content: namely, that the number of law enforcement requests for this information is growing. Our response is simple: of course it is. That is because in the digital age, a growing percentage of the available evidence in any criminal case is going to exist in the digital crime scene. Communications records have taken their place alongside physical evidence, biological evidence, testimonial evidence, and the other traditional categories. Laws and policy should reflect this reality and ensure law enforcement access to evidence that by its nature can't make a mistaken identification in a lineup or testify untruthfully, and should further ensure that law enforcement does not face greater obstacles to gathering digital evidence that we do to the other types.

A casual review of transparency data supplied by major service providers will disclose that law enforcement legal demands affect only a tiny percentage of accounts. I encourage the committee to keep these numbers in mind when some parties claim that law enforcement is "snooping" without regard to privacy. When we request these records, it is for a reason - we believe that the

records constitute evidence that will help us identify sexual predators, recover kidnapping victims, successfully prosecute murderers. Any consideration of changes to ECPA that will make obtaining communications records more time-consuming and laborious should reflect an understanding of how those changes will impact our ability to do our job, and whether or not the public would truly be upset about the balance as it is currently struck.

Current emergency provisions within ECPA are not adequate to allow law enforcement to respond effectively in all cases. Few dispute that law enforcement should have rapid access to communications records in a life-threatening emergency, but few outside of our community truly understand how flawed the current emergency options are. The “emergency” provision in current law (18 USC 2702(b)(8)) puts the decision to release records before legal process is obtained, and about whether a situation is an “emergency,” in the hands of the provider, rather than the law enforcement experts who are the boots on the ground. This has led to situations where responses to legitimate law enforcement requests have been delayed. In some cases, providers make a decision never to provide records in the absence of legal process, no matter the circumstances, as baffling as that may sound in the light of day.

Another Tennessee case comes to mind; once again, my unit was handling the communications component of an AMBER Alert investigation. One of the many leads that we received about someone who might have knowledge of the missing child's location appeared in a post on the site of a social media provider. Keep in mind that when we contacted them, this was only one of a flood of leads, any one of which could be critical to rescuing the victim. We can't know which one until we receive the evidence we need. That social media provider told us that while they agreed that the situation was an emergency, they were aware that the emergency provision in ECPA was permissive rather than mandatory, and it was their policy never to provide records on an exigent basis; they always wanted legal process (in this case, a search warrant) first. Could we have found the victim sooner, and spared them additional time in the hands of their abductor? We'll never know.

We would further point out that 18 USC 2258, which has been erroneously cited as an emergency option for law enforcement in child exploitation cases, is in fact a requirement that service providers send information about online child exploitation to the National Center for Missing and Exploited Children. Law enforcement cannot use it as a means to obtain records directly. The service providers still require legal process or an emergency declaration under 2702 before they will provide the evidence that generated the referral to law enforcement.

Any effort to reform ECPA should address the creation and logging of certain types of records. Certain types of widely used electronic communications are not retained by some providers, which can hinder law enforcement investigations. In particular, law enforcement faces challenges with respect to “IP logs,” records of which computer or other device is linked to a particular communication. Without a statutory requirement for logging and retention of those records, it is possible to make online threats or victimize children with impunity, secure in the knowledge that law enforcement cannot identify the point where the communications were made. I am well aware that retention means a cost for service providers; it is for precisely that reason that voluntary compliance is not likely to work, and a statutory requirement should be considered. I would urge Congress to find a balance that is not overly burdensome to service providers, but that ensures that law enforcement has access to critical evidence for at least some period of time.

Preservation provisions under current law should be revisited to ensure that law enforcement can prevent service providers from notifying customers of the existence of the request. One provision of the bill the committee is considering would cause prior notification to law enforcement before a provider notifies a customer or subscriber about the existence of a warrant, order, or subpoena, and we believe that provision is important. However, a similar provision relating to preservation orders under 2703(f) should be considered. There are service providers who have stated a policy of notifying customers of any government inquiry unless they are in receipt of process ordering them not to do so. The threat to investigations is clear if these situations are not handled appropriately, and there should be no room for interpretation by service providers in this matter.

Conclusion

Any effort to modify the standard of proof for access to stored content that does not address the concerns outlined above will lengthen law enforcement's investigative timeline, and therefore reduce our effectiveness. A robust debate about balancing personal privacy and security is beneficial to all Americans, but the people and their representatives must be able to make an educated judgment about what they are giving up and what they are getting. There is no question that a growing number of personal details about all Americans move in the digital world, and some of those details make their way into digital crime scenes. Just as there is no question that the people living those lives have an interest in preserving the privacy of that information, there can be no question that some of those devices hold the keys to finding an abducted child, apprehending a dangerous fugitive, or preventing a terrorist attack.

Our society benefits from an open exchange of ideas on topics critical to the public interest, and we believe that the ECPA reform debate remains largely one-sided. Redrafting the laws governing law enforcement access to communications records raises significant implications for law enforcement's ability to protect the public. I urge the members of this committee to ensure that members of the state and local law enforcement community who are in the trenches doing this work every day - and whose jobs will be significantly impacted by any changes in the law - are given the opportunity to continue to share their perspective on the potential human implications of any proposed reform of the Electronic Communications Privacy Act. Competing factors must be balanced appropriately, yet to date the conversation around the issues I have described has been mostly absent. We must be mindful that any restriction of law enforcement's lawful access to electronic evidence, whether by redefining legal barriers, heightening protections for evidence in the digital world compared to the physical world, or allowing service providers to erect new technological barriers, may well come at a price, and some of that price could be paid by our most vulnerable citizens. We should be sure we are willing to require them to pay it. We can enhance citizens' privacy, and we can also ensure criminal investigators get evidence they need quickly and reliably when lawfully authorized to do so.



**Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google Inc.
Senate Judiciary Committee
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

Chairman Grassley, Ranking Member Leahy, and members of the Committee, thank you for the opportunity to appear before you this morning to discuss updating the Electronic Communications Privacy Act (ECPA).

My name is Richard Salgado. As the Director for Law Enforcement and Information Security at Google, I oversee the company’s response to government requests for user information under various authorities, including ECPA. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the U.S. Department of Justice, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and Stanford Law School.

Google is a member of the [Digital Due Process \(DDP\) Coalition](#), which supports updating ECPA. [More than 100 organizations, trade associations, and corporations](#) are DDP members. DDP members span the ideological spectrum, ranging from the American Civil Liberties Union (ACLU) and the the Center for Democracy & Technology (CDT) to Americans for Tax Reform (ATR) and FreedomWorks. The diverse array of organizations, trade associations, and corporations that comprise the Digital Due Process Coalition is a testament to the breadth of support for updating ECPA in the Internet era.

Google strongly supports [S. 356](#), the Electronic Communications Privacy Act 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 that there is strong interest in aligning ECPA with the Fourth Amendment and users’ reasonable expectations of privacy.

ECPA Reflects the Pre-Cloud Computing Landscape of the 1980s

ECPA was enacted in 1986, well before the web as we know it today even existed. The ways in which people use the Internet in 2015 are dramatically different than in 1986.

- In 1986, there was no generally available way to browse the World Wide Web, and commercial email had yet to be offered to the general public. Only 340,000 Americans subscribed to cell phone service, and not one of them was able to send a text message, surf the web, or download applications. To the extent that email was used, users had to download messages from a remote server onto their personal computer. Holding and storing data was expensive, and storage devices were limited by technology and size.
- In 2015, hundreds of millions of Americans use the web every day, to work, learn, connect with friends and family, entertain themselves, and more. Data transfer rates are significantly faster than when ECPA became law, making it possible to share richer data, collaborate with many people, and perform more complicated tasks in a fraction of the time. Video sharing sites, video conferencing applications, search engines, and social networks, all the stuff of science fiction in 1986, are now commonplace. Many of these services are free. As a result of these technological advances, Americans are increasingly relying on third party service providers to store their online content, including videos, family photos, and confidential communications. The expectation is that such service providers can and will provide infinite storage indefinitely.

The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2015, ECPA frustrates users' reasonable expectations of privacy. 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 documents stored in a desk drawer. There is no compelling policy or legal rationale for this dichotomy, but it is one that ECPA continues to make, despite [widespread agreement that the statute should be updated](#).

ECPA Must Be Updated

Although the benefits of cloud computing have become more obvious and widespread, the outdated technology assumptions baked into parts of ECPA frustrate users' reasonable expectations of privacy. This is an unfortunate and unintended consequence of technological advancement, as Congress passed ECPA in 1986 in order to protect the privacy of users of electronic services in light of innovation. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today. This leaves us, in some circumstances, with complex and baffling rules that are both difficult to explain to users and difficult to apply.

One of the most baffling and complex set of rules is around compelled disclosure of communications content. ECPA provides that the government can compel a service provider to

disclose the contents of an email that is older than 180 days with nothing more than a subpoena (and notice to the user, which can be delayed in most cases). If the email is 180 days or newer, the government will need a search warrant. In its testimony before the House Judiciary Committee in 2013, the [Department of Justice \(DOJ\) acknowledged](#) that there is “no principled basis to treat email less than 180 days old differently than email more than 180 days old.” DOJ also recognized in its 2013 testimony that the statute should “not accord lesser protection to opened emails than it gives to emails that are unopened”, which is another problematic distinction that ECPA makes.

In 2010, the Sixth Circuit opined in [United States v. Warshak](#), 631 F.3d 266 (6th Cir. 2010) that ECPA violates the Fourth Amendment to the extent that it does not require law enforcement to obtain a warrant for email content. In so doing, the Sixth Circuit effectively dispensed with ECPA’s 180 day rule and the distinction between opened and unopened emails as irreconcilable with the protections afforded under 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 embraced by companies and observed by governmental entities. In many ways, then, S. 356 is a modest effort to codify the status quo and implement the Sixth Circuit’s conclusion that the Fourth Amendment requires a warrant in all cases where the government seeks to compel a provider to disclose communications content from a company covered under ECPA.

The inconsistent, confusing, and uncertain standards that currently exist under ECPA fail to preserve the reasonable privacy expectations of Americans today. Moreover, providers, judges, and law enforcement agencies alike have difficulty understanding and applying the law to today’s technology and business practices. By creating inconsistent privacy protection for users of cloud services and inefficient and confusing compliance hurdles for service providers, ECPA has created an unnecessary disincentive to move to a more efficient, more productive method of computing.

The Supreme Court Recognizes the Importance of Affording the Highest Privacy Protections to Electronic Communications

Between the last time I testified in support of updating ECPA in March 2013 and now, the Supreme Court issued a landmark decision in [Riley v. California](#), 134 S.Ct. 2473 (2014), where it unanimously held that officers must generally obtain a warrant before searching the contents of a

cell phone incident to an arrest. Writing for the Court, Chief Justice Roberts rejected the government's invitation to create "various fallback options for permitting warrantless cell phone searches under certain circumstances," noting that a regime with various exceptions and carve-outs "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:

"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 Justice Roberts sought to revitalize in *Riley*. But 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 entreaties and to codify the bright-line, warrant-for-content standard that is reflected in S. 356, which is sponsored by Senators Lee and Leahy.

Congress Should Reject Proposals That Weaken the Core Privacy Protections in S. 356

Civil Government Agency Issue

Some governmental entities have argued that the *Warshak* rule hampers their ability to investigate and enforce civil violations because civil agencies do not have warrant authority and thus lack the ability to obtain content. These governmental entities have proposed amending ECPA so that agencies can ultimately bypass the target of, or even potential witnesses in, civil investigations and issue legal process (on something less than a warrant) to third party service providers covered by ECPA. SEC Chairwoman Mary Jo White alluded to such an idea in an April 2013 [letter to Senator Leahy](#).

It makes little sense, however, to enact a bright-line, warrant-for-content standard while simultaneously creating a new carve-out that would eviscerate that bright-line rule. Congress should eschew proposals that would create a civil agency carve-out to such a bright-line rule for the following reasons.

First and foremost, a civil agency carve-out would contravene *Warshak* and the Fourth Amendment principles that animated the Sixth Circuit's conclusion in that case. Civil government agencies are still government agencies. The power to compel providers to disclose the content of

users' communications should be reserved for criminal cases. Congress should be deeply skeptical of efforts to draft around the Fourth Amendment, which is what some governmental entities are asking it to do.

Second, civil agencies have long done their job without such an exception. They can and do directly subpoena the targets of or witnesses in civil investigations to obtain relevant evidence, including emails and other content the targets or witnesses have stored with providers. This is, of course, how civil litigation routinely works; a discovery request is served on a party or witness and the party or witness is expected to produce responsive material that is in her possession, custody, or control. There is no reason to radically alter our civil litigation system simply because of the advent of cloud computing, which enables litigants to theoretically obtain the same data from service providers like Google. Electronic communication and remote computing service providers ("providers") are not, nor should they be, discovery agents for governmental entities that are conducting civil litigation.

Third, if targets and witnesses of civil investigations are intransigent or uncooperative, governmental entities have a broad array of tools to compel compliance. Civil agencies can always enforce subpoenas when a person fails to produce responsive documents. If a target or witness subsequently fails to produce responsive material pursuant to a court order to do so, the judge may impose sanctions, which could include the denial of counter-claims, adverse inferences as a result of the target's intransigence, fines, default judgments, and even jail time.

Fourth, there is no heightened risk of spoliation or destruction of evidence by requiring civil agencies to subpoena the targets of their investigations. To the extent that civil agencies are concerned about spoliation or destruction of evidence, those concerns are exogenous to ECPA reform. If civil agencies believe that targets and witnesses of investigations, or adversaries in litigation altogether, can't be trusted to produce responsive material, that is a problem neither unique to ECPA, nor addressable by compromising the constitutional requirement for clear rules about government access to user communications.

Fifth, civil discovery often brings with it complex and difficult disclosure issues around relevance, attorney-client privilege and other privileges, trade secrets, confidential business information and the like. If served with civil process to disclose a user's content, a provider will be ill suited to raise these objections or assert privileges; that is something the user should do as part of responding to record requests directed to the user. Congress should eschew any legislative change that would put service providers in the untenable position of making these types of critical judgment calls, which have enormous implications for privacy and due process. The risks of a provider turning over privileged or otherwise protected material increases significantly with the volume of

material that is sought by a civil agency. If a civil agency seeks three years' worth of email, it is likely, if not a foregone conclusion, that irrelevant and privileged material about a user will be produced.

Sixth, it is important to remember that civil agencies, even pre-*Warsake*, have operated under ECPA, and have never been able to compel production of all content. Despite this, civil agencies prosecute offenses and undertake enforcement actions against violators with regularity. In its [2014 annual report](#), the SEC notes that it brought a “record number of cutting edge enforcement actions.” In that same report, the SEC said that it brought “more cases than ever before”, including “a number of first-ever cases that span the securities industry.” It did so, as [Chairman White testified](#) earlier this year, without issuing subpoenas for content from providers under ECPA.

Finally, while some civil agencies have raised hypothetical concerns that a bright line, warrant-for-content rule would frustrate their investigations, there is scant evidence to suggest that civil agencies typically encounter such scenarios or that, even when they do, the investigations are hindered. In the 2013 letter from SEC Chairman White to Senator Leahy, the SEC cited a single example where it ostensibly could not have brought a case but for the ability to serve a subpoena directly on a provider to obtain email content about the target. After examining the record in that case, however, the [Center for Democracy and Technology](#) found that the case cited by the SEC “actually shows that the need for new authority is greatly overstated, if not totally unjustified,” and that it “illustrates precisely the risk of indiscriminate production of personal emails that we have warned about.”

Emergency Exception

Under current law, service providers [may disclose the contents of communications or customer records to a governmental entity in an emergency](#) involving danger of death or serious physical injury to any person. Some law enforcement agencies, however, propose *requiring* service providers to disclose the contents of communications and customer information whenever any federal, state, or local governmental entity believes there is an emergency under ECPA.

In November 2013, Google began including information about emergency requests in its [bi-annual transparency report](#) covering government demands for user data. Other service providers, including Facebook, Microsoft, and Yahoo, also now include information about emergency requests in their transparency reports.

[This data helps shed light](#) on the volume of emergency requests that service providers receive, which is very low in comparison to the total number of compulsory legal demands that service providers receive under ECPA. In the second half of 2014, for example, Google received 171 emergency requests affecting 272 user accounts in the U.S. That figure represents less than 2%

of all compulsory legal demands in the U.S. received by Google. Moreover, Google voluntarily disclosed some or all data in response to 80% of such emergency requests. (By comparison, Google disclosed some or all data in response to 78% of compulsory legal demands in the U.S. in the second half of 2015.) Effectively, what this means is that Google only withheld user data in response to an emergency request on approximately 34 occasions in the second half of 2014. Further information about Google's handling of emergency requests appears in the table below.

| Timeframe | Emergency Requests | Users/Accounts Impacted by Emergency Requests | Percentage of Cases Where Some or All Data Provided in Response to Emergency Requests |
|----------------------|---------------------------|--|--|
| July - December 2014 | 171 | 272 | 80% |
| January-June 2014 | 171 | 241 | 65% |
| July-December 2013 | 153 | 217 | 78% |
| January-June 2013 | 119 | 175 | 81% |

There are many reasons why a service provider may decline to voluntarily disclose the contents of communications or customer records in response to an emergency request.

For example, the service provider may not have any responsive data that pertains to the target of an investigation. For [Microsoft](#), according to its transparency report, this accounts for more than 26% of requests for which no data is provided in the U.S.; Microsoft simply doesn't have any responsive data to provide.

In addition, the government agency may try to use the process where there is no "emergency involving danger of death or serious physical injury to any person". Service providers take seriously their obligation to protect their users' privacy. It unfortunately appears to be the case that some law enforcement make emergency disclosure requests because it is easier than getting legal process, with the checks that come with it, even though legal process is available in a timely manner. It's not unusual, when we turn down an emergency request because of the lack of a life or limb emergency, that we receive legal process shortly thereafter.

By granting providers the right to disclose when they believe there is such an emergency, but not an obligation to disclose when the authorities assert there is, we help ensure that law enforcement uses legal process as the preferred means to obtain user data, and the emergency

process only in true exigent circumstances.

Delay in securing legal process should not be an issue. In every judicial district, a search warrant is a telephone call away. [Rule 41\(d\)\(3\)](#) permits a magistrate to respond to a telephonic request for a warrant any time, including after-hours where it is inconvenient to go to court or in an exigent situation where time is of the essence or evidence could be lost. Governmental entities avail themselves of this option and consequently obtain user data in a timely manner when exigent circumstances exist.

Finally, in 2010, the [Inspector General of the Department of Justice](#), in a report concerning the FBI's use of exigent letters and other informal requests to obtain certain customer records on an emergency basis, concluded that the abuses found made it "critical for the Department and Congress to consider appropriate controls on any use by the FBI of its authority to obtain records voluntarily...." Legislation that would require service providers to disclose the content of users' communications or customer records upon the mere assertion of an emergency would have the opposite effect, wholly stripping service providers of any discretion to ensure that the emergency authority under ECPA is utilized appropriately and subject to reasonable checks and balances.

Time Limits

Some law enforcement officials propose imposing rigid time limits for providers to respond to legal process issued under ECPA. Judges, however, routinely prescribe deadlines for compliance that are tailored to the exigencies and gravity of particular cases, as well as the need for the underlying evidence. It is unclear why such a proposal is necessary or why Congress is in a better position to manage the individual dockets of judges that oversee cases. Presumably it is because some law enforcement officials believe that providers covered under ECPA do not comply quickly enough with legal process. But courts, not legislatures, are better positioned to determine compliance deadlines in particular cases based on the needs of law enforcement and the underlying facts of such cases.

Statutorily prescribing time limits in a manner that is divorced from the context of individual cases would have unintended consequences that likely redound to the detriment of law enforcement. If there is an arbitrary deadline to produce, with penalties for late production, service providers will be compelled to focus on older requests, even when law enforcement agencies might want service providers to focus on more recent requests that have greater urgency.

A rigid time limit would significantly weaken the flexibility that covered service providers currently have to address emergency requests, diverting their attention instead to the longest outstanding requests, even if there is far less urgency attached to such requests. Service providers

that now expedite emergency requests from law enforcement in the absence of a rigid statutory timeframe for production would be constrained to do so in the future if they faced penalties for failing to comply with an arbitrary time limits codified under ECPA. Flexibility, not rigidity, is key for triaging unexpected volume, particularly when it relates to emergency requests.

An artificial and arbitrary time limit for production would also reduce the ability of service providers to verify the validity of legal process. There are more than ten thousand agencies that have subpoena power in the U.S. alone, and it is a challenge to make sure that any particular demand is valid. This is not just a theoretical concern. We do receive fake legal process designed to trick us into releasing user information. Current law enables providers to scrutinize and validate legal process, and, as a result, providers are able to identify fraudulent activity and report it to authorities.

Slow response rates can be attributable to factors that are beyond the control of service providers. For example, when Google receives legal process that is overbroad, vague, or ambiguous, that will invariably slow our response time. Moreover, a single legal request can ask for information covering multiple products and concern multiple account holders, which obviously increases the time and resources necessary to respond. Finally, law enforcement agencies often demand nondisclosure to users without proper nondisclosure orders. That, too, leads to delay. There is no responsible way to codify a statutory time limit to respond.

Proposals to impose time limits pursuant to ECPA legal process should also consider the significant increase in concomitant demands that service providers receive. Since 2009, government requests for user data issued to Google in criminal matters in the U.S. alone has [increased 179%](#). Such proposals should also account for the [explosive growth in demands for location information](#) that wireless carriers and other providers are receiving from law enforcement.

Compelled Consent

Some agencies also recommend that Congress amend the voluntary disclosure provision under [18 U.S.C. 2702\(b\)\(3\)](#) to require providers to disclose content with the consent of users. While this proposal may have intuitive surface appeal, there are important practical considerations that militate against adoption.

First, if the government obtains the consent of a user to disclose content, the providers are an unnecessary and inefficient conduit for disclosing this content. As noted above, providers are poorly situated to determine relevance and applicable privileges (including the attorney-privileged material), even assuming the user has actually consented. Providers should not be discovery agents for civil agencies under circumstances where users have consented to providing content. Civil agencies can obtain content directly from targets or witnesses if they obtain consent.

Second, Congress should be wary of proposals that would presume or deem consent based on unavailability, death, minor status, or other circumstances where users have not provided actual consent. Nor should consent be presumed or deemed given merely because the target or witness of an investigation did not respond to a legal request. As mentioned above, civil agencies have a broad array of tools in their arsenal in the event that uncooperative or intransigent witnesses fail to respond to legitimate requests for information.

Third, authenticating users and verifying consent is not always simple. Providers “authenticate” their users through the account information provided, and if a user confirms receipt of the authentication request, a provider is entitled to rely on it. That process is time-consuming, labor-intensive and often results in more questions than answers as users “object” to production or ask about the nature of inquiry. If a user doesn’t respond, or for example, if a user is locked out of her account, service providers may rely on other factors to authenticate users, some of which may not always be useful proxies for verifying identity. Moreover, even if a user consents to provide content pursuant to legal process, there may be others (including joint account holders) whose consent may be required. But all of this is an unnecessary burden because users should be required in the first instance to comply with their discovery obligations without entangling service providers.

Direct Notice

S. 356 requires law enforcement agencies to provide notice directly to a subscriber or customer of a provider within ten business days of receiving communications content pursuant to the issuance of a warrant. Direct notice is a core privacy protection in S. 356 that must be preserved. Absent direct notice, users may not have a meaningful opportunity to challenge the legality of the warrant in a criminal proceeding. Moreover, absent direct notice, users may not have the opportunity to assert relevant legal privileges or challenge the breadth of information that may be sought. In the physical world, of course, notice of a warrant is direct and palpable at the time of execution.

Notably, S. 356 allows law enforcement agencies to delay notification to users under ECPA in some cases. Specifically, it allows governmental entities to seek initial delays of up to 180 days if notification to a user would lead to an adverse result, and governmental entities can seek an extension of this delay for an additional 180 days to the extent an adverse result would persist. In light of these generous delay provisions to accommodate situations where an adverse result might occur, it is critical to preserve direct notification provisions that afford users a meaningful opportunity to challenge warrants that may violate the Fourth Amendment.

* * * * *

It is axiomatic that 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 commensurate manner to other papers and effects stored in the home, which are protected 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.



Statement of Chris Calabrese
 Vice President, Policy
 Center for Democracy & Technology

Hearing before the U.S. Senate Judiciary Committee on "Reforming the
 Electronic Communications Privacy Act"

September 16, 2015

Chairman Grassley, Ranking Member Leahy, and members of the Committee:

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology 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 (ECPA) and urge the committee to speedily pass S.356, "Electronic Communications Privacy Act Amendments Act of 2015."

Every day, whistleblowers reach out to journalists (and members of this Committee), advocates plan protests against government 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 always kept up.

The foundational value that ECPA reform seeks to uphold, as embodied by S.356, is the right to privacy for the content of our communications, even as technology evolves. In the face of an outdated statute, the courts have stepped in, creating key legal precedents and strong limits on access. 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. Reform efforts also face a concerted assault from civil agencies that seek to use statutory changes as a tool to gain new powers.

The Committee has consistently sought to solve these problems through strong reform measures, passing legislation nearly identical to S.356 in both 2012 and 2013. CDT continues to believe that a legislative solution – passage of S.356 – is the best way to advance a modest but critical privacy protection.



Support for privacy reform is deep and abiding. More than one hundred technology companies, trade associations, and public interests groups have signed onto ECPA reform principles.¹ 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 also enjoys widespread support, with more than 290 cosponsors – including a majority of Republicans and Democrats.

The Need for Reform

In 1986, when ECPA was written, few Americans owned computers and even fewer used email. Hard drives were small. Service providers offered little storage capacity and the storage they did sell was expensive. The World Wide Web didn't exist. Neither did cloud computing or broadband or social media or smartphones. The little data that was stored was kept on local computers.

Obviously that is not the world we live in today. Decades after the beginning of the Internet Age we store a vast array of sensitive communications with third parties – emails, text messages, work documents, pictures of our children, and love letters. Under ECPA they receive widely varying degrees of protection – most of which are inadequate and out of touch with consumer expectations.

These changes in technology – the rise of remote storage and cloud computing, the digitization of almost all communication – have two main implications for ECPA. First, they create serious inconsistencies in how similar communications are treated and the reasonable expectation of privacy they deserve. Second, they have disrupted the fundamental balance created in ECPA between privacy rights, law enforcement interests and the needs of innovators.

An Inconsistent Law

It can be helpful in understanding the conflicting standards and illogical distinctions that plague the current statute by considering the technological reality at the time of the passage of ECPA.

In 1986, Congress created two categories of providers and accorded users of those services different levels of protection. Legislators defined an electronic

¹ *About the Issue: ECPA Reform*, DIGITAL DUE PROCESS, <http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E0200C296BA163>.



communications service (ECS) as “any service which provides to users thereof the ability to send or receive wire or electronic communications.”² It was aimed at protecting the nascent use of email. Today, ECSs typically include any service that allows users to communicate with each other whether by email, text message, social network or other means. Under ECPA, those communications are protected by a warrant for the first 180 days after they are sent and are thereafter accessible with a subpoena. That 180-day rule is an outdated reflection of the fact that in 1986 hard drive capacity was incredibly expensive and no one contemplated long-term storage. The assumption was that if a user left an email on a server that long, it was abandoned and merited a lower privacy protection.

The second category of service under ECPA is a remote computing service (RCS), defined as “the provision to the public of computer storage or processing services by means of an electronic communications system.”³ Today, this would likely cover a cloud-based service accessed solely by an individual user, such as a Dropbox account. Under ECPA, RCSs receive only the protection of a subpoena. In 1986, RCSs tended to be major companies handling data for other major companies. As such, records in RCS storage appeared more like business records, and hence lawmakers granted them subpoena protections.

These distinctions make little sense today. Emails and other content are stored indefinitely and data held by RCSs are clearly as private as those by ECSs. It is often hard to glean in which category a particular service belongs. If a user stores a document remotely so she can later edit the document, does it move from RCS to ECS storage when she permits others to edit it as well? It also leads to wildly uneven results. The same communication could be protected by a warrant if stored on a home computer, a subpoena when stored as draft in an inbox, a Title III super warrant when in transit, a warrant for the first 180 days in an inbox and then a subpoena after that.⁴

Further, this one distinction only scratches the surface of the confusion over ECPA. Even basic questions over what type of stored records ECPA applies to can be confusing, given the limited definition of electronic storage. Nor does the statute contain basic protections like a suppression remedy for illegally obtained information or reporting requirements for how often communications are shared with the government.

² 18 U.S.C. § 2510(15) (2012).

³ *Id.* at § 2711(2).

⁴ Orin S. Kerr, *A User’s Guide to the Stored Communications Act and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).



These problems have not gone unnoticed. Starting in 2007, CDT began working through its Digital Privacy and Security Working Group (“DPSWG”) to find common ground on a solution to some of ECPA’s problems. In 2010, we announced the formation of the Digital Due Process (DDP) coalition, consisting of nine companies and twelve trade associations, think tanks and advocacy groups. DDP supported four key principles for reforming ECPA – one of which was the warrant for content fix at the heart of S.356. DDP has blossomed today into a broad coalition of more than a hundred groups and companies, including major technology companies, advocacy organizations from the right and the left and grassroots organizations representing millions of members.⁵

Congress has recognized the need for reform, as well. This Committee held a hearing on the issue in 2010 and voted out of committee legislation either identical or similar to S.356 in both 2012 and 2013. The House of Representatives has also weighed in. The companion bill to S.356, H.R. 699, “The Email Privacy Act,” is the most cosponsored bill in the House with more than 290 cosponsors including a majority of both the Republican and Democratic caucus.

The federal courts and the tech industry have also attempted to fill the void left by the lack of reform. In 2003, in *Theofel v. Farey-Jones*, the Ninth Circuit clarified confusion in the statute regarding when an email was in electronic storage and rejected the Justice Department’s distinction between opened and unopened e-mail.⁶ Most significantly, in 2010, in *U.S. v. Warshak*, the Sixth Circuit ruled that people have a reasonable expectation of privacy in email content and that it should only be accessed with a search warrant.⁷

The *Warshak* decision was a watershed. While it technically only applied in the Sixth Circuit, the difficulty in determining where a particular user was located and the persuasiveness of the court’s reasoning led most, if not all, major technology companies to adopt a warrant standard for all stored content. Even more significantly, it cast into question the constitutionality of a significant portion of the statute and made the need for reform even more urgent.

⁵ For a full list, see *Who We Are*, DIGITAL DUE PROCESS, <http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B45500C296BA163>.

⁶ *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003).

⁷ *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).



The Balance in ECPA

At the time of its passage, the goal of ECPA was to preserve “a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement,”⁸ and to support the development and use of new types of technologies and services.⁹ Congress wanted to encourage the innovation represented by these new technologies and realized that would not be possible if the privacy of users was not protected.¹⁰

ECPA accomplished that goal by creating a familiar framework – a high level of protection for the content of communication and a lower protection for business records or abandoned communications. Notably, this framework was prescient in recognizing that 3rd parties could and would hold sensitive information that merited warrant protection.

Since this initial balance was struck, we have seen a technological revolution and the result has been a statute that is now much less protective of privacy and hinders innovation.

A short (and probably incomplete) list of the communications content that I store with third parties today includes:

- Work and personal email,
- Text messages,
- More than a decade of photographs,
- All of my music,
- My passwords to all my online accounts,
- Social networking posts – many of which are shared with very few people,
- My notes – both personal and work,
- All of my personal contacts,
- My calendar,
- Hundreds of books, and
- Home videos and movies.

The striking thing about this list is how pedestrian it is. Most Americans could create a similar list; some would likely be able to add many more categories. Yet all of this is protected under a legal framework that is dramatically out of date.

⁸ H.R. REP. NO. 99-647, at 19 (1986).

⁹ S. REP. NO. 99-541, at 5 (1986) (noting that legal uncertainty over the privacy status of new forms of communications “may unnecessarily discourage potential customers from using innovative communications systems”).

¹⁰ *Id.*; H.R. REP. NO. 99-647, at 19.



Protections are largely reliant on a handful of court decisions and strong government access policies from technology companies.

The need for reform of ECPA to support innovation is equally striking. This Committee is familiar with the importance of cloud computing. Businesses all over the world are looking to cloud-based services for their information management needs in order to save money on equipment and to achieve better computing reliability and data security. Cloud-based services allow companies to expand their computing capacity quickly, which is particularly valuable for start-up businesses and entrepreneurs. Such services give employees the flexibility to share information and collaborate. The global software as services market is expected to reach \$106 billion by next year.¹¹ American companies have been the global leaders in this area, and it has been an engine for U.S.-based innovation, economic growth and job creation.

Currently, ECPA does not provide a solid legal foundation to continue this growth. When businesses contract out to cloud providers, there is a strong argument under ECPA that those cloud providers are offering the services of an RCS and hence the information they store is only protected by a subpoena. Contrast that with the full protection of a warrant offered when someone saves information on her own personal computer. As Fred Humphries, Vice President of U.S. Government Affairs at Microsoft said, "Our goal is simple: the law should treat data stored in the cloud as closely as possible to data that we previously stored in our homes or in our offices."¹²

At the same time, law enforcement's ability to collect information has grown astronomically. It's not just access to the content of communication. Everything we do online – and increasingly offline through our mobile devices – also produces metadata. Our location, with whom we are communicating, our friends and social networks – all of it is accessible to law enforcement under a variety of legal standards, most of which are lower than a warrant backed by probable cause. While increased protections for metadata are not part of S.356, it is important to keep this cornucopia of new information in mind when considering any reform effort. The reality is that we currently live in a golden age of surveillance where the government has access to copious amounts of

¹¹ Louis Columbus, *Roundup of Cloud Computing Forecasts and Market Estimates, 2015*, FORBES (Jan. 24, 2015), <http://www.forbes.com/sites/louiscolombus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/>.

¹² Microsoft Corporate Blogs, *A day of action to demand ECPA reform*, MICROSOFT (Dec. 5, 2013), <http://blogs.microsoft.com/on-the-issues/2013/12/05/a-day-of-action-to-demand-ecpa-reform/>.



information about all of us. S.356 is just a level set in one area, returning privacy protections to the content of communications while we continue to see erosions in many others.¹³

Law enforcement has not denied the need for reform in this area. At a hearing earlier this year, FBI Director James Comey said about ECPA, "There is an outdated distinction. For email, over 180 days, I think, under the 1980s statute is treated as something that you could in theory obtain without a search warrant. We don't treat it that way. We go get a search warrant from a Federal judge no matter how old it is. So a change wouldn't have any effect on our practice."¹⁴ Similarly, in a past hearing on reforming the ECPA, the Department of Justice agreed "that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened."¹⁵ Given this acknowledgement that a problem exists – and the reality that there is a constitutional infirmity in the statute protecting all stored communications – it is frustrating that some in law enforcement continue to resist commonsense reform.

The Legislation

The "Electronic Communications Privacy Act Amendments Act" (S.356) does not fix all the problems described above, but it does remedy the constitutional infirmity identified by *Warshak* and provide a strong, consistent and easily administered legal protection for the content of communications.

The key to the protections in S.356 can be found in Section 3. It amends ECPA so that the disclosure of the content of email and other electronic communications by an ECS or RCS is subject to one clear legal standard – a search warrant issued based on a showing of probable cause. The provision eliminates the confusing and outdated "180-day" rule. Section 3 also requires that

¹³ For more on the golden age of surveillance, see Peter Swire, *Going Dark or a Golden Age for Surveillance?*, CDT.ORG (Nov. 28, 2011), <https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/>.

¹⁴ *Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary*, 113th Cong. 69 (2014) (statement of the Hon. James B. Comey, Director, Federal Bureau of Investigation).

¹⁵ *ECPA Part 1: Lawful Access to Stored Content: Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Elana Tyrangiel, Acting Assistant of Attorney General, Department of Justice Office of Legal Policy).



the government notify the individual within either 3 or 10 days if their information was disclosed.

Section 3 also reaffirms current law to clarify that the government may use an administrative or grand jury subpoena in order to obtain certain kinds of electronic communication records from a service provider, including a customer's name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

Lastly, the section contains a rule of construction regarding government access to internal corporate email. It states that nothing in the bill precludes the government from using a subpoena to obtain email and other electronic communications directly from a company when the communications are to or from an officer, agent or employee of a company.

Section 4 permits delayed notice under the same standard as current law. A court may extend the delay periods for a period of up to an additional 180 or 90 days at a time (depending on whether an investigation is criminal or civil). Law enforcement may also obtain an order barring providers from disclosing the existence of a warrant.

S.356 also grants new authority to assist government investigations. In cases where there has been a delay, Section 4 requires that service providers notify the government in advance when that time period expires and they intend to notify a customer about the warrant. Current law requires no such advance notice. The purpose of this provision is to ensure that the government has an opportunity to protect the integrity of its investigation and, if warranted, to ask a court to delay the notification, before such notice is given. It also doubles the period for which notice to a user of law enforcement access to communications content can be delayed. Finally, it adds civil discovery subpoenas to the list of subpoenas that can be used to compel disclosure of subscriber identifying information, placing all subpoenas on the same footing

S.356 is also noteworthy for what it does not do. It does not impact national security powers under the Foreign Intelligence Surveillance Act – a rule of construction in Section 6 makes this clear. It does not affect the traditional exceptions that allow law enforcement to access communications without a warrant – exigency, consent and the other exceptions found in 18 USC 2702. Nor does it interfere with the existing process that allows providers to work with the National Center for Missing and Exploited Children to identify and help prosecute child pornography under 18 USC 2258A.



This simple change to the law – treating searches of an individual’s inbox the same way we treat searches of her home – is profoundly important to personal privacy and American business while not unduly interfering with law enforcement’s ability to protect public safety.

Issues of Special Note

Opponents of S.356 have identified two areas of concern – access by civil agencies and the handling of emergencies. I will address each in turn.

Civil Investigation Carve Out

In a letter to this Committee in April 2013, the Chair of the Securities and Exchange Commission (SEC) stated that a warrant requirement would block the SEC from obtaining digital content from service providers.¹⁶ The SEC is a civil agency and lacks authority to issue warrants, relying instead on subpoenas for investigations. The SEC argued that ECPA reform should allow civil agencies to obtain digital content from service providers without a warrant. However, the SEC’s request for new authority is unnecessary and troubling.

The scope of this request is very broad. While the SEC has only requested that all federal civil law enforcement agencies be granted the power to compel emails and other content from service providers, ECPA’s provisions have always applied to all government – including state and local agencies.¹⁷ But even if this authority was somehow limited to federal agencies, it would mean that the Internal Revenue Service (IRS), Environmental Protection Agency (EPA), Consumer Financial Protection Bureau (CFPB), and potentially many more agencies would have a new authority to demand a target’s emails from service providers without going directly to the target of an investigation.

An effective and time-honored method to access these types of communications in civil investigations already exists. Civil agencies can already obtain digital content with a subpoena issued directly to the target of the investigation – such as a user who sent or received emails. Civil agencies can enforce these subpoenas on individuals in court, and courts can order the user to disclose the data sought under the subpoena.¹⁸ In addition, ECPA already allows civil

¹⁶ See Letter from the Hon. Mary Jo White, Chair, Securities and Exchange Comm’n, to Sen. Patrick Leahy, Chair, Sen. Judiciary Comm. (Apr. 24, 2013), available at <https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf>.

¹⁷ See *id.* at 3.

¹⁸ See, e.g., *FTC v. Sterling Precious Metals, LLC*, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013).



agencies to issue preservation orders – without court approval – that direct service providers to prevent deletion of information from a user’s account, thereby preventing destruction or alteration of evidence, while a motion to compel is being pursued.¹⁹ ECPA reform would not change any of these existing powers for civil agencies.

In reality, what the SEC is seeking is a new authority. The SEC Chair recently testified that the agency does not obtain digital content from service providers.²⁰ The SEC has also provided no evidence – despite repeated requests – that it has ever sought content from service providers since the *U.S. v. Warshak* in 2010.²¹

If granted, the authority the SEC seeks would result in a significant erosion of privacy. There are many more potential violations of civil law than criminal law – creating more potential predicates to investigate an individual. If civil agencies are empowered to serve subpoenas on service providers for a target’s communications, the service provider may disclose the target’s entire account – often years of email communications. This would most likely include information that is irrelevant to the agency’s investigation, as well as information that is protected under the target’s attorney-client or other privilege, since the service provider would not filter out this information. Finally information gathered as part of a civil process could be shared for use in a parallel criminal investigation – creating a major backdoor to the protections in the bill.²²

¹⁹ 18 U.S.C. § 2703(f). Evidence preservation orders can be issued at early stages of an agency’s inquiry, even before launching a formal investigation.

²⁰ Dustin Volz, *SEC Reveals It Doesn’t Use Email Snooping Power It Defends*, NAT’L J. (Apr. 16, 2015), <http://www.nationaljournal.com/tech/sec-reveals-it-doesn-t-use-email-snooping-power-it-defends-20150416>.

²¹ See Letter from the Center for Democracy & Technology et al. to the Hon. Mary Jo White, Chair, Securities and Exchange Comm’n 2 (Apr. 9, 2014), available at <https://cdt.org/files/2014/04/SEC-ECPA-reform.pdf>.

²² For example, Form 1662 of the Securities and Exchange Commission, which is designed to be used with all SEC civil subpoenas, expressly states:

The Commission often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors. There is a likelihood that information supplied by you will be made available to such agencies where appropriate. Whether or not the Commission makes its files available to other governmental agencies is, in general, a confidential matter between the Commission and such other governmental agencies.

SECURITIES AND EXCHANGE COMMISSION, SEC 1662 (09-14), <http://www.sec.gov/about/forms/sec1662.pdf>.



Rather than granting civil agencies a new authority to subpoena service providers, Congress could instead clarify and codify agencies' power to obtain digital content from targets. This would be consistent with the principle of technology neutrality – civil agencies can use courts to force targets to respond to subpoenas for digital content stored in the "cloud," just as they can with content stored on a computer hard drive or physical documents stored in a safe.

Changing Rules for Emergency Exceptions

Under ECPA, electronic communications providers cannot give content and sensitive user information to the government absent a court order, subpoena or warrant. However, the law does contain an exception so that in an emergency situation involving danger of death or serious bodily harm, the provider may disclose content and user records to law enforcement absent the legal process that would otherwise be required.²³ Because these requests receive no independent judicial oversight, providers have discretion to assess whether the request is proper and should be fulfilled absent the required legal process. As ECPA reform legislation continues to gather strong support, some have called for a new provision that would change this rule to mandate compliance with any emergency request for user data or content. Such a change is unnecessary, and would raise significant privacy and security problems.

Although most emergency requests are appropriate and receive speedy compliance, there are enough instances where requests are deemed improper that misuse of the emergency authority should not be ignored. Providers' authority to evaluate the legitimacy of these requests is a crucial check against this type of abuse. For example, in 2014, Google rejected 94 out of 342 requests.

The government has previously abused its ability to engage in emergency requests. A 2010 Department of Justice Inspector General report stated that the Inspector General "found repeated misuses of [the FBI's] statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions."²⁴ Based on this, the Inspector General report recommended Congress consider "appropriate controls" on the FBI's ability to obtain records in emergency situations. With mandatory compliance and no judicial oversight, such abuses could become more frequent.

²³ See 18 U.S.C. §§ 2702(b)(8), (c)(4).

²⁴ See OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 268 (Jan. 2010), available at <https://oig.justice.gov/special/s1001r.pdf>.



Right now, emergency requests are very rare. America's largest Internet and electronic communications companies only receive a small number of requests. For example, Google only received 342 emergency requests²⁵ and Microsoft only received 475 requests²⁶ throughout all of 2014. In comparison, Google received 20,280 subpoenas and search warrants and Microsoft received 12,364 similar requests during that same year.

In the event that a provider denies a request for an emergency disclosure without legal process, the government still has options available. Law enforcement can revise its request to obtain content or data if appropriate justification has not been provided. Additionally, government entities may also seek information through ECPA's mandatory disclosure provisions without delay. In all judicial districts, a magistrate is available for after-hours requests that require immediate action, and Rule 41 of the Federal Rules of Criminal Procedure stipulates for telephonic search warrants to be obtained at all hours.

Requiring providers to comply with any emergency request would also endanger data security by interfering with providers' ability to assess the validity of requests. Data thieves regularly attempt to take customer information by posing as law enforcement and demanding that data be provided pursuant to an emergency. Congress criminalized this activity because of the serious threat it poses.²⁷ Providers must have the capability to ensure that requests are not fraudulent and prevent disclosure of user data to unauthorized third parties. Mandating disclosure in response to all emergency requests and removing discretion to appeal for clarification, additional information, or a more secure method of disclosure would undercut providers' ability to protect users' sensitive information.

The current system for disclosure of user information and content pursuant to emergency requests absent a court order works effectively. It protects both public safety and user privacy and security, and should not be changed. Providers take seriously both safety needs and their users' privacy rights. Voluntary disclosure that assesses government requests allows them to effectively protect both.

²⁵ See *Google Transparency Report: Security and Privacy*, GOOGLE, <http://www.google.com/transparencyreport/userdatarequests/US/>.

²⁶ See *Microsoft Law Enforcement Requests Report*, MICROSOFT, <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>.

²⁷ See 18 U.S.C. § 1039 (2012).



We thank the Committee for holding a hearing on this important issue and urge you to act swiftly to mark-up S.356, "Electronic Communications Privacy Act Amendments Act of 2015."



Hearing on

“Reforming the Electronic Communications Privacy Act”

United States Senate Committee on the Judiciary

September 16, 2015

Washington, DC

**Testimony of Victoria Espinel
President and CEO
BSA | The Software Alliance**

Testimony of Victoria Espinel
President and CEO, BSA | The Software Alliance
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015
Washington, DC

Good morning Chairman Grassley, Ranking Member Leahy, and members of the Committee. My name is Victoria Espinel, and I appreciate the opportunity to testify today on behalf of BSA | The Software Alliance (“BSA”). BSA is the leading advocate for the software industry in the United States and around the world.¹

BSA members have a keen interest in today’s hearing on “Reforming the Electronic Communications Act.” We support efforts to update ECPA, and urge this Committee to advance legislation that would better reflect today’s technology. Importantly, updating ECPA would remove outdated distinctions in the law that provide lower levels of legal protections for digital communications.

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. That result would have damaging implications for general productivity and the continuing growth of the digital economy.

The bipartisan ECPA Amendments Act, introduced by Senators Lee and Leahy, improves the trust equation between providers and customers by: 1) protecting email communications from government intrusion without a warrant; and 2) providing clarity to technology companies on their legal obligations to law enforcement, so that providers can be transparent with their customers about how they treat their customers’ stored content.

We are generating an enormous amount of data every day – just think: more than 90 percent of the world’s data was created in the past two years² – but the policy environment tied to data services has not kept pace with this increased use or technological progress. The protections for this 21st century world of data services rest on a framework of 20th century law. Because the law has not kept pace, consumers, businesses and law enforcement all lack sufficient clarity and predictability about the regulations and laws that govern the gathering, storing, sharing, and beneficial use of data.

As the data services sector continues its rapid growth, crucial issues have emerged that will affect its future, such as government access to information, cybersecurity, trade rules and cross-border data flows. Uncertainty over these issues will only continue to grow as time passes and technology evolves, with important implications at home and abroad. In order to realize the full beneficial potential of these data services, and in order to reach the best possible decisions, we must have clear rules.

Congress must update ECPA to bring the law in line with industry practices that have been adopted to protect the constitutional interests of our customers. Many of these reforms are so non-controversial that

¹ BSA’s members include: Adobe, Altium, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

² IBM, *What is big data?*, at: <http://www.ibm.com/software/data/bigdata/what-is-big-data.html>.

even today's federal government witnesses accept their wisdom. But these reforms should not be weakened by other changes that would force software companies and other digital service providers to be put in the middle of disputes between the government and the targets of civil investigations.

In addition, BSA members believe that Congress should address issues emerging now, specifically those related to demands by law enforcement agencies in one country for data held in another country. This issue has significant implications for our law enforcement and privacy interests, and for the global competitiveness of our digital services sector. The issue is thoughtfully addressed in the bipartisan Law Enforcement Access to Data Stored Abroad (or LEADS) Act, introduced by Senators Hatch, Coons, and Heller and co-sponsored by a bipartisan group of 12 senators.

Software and the Economy

The commercial software industry is one of the world's most powerful engines of economic growth, with global software revenue exceeding \$407 billion in 2013.³ That was a 4.8 percent increase from 2012 revenue of \$388.5 billion and significantly higher than the global GDP growth rate of 3.4 percent.⁴ The software industry also generates millions of high-quality, high-paying jobs – with a median salary that far exceeds the national average, and a growth rate that should make it the second-fastest growing U.S. industry sector over the next few years.⁶

But the true impact of the software industry is much more difficult to measure. This is because software is creating entirely new opportunities for growth. Consider, for example, one type of software: apps. That industry is expected to grow from \$11 billion in 2014 to \$77 billion in 2017.⁷ And the just-emerging data analytics market, which relies on software to gather and analyze once-incomprehensible datasets, will reach \$125 billion worldwide by 2015.⁸

Software also increasingly enables everything we do and is revolutionizing every other market sector. From financial services and health care to education and entertainment, software generates even greater economic returns through its use by customers because it enables businesses and individuals across the economy to become more efficient, productive, and competitive, and because it provides them with the tools for further innovation.

But the promise of that growth is not guaranteed. In fact, if our laws do not continue to grow with our technology, the global competitiveness and growth of the US software industry will suffer.

³ Gartner, *Gartner Says Worldwide Software Market Grew 4.8 Percent in 2013*, available at <http://www.gartner.com/newsroom/id/2696317>

⁴ *Id.*

⁵ International Monetary Fund, *World Economic Outlook Database*, http://www.imf.org/external/pubs/ft/weo/2015/01/weodata/weorept.aspx?pr.x=28&pr.y=2&sy=2006&ey=2015&scsm=1&ssd=1&sort=country&ds=.&br=1&c=001%2C110%2C163%2C200&s=NGDP_RPCH&grp=1&a=1

⁶ See BSA, *Powering the Digital Economy: A Trade Agenda to Drive Growth* (2014), at http://digitaltrade.bsa.org/pdfs/DTA_study_en.pdf.

⁷ Entrepreneur, *By 2017, the App Market Will Be a \$77 Billion Industry*, (Aug. 26, 2014), at <http://www.entrepreneur.com/article/236832>.

⁸ Forbes, *Big data and analytics market will reach \$125 billion worldwide in 2015* (Dec. 11, 2014) <http://www.forbes.com/sites/gilpress/2014/12/11/6-predictions-for-the-125-billion-big-data-analytics-market-in-2015/>

The Trust Equation

Americans in every corner of our country, and in every facet of our personal and working lives, rely on digital technologies and the Internet. Reflecting this fact, the software industry is in the midst of a transformation. Our industry is changing from an industry that sells a product in a box to one that provides a range of data-driven services to our customers – customers who could be anywhere in the world. This shift means that an increasing amount of sensitive data – from an individual user’s personal correspondence to corporate communications – is held by our companies on behalf of their customers.

This new technological dynamic is built on a foundation of trust: individuals and small companies will take advantage of the convenience of global, always-on services from a software company that holds *and protects* data. Those users must trust that our companies will guard their data with the best possible security and protect it from unlawful access – by anyone.

If consumers and companies do not trust that their data will be safe, they will be reluctant to take advantage of such software-enabled services. They will lose out on the cost savings and tremendous efficiencies that cloud computing can provide, all of which harms our global competitiveness.

That trust is currently being challenged by a range of factors, including the misperception that US law enforcement has unfettered access to the data held in US companies’ data centers. In order to restore and maintain customer trust, BSA members believe Congress must update US privacy laws, particularly the Electronic Communications Privacy Act of 1986 (“ECPA”).

BSA Supports the ECPA Amendments Act

BSA supports S. 356, the ECPA Amendments Act. We thank Senator Lee and Senator Leahy for introducing this bipartisan, bicameral legislation to modernize the current framework for law enforcement access to electronic communications in a manner that strengthens privacy protection while ensuring the needs of law enforcement are met. And we thank Senators Cornyn, Blumenthal, Coons, Franken, Vitter, Durbin, and Cruz, all members of this Committee who have cosponsored this important legislation.

We have been working alongside CDT and the other members of the Digital Due Process coalition almost from its inception. For more than five years, we have worked to close the loophole that allows access to email without a warrant based on the law’s outdated conceptions of technology. When ECPA was enacted, the high cost of computer storage meant that email users who wanted to “archive” an electronic communication needed to print it out and file it in a desk drawer.⁹ The thought of an inbox with years’ worth of sensitive personal communication was simply inconceivable. It made a certain amount of sense for Congress to draw a line at 180 days and consider email older than that as “abandoned” and allow law enforcement access with something less than a warrant.

Today, ending this warrant exception is at the core of the ECPA reform conversation, and the ECPA Amendments Act is much-needed legislation that will help ensure continued user trust in digital services. The ECPA Amendments Act requires the Government to obtain a warrant for **all** electronic content and clarifies rules regarding notice to customers, so that companies can be transparent about privacy protections.

BSA supports the ECPA Amendments Act because consumers, businesses and governments all will benefit from greater clarity in the law about the appropriate ways for law enforcement to access data. Just

⁹ In doing so, it should be noted, such an “archived email” again enjoyed the protection of the warrant requirement by being placed in a drawer rather than disappearing deeper into a virtual inbox.

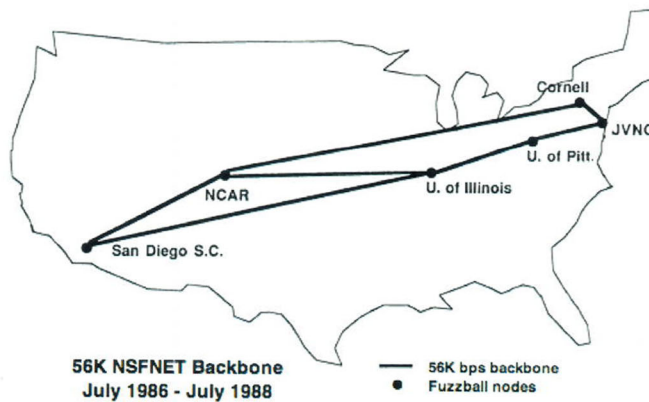
as the Government must show a warrant to an individual when it searches her home, the Government should show an individual a warrant authorizing a search of her email.

These “core ECPA reforms” are essential. Unfortunately, more than five years after we began the Digital Due Process effort, additional unanticipated consequences flowing from ECPA’s age have emerged.

The Need to Address Cross-Border Data Requests

Today, in addition to ECPA’s lack of a clear, consistent warrant requirement for access to data, it has become clear that the law provides no guidance for handling law enforcement data requests that cross borders. US law enforcement is increasingly using US process to gain access to information that is held outside the United States regardless of whether it is stored on behalf of customers in the United States.

Why did ECPA not anticipate or provide for law enforcement access of content stored abroad? It is helpful in this regard to remember that the “Internet,” as we know it today, looked much different in the 1980s. In fact, today’s globe-spanning network looked something like this:



Not only did ECPA not consider a world where vast amounts of data could be stored for mere pennies, it also did not imagine a worldwide network of connected computers and devices. The thought of being able to communicate in real time from our phones to nearly any place on earth was barely even the stuff of science fiction. The ECPA of that time did not consider that one day major US service providers would have customers in countries all around the world, or that they would be storing years’ worth of their communications in data centers in a whole range of locations. Today, as one social media company portrays it, the Internet looks something more like this:



Source: <https://www.facebook.com/notes/facebook-engineering/visualizing-friendships/469716398919>

Today's Internet, clearly, is a much different network. Now, a person can log on to a computer in London in order to access their email, which is held by a US company on a server in Ireland, in order to email their family here in Washington. The network transcends borders. And while the Internet may easily reach across borders, the case is not the same for US laws.

Such an approach would never be acceptable in the offline world. Consider, for example, if the Justice Department were seeking evidence that was being held in a safe in a Marriott in London. The FBI would never serve a warrant on Marriott's headquarters in Maryland, demand that their employees send someone into the room, take pictures of the items in the safe, and send them back to Washington. Such a search would be seen as an incredible affront to British sovereignty.

This not only threatens the trust that our international customers place in us to protect their data. It also forces US software companies to choose between violating ECPA by refusing a US demand or breaking the law of the country in which the data is held. This is true even though there is a system for access to evidence held overseas – the Mutual Legal Assistance Treaty (MLAT).

BSA Supports the LEADS Act

BSA and its member companies support the bipartisan, bicameral LEADS Act to address this issue. We thank Senators Hatch, Coons, and Heller for introducing S. 512, and Senator Vitter and the other nine Senators who have cosponsored it.

As proposed by Senator Hatch, the LEADS Act creates a clear framework for access to data stored abroad. Warrants can only be used within the territory of the United States. LEADS recognizes that law enforcement has a legitimate need to obtain the content of electronic communications relating to US persons even when the data is stored abroad. LEADS therefore authorizes an ECPA warrant to be used for data stored abroad if the warrant seeks the content of a US customer. If the data of a non-US person is

stored abroad, then US law enforcement would coordinate with foreign law enforcement agencies to obtain the data, just as it would in the physical world.

One way that is done is through an MLAT.

MLATs create frameworks that allow a law enforcement agency in one country to obtain evidence located in another. The LEADS Act will improve and modernize the MLAT process. If the customer is not a US person, law enforcement can still obtain the data in a number of ways, including through the MLAT process. LEADS would require updates to the MLAT process to improve efficiency and transparency.

BSA supports the creating an international framework to address this issue. We believe the LEADS Act is a good way to accomplish this. Creating that framework will protect Americans' privacy by setting strong international standards. 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.

Further, the international framework that LEADS creates is critical to the international competitiveness of US technology providers. BSA member companies are at a competitive disadvantage when competing for customers abroad if foreign customers believe US law enforcement will be able to access their information stored in their own country.

Finally, the LEADS Act also would prevent providers of data services from being put in the position of having to violate one country's law or another's when served with a US warrant for data of a foreign customer stored outside the United States.

Action in the Courts: A Call for Congressional Action.

The misperception that US law enforcement agencies have unfettered access to data is exactly that – a misperception. But that misperception and the harm it is doing to user trust in software-enabled solutions is real.

Already, amid the ongoing international surveillance revelations, European governments and businesses are openly questioning the trustworthiness of US technology companies. The German government, for example, has crafted procurement rules that will bar many US companies from providing software solutions and services to the state. And the German government is not stopping there. They are sending signals to the private sector that industry should follow regulators' lead. But Germany is not the only example. Brazil, Nigeria, Russia, China are among the countries taking similar steps.

Perhaps most damaging to customer trust are real examples of US law enforcement trying to obtain data without using the proper channels. A case argued in the Second Circuit Court of Appeals in New York last week has the potential to set a significant precedent. In that case, the Department of Justice is seeking to force Microsoft to turn over the contents of one customer's email inbox. In the United States, such a demand requires a warrant, and the Department of Justice has successfully obtained a warrant for the information Microsoft holds here in the United States.

The problem in this case is this: Microsoft's customer is likely in the vicinity of the company's Dublin datacenter—where the data is stored—and which Irish law governs. In the same way that U.S. police can't simply fly to Ireland and knock down a suspect's door to raid their home, their jurisdiction online must be respectful of borders as well. Barging into an Irish data center, however it's done, would be an incredible invasion of Irish sovereignty. And imagine the uproar if foreign police tried such a move in the United States.

Instead, through a long-standing and well-developed process, many countries have developed rules for obtaining access to information that is held overseas. Those rules are embodied in Mutual Legal Assistance Treaties, or MLATs, and the United States even has an MLAT with Ireland. The Irish government has filed a brief in the 2nd Circuit case letting the court know that, had the Justice Department used the MLAT process, they would already have the information that they will be in court this week to seek.

Rather than using that MLAT process, however, the Justice Department is misguidedly arguing that a user's email belongs not to the user -- but to the email provider. This flies in the face of what digital customers the world over believe about owning their own online files and communications, and it runs contrary to generations of understanding about the privacy of our papers and letters.

Consider the United States Postal Service: would the Justice Department ever try to argue that the contents of your envelopes no longer belong to you once they are dropped in the mail? They wouldn't, and that is the bedrock of the years of trust between customers and the companies and institutions we all rely on to deliver our communications.

Rather than taking this battle to the courts, we urge the Justice Department to work with governments and industry around the world to craft a forward-looking system to address these questions. The goal should be a system of rules that both preserves the rule of law and applies effectively across borders. If the United States does not take a lead in guiding this process, we will be left instead with countries racing to establish a system with the fewest protections possible. Such a regime would neither respect international sovereignty nor fundamental human rights or online privacy. As the digital economy continues to grow, our world will only continue to shrink. Already some online crime is global. The tools that law enforcement uses to investigate and prosecute such crime should be global as well.

That effort should begin here in Congress, with ECPA reform. As Judge Lynch noted in his concluding remarks, "It would be helpful if Congress would engage in that kind of nuanced regulation."

In the coming weeks and months, the court must wrestle with these issues itself. But the judges in the case already have made at least one determination: Congress needs to act.

**Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

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 ECPA, and various ways of doing so. The Committee’s last hearing on the topic was four and a half 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 provide the government with a means to access those communications and related records in certain circumstances. However, dramatic changes in the use of communications technology have occurred since then.

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 communications 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 the like. 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 the requirements of 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’s more than 180 days old, or whether it’s 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 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 on a timely basis.

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 in 2011, if we are considering changing the legal standards under ECPA, we should also “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 the 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 couldn't agree more. I'm grateful for the presence of all the witnesses here today and look forward to their testimony. I now recognize Senator Leahy for his opening statement.

**Statement Of Senator Patrick Leahy (D-Vt.),
Ranking Member, Senate Committee On The Judiciary
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

Congress passed the Electronic Communications Privacy Act twenty-nine years ago, when most Americans communicated on land lines, when call waiting was novel, and when few had heard of email. Yet Congress anticipated that the new world of electronic communications would need privacy protections. ECPA provided just that.

Since 1986, technology companies have continued to create new ways of communicating. But the privacy rules governing this critical area 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.

But we do not expect our private letters or photos stored at home to lose Fourth Amendment protection simply because they are more than six months old. Neither should our emails, texts, or other documents we store in the cloud. If I send Senator Grassley a birthday note tomorrow, its long-term constitutional protection should not depend on whether I give him a card that he puts in his desk, or send him a text that is stored in the cloud.

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, including nine members of this committee. In the House, a supermajority of nearly 300 cosponsors supports this bill. An extraordinary coalition of industry and civil society supports this bill, led by Americans for Tax Reform, the Center for Democracy and Technology, Heritage Action, and the ACLU. This bill has been reported from the Judiciary Committee by voice vote in each of the last two Congresses. Passing this bill is – to use a technical term – 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 legitimate warrant exception. The ECPA Amendments Act simply 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 they must abide by the same constitutional constraints that apply to everyone else. They have not been able to obtain emails without a warrant because of the 2010 federal court ruling, and our bill would not alter that status quo.

I look forward to hearing from all the witnesses who have been invited this morning. 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 focusing on this important issue. I urge him to move this legislation through committee, as we have done twice in the last four years.

#####

Senate Committee on the Judiciary
Questions for the Record from Senator Grassley
To: Elana Tyrangiel
Principal Deputy Assistant, Office of Legal Policy
U.S. Department of Justice

1. In your statement for the record, you described a series of types of cases that would be affected if the Department's civil regulators and litigators had no mechanism to compel the disclosure of content from providers—including civil rights enforcement, false claims act actions, and environmental litigation. Can you describe these scenarios in more detail, including how often these types of cases arise?
2. Please cite case law and any other legal authority that supports the Department's position that so long as notice and an opportunity to be heard is provided to the subscriber, it is lawful and Constitutional to compel the disclosure of electronic communications content from a provider through a subpoena, as opposed to a warrant.
3. Please describe any concerns the Department has about the notice provisions in S. 356, the Electronic Communications Privacy Act Amendments Act of 2015.
4. If a U.S. provider chose to store data outside the United States, the LEADS Act would make it harder for the Department to gather evidence against individuals in the United States illegally than against U.S. citizens. That seems backwards—and it's possible then, that LEADS could act as a kind of get-out-of-jail free card for individuals here illegally. Can you expand upon the Department's concerns about the LEADS Act you referenced in your statement for the record?
5. Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses, and/or anything else you did not have a chance to respond to that was discussed at the hearing.

**Senate Committee on the Judiciary
“Reforming the Electronic Communications Privacy Act”**

Questions for the Record: Senator Amy Klobuchar

1) *Question for Ms. Tyrangiel*

Currently in the law, there is a line between communications older than 180 days, requiring a search warrant for newer communications and only a subpoena for older communications.

- Is there a justifiable reason to distinguish the amount of protection based upon the age of communications, or is this an outdated standard in need of reform?

2) *Questions for Ms. Tyrangiel and Mr. Littlehale*

The Justice Department, and in particular the Federal Bureau of Investigations (FBI), often works in concert with local law enforcement.

- How can we enhance cooperation between law enforcement at the federal level?
- Are there notable differences in the collection of electronic information through ECPA at the federal level compared to the local level? If so, what can be done to ensure uniform processes for all law enforcement agencies?

**Written Questions of Senator Patrick Leahy,
Ranking Member, Senate Committee On The Judiciary
For Elana Tyrangiel
Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of
Justice
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

1. You testified that it no longer makes sense to provide less privacy protection to emails that are more than 180 days old and to emails that have been opened. The Electronic Communications Privacy Act currently requires the government to obtain a warrant before compelling the disclosure of email less than 180 days old. 18 U.S.C. § 2703(a). Is the Department seeking the authority in civil investigations to obtain email, regardless of age, from providers without a warrant?
2. Because the cost of electronic storage has plummeted over the past two decades, service providers now store years of email or other documents for their customers. The full contents of an email account could reveal an enormous amount of information about an individual – much of which may be entirely irrelevant to the investigation. Please explain the process that is undertaken when the Department of Justice obtains a warrant for the contents of an individual’s stored electronic communications from a third-party service provider. Please also explain the process used when, prior to the *Warshak* decision, the Department of Justice used a subpoena to obtain the contents of an individual’s stored electronic communications from a third-party service provider. In particular, please answer the following questions for both the criminal and civil contexts:
 - a. Does the Department often obtain the entire contents of the email account? Are these requests limited by date range or other factors? If so, how often?
 - b. How is the information received from service providers stored, and who has access to it?
 - c. How is this data searched or sorted for relevance to the pending investigation?
 - d. What controls are in place to protect the security of this information?
 - e. Is the information that is deemed irrelevant to the investigation deleted? If so, when?
3. In a prior committee markup of the ECPA Amendments Act, the Judiciary Committee added a provision making clear that agencies can continue to issue subpoenas to corporations for the contents of their employees’ email. This recognizes that corporations do not have the same privacy interests as individuals. How important is this corporate email provision to the Department?

**Written Questions of Senator Patrick Leahy,
Ranking Member, Senate Committee On The Judiciary
For Chris Calabrese
Vice President, Policy, Center for Democracy & Technology
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

1. In its testimony, the SEC asked Congress for the authority to obtain the contents of electronic communications from third-party service providers without a warrant. How do you respond to this proposal? What are the implications of requiring providers to go into their users’ accounts to look for and produce communications and documents that are responsive to a civil investigation?

The Center for Democracy & Technology (CDT) believes a warrant is the “gold standard” for privacy protection in the U.S., which is why it is embedded in the Fourth Amendment of our Constitution. The most invasive kind of searches, such as a search of your home or your personal belongings (including your letters), must generally be conducted with a warrant rather than an instrument that requires a lower standard of review. The warrant itself is very narrow in scope: the government must prove to a judge or magistrate that there is probable cause to believe that specific evidence related to a crime is currently in the specified place to be searched. Other places and items, unless in plain view during the search, cannot be touched.

One of the most troubling parts of the SEC proposal is that it does not specify the standard that must be met before conducting a search. Instead, the SEC testimony talks about allowing subjects of the order to “raise with a court any privilege, relevancy, or other concerns” (pg. 5). These are issues raised in relation to a subpoena, which suggests the subpoena standard is the standard the SEC would want to use if its proposal were implemented.

If agencies are able to use something substantially the same as the subpoena standard, the government would only need to prove that the customer records sought are relevant to an investigation. Because it requires such a low standard of review, the subpoena is by far the easiest instrument for the government to use. It is also the broadest in scope, because a large number of communications can be considered “relevant” to an investigation.

This problem is compounded by the fact that the predicate to begin a civil investigation is much broader than a criminal investigation. Simply put, many more actions are violations of civil law versus criminal law. For example, under the SEC’s proposal, the government could obtain personal electronic communications relevant to misfiling your tax returns or violating the health code. In addition to this problem, subpoenas can also be directed not only at people subject to the investigation, but also to any witnesses with relevant information.

Worst of all – this authority is both unnecessary and likely unconstitutional. As the Committee knows, a 2010 appellate court decision, *US v. Warshak*, made clear that email content enjoys a reasonable expectation of privacy under the Constitution, and the proper authority for accessing such content is, therefore, a warrant. Both the SEC and the FTC admitted in the hearing that

since *Warshak*, neither has tried to use subpoenas to access email content. Despite not accessing such content, they still managed to conduct robust investigations.

The SEC proposal amounts to an unconstitutional solution to a nonexistent problem – one aimed at getting an unprecedented level of access to Americans’ email inboxes. Such a proposal would represent a serious invasion of privacy and raise major concerns for CDT and other privacy and civil liberties organizations.

**Written Questions of Senator Mike Lee
For Chris Calabrese
Vice President, Policy, Center for Democracy & Technology
Hearing on “Reforming the Electronic Communications Privacy Act”
September 16, 2015**

1. The ECPA Amendments Act and its House companion, the Email Privacy Act, have enjoyed incredible support from members of Congress and from all walks of the private sector. Over 290 members of the House and 24 Senators have cosponsored the bills. The bills have the support of privacy advocates, civil libertarians, former prosecutors, Fortune 500 companies, small businesses, and startups. And more than 100,000 Americans have signed a petition urging the White House to support ECPA reform.

- Why has this bill and this movement garnered such tremendous support?

The reasons for that support are straightforward. The first is that privacy is immensely popular. Polls demonstrate that an overwhelming majority of Americans support the change – more than 84 percent in a poll of key states. In an age where more and more personal information is held by third parties, and government intrusions such as those by the National Security Agency are rampant, people want legal protections that assure them that their personal information is safe and won’t be arbitrarily accessed by the government.

Second, this is a commonsense reform that provides meaningful change without being radical. Searches conducted using a warrant are well understood and enshrined in the Constitution. Law enforcement officials are very familiar with warrants, and they can be quickly attained. The bill also represents a fairly straightforward advancement of privacy into the 21st century. It is logical that a letter and an email should enjoy the same protections, and these protections are what Americans expect and deserve for their electronic communications.

Third, in many ways the bill already represents the status quo. Many police – including entities like the FBI – already obtain search warrants before accessing the contents of communications. Similarly, many large providers follow the *Warshak* decision and demand a warrant before turning over content.

In sum, the public, the courts, law enforcement and companies have all settled on a warrant standard. It is simply up to the Senate to do the same.

Support for reform continues to build in the House. As of October 8, 2015, more than 300 members of the House have cosponsored ECPA reform legislation.

2. During the last panel, some of the agencies expressed a need to compel disclosure from a service provider in circumstances in which they are unable to get information directly from the target.
 - Why would a system that allows direct subpoenas to service providers be problematic from a privacy standpoint and how would it effect the efforts for email privacy reform?

[Please note – the response to the question is identical to our response to Senator Leahy’s similar question.]

The Center for Democracy & Technology (CDT) believes a warrant is the “gold standard” for privacy protection in the U.S., which is why it is embedded in the Fourth Amendment of our Constitution. The most invasive kind of searches, such as a search of your home or your personal belongings (including your letters), must generally be conducted with a warrant rather than an instrument that requires a lower standard of review. The warrant itself is very narrow in scope: the government must prove to a judge or magistrate that there is probable cause to believe that specific evidence related to a crime is currently in the specified place to be searched. Other places and items, unless in plain view during the search, cannot be touched.

One of the most troubling parts of the SEC proposal is that it does not specify the standard that must be met before conducting a search. Instead, the SEC testimony talks about allowing subjects of the order to “raise with a court any privilege, relevancy, or other concerns” (pg. 5). These are issues raised in relation to a subpoena, which suggests the subpoena standard is the standard the SEC would want to use if its proposal were implemented.

If agencies are able to use something substantially the same as the subpoena standard, the government would only need to prove that the customer records sought are relevant to an investigation. Because it requires such a low standard of review, the subpoena is by far the easiest instrument for the government to use. It is also the broadest in scope, because a large number of communications can be considered “relevant” to an investigation.

This problem is compounded by the fact that the predicate to begin a civil investigation is much broader than a criminal investigation. Simply put, many more actions are violations of civil law versus criminal law. For example, under the SEC’s proposal, the government could obtain personal electronic communications relevant to misfiling your tax returns or violating the health code. In addition to this problem, subpoenas can also be directed not only at people subject to the investigation, but also to any witnesses with relevant information.

Worst of all – this authority is both unnecessary and likely unconstitutional. As the Committee knows, a 2010 appellate court decision, *US v. Warshak*, made clear that email content enjoys a reasonable expectation of privacy under the Constitution, and the proper authority for accessing such content is, therefore, a warrant. Both the SEC and the FTC admitted in the hearing that since *Warshak*, neither has tried to use subpoenas to access email content. Despite not accessing such content, they still managed to conduct robust investigations.

The SEC proposal amounts to an unconstitutional solution to a nonexistent problem – one aimed at getting an unprecedented level of access to Americans’ email inboxes. Such a proposal would represent a serious invasion of privacy and raise major concerns for CDT and other privacy and civil liberties organizations.

3. When we use a service provider like Google to manage our email, we put our private communications in the hands of a third party.

- In what ways are email and cloud computing different from bank records or other business records that enjoy less privacy protection under current law?

Email and the content of communications held in cloud computing storage are very different than business records. The first and most obvious difference is the vast scope of email and other communications. While business records certainly contain information that is worthy of a high level of privacy protection, email services and other cloud storage sites contain documentation of a user’s entire life. As I mentioned in my testimony, my personal information held in cloud storage includes:

- Work and personal email,
- Text messages,
- More than a decade of photographs,
- All of my music,
- My passwords to all my online accounts,
- Social networking posts – many of which are shared with very few people,
- My notes – both personal and work,
- All of my personal contacts,
- My calendar,
- Hundreds of books, and
- Home videos and movies.

This is vastly more information than what is found in any business record. These accounts are also under my control. I am the sole creator of the content. I can decide what to keep or delete, whom to share files with, and how to access them. Business records, by contrast, are created throughout the course of a service or transaction, and are used to make those services or transactions possible. They are under the control of the business, and the user often has little, if anything, to do with their content or creation.

Email and similar technologies also play a crucial role in preserving constitutional rights. Americans' ability to organize protests, act as whistleblowers to the press, petition the government, and protest government wrongdoing are enshrined in the First Amendment. Today, such activities are all largely conducted electronically. The role that electronic communications play in society today is similar to the role that letters and phone calls have played in the past. That is part of the reason why courts have found that Americans' use of these technologies enjoys a reasonable expectation of privacy under the Fourth Amendment.

Senate Committee on the Judiciary
Questions for the Record from Senator Grassley
To: Andrew Ceresney
Director, Division of Enforcement
U.S. Securities and Exchange Commission

1. **In your statement for the record, you described a series of types of cases that would be affected if the Commission lacks a mechanism to compel the disclosure of content from providers—including securities law violations, Ponzi schemes, and other fraud enforcement actions. Can you describe these, and other, scenarios in more detail, including how often these types of enforcement actions arise?**

Response:

There are a number of scenarios where the authority to obtain electronic communications from an internet service provider (ISP) is critical to the SEC's ability to investigate wrongdoing and protect investors from fraud and other misconduct affecting the financial markets. Many of the SEC's investigations involve instances where the individual from whom we are seeking documents – often the person being investigated – no longer possesses or can no longer retrieve (or claims the lack of possession or ability to retrieve) electronic communications because the individual deleted the communications, has damaged hardware, or otherwise is unable or unwilling to access and produce them.¹ In other instances, the SEC may not be able to subpoena relevant electronic communications directly from an individual because he or she lives in, or may have fled to, a foreign jurisdiction. In each of these scenarios, if there is no mechanism for the SEC to compel the disclosure of content from ISPs, the SEC would be unable to obtain otherwise responsive electronic communications relevant to its investigations.

While these scenarios may arise in any of the SEC's investigations, they are most likely to occur in investigations involving individual actors or non-regulated entities.² In such cases, emails or other electronic communications stored at an ISP³ are likely to be more relevant and parties are more likely to be uncooperative in their document productions (and not having a way to obtain such emails would further incentivize them to be uncooperative). As to the specific types of cases that would be most affected, they include offering frauds such as Ponzi schemes and pyramid schemes,⁴ market manipulation cases such as "pump and dumps,"⁵ and insider trading

¹ In these situations, efforts to enforce a subpoena against the individual to obtain the communications will often be ineffective, particularly if the individual is aware we cannot get the information from an ISP. Under the current language of the bill, even in instances where an individual claims to have produced all relevant electronic communications in his possession but we have learned from other witnesses that there are additional electronic communications, we often would be unable to establish that the individual has the communications in his possession and therefore did not fully comply with the subpoena.

² Regulated entities have significant document retention obligations under the federal securities laws and, as a general matter, the SEC is more likely to be able to obtain relevant electronic communications directly from the regulated entity in investigations involving these entities.

³ These include relevant emails sent and received from personal email accounts or email accounts set up for business purposes, as well as email accounts set up by wrongdoers for use in fraudulent schemes.

cases. These schemes are often perpetrated by individual actors and often victimize the elderly or other vulnerable retail investors. Protecting these investors through enforcement actions is crucial to the SEC's mission and these kinds of cases account for a significant portion of the SEC's enforcement activity each year.⁶

2. Please cite case law and any other legal authority that supports the Commission's position that so long as notice and an opportunity to be heard is provided to the subscriber, it is lawful and Constitutional to compel the disclosure of electronic communications content from a provider through a subpoena, as opposed to a warrant.

Response:

When assessing the constitutionality of obtaining electronic communications content from a provider through a subpoena, the law of the land is the Supreme Court's recent decision in *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), which makes clear that the Fourth Amendment does not require a warrant before obtaining content from a subscriber or a subscriber's ISP. In *Patel*, the Supreme Court affirmed its long-standing precedent that obtaining information through a subpoena is constitutional if the subpoenaed party is "afforded an opportunity to obtain precompliance review before a neutral decisionmaker." *Id.* at 2452, citing *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) and *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 545 (1967). The Court discussed at length the constitutionality of the administrative subpoena process, explaining that it allows a subpoenaed party to "move to quash the subpoena before any search takes place," at which point a neutral decisionmaker "would then review the subpoenaed party's objections before deciding whether the subpoena is enforceable." *Id.* at 2453. The Court noted that "[p]rocedures along these lines are ubiquitous" and confirmed that they are constitutional. *Id.* at 2453–54. While *Patel* is a 5-4 decision – the majority concluded that the city ordinance at issue was unconstitutional precisely because it did not afford an opportunity for precompliance review – all nine Justices confirmed the constitutionality of obtaining information through administrative subpoenas when there is opportunity for precompliance review.

⁴ Generally speaking, an offering fraud involves a security that is offered to the public, where the nature of the security or terms of the offer are materially misrepresented. The offerings, which can be made online, may make misrepresentations about the likelihood of a return or of the use of proceeds. Other online offerings may not involve material misrepresentations, but may nonetheless fail to comply with the registration provisions of the federal securities laws.

⁵ "Pump-and-dump" schemes involve the touting of a company's stock (typically microcap companies) through false and misleading statements to the marketplace. In these schemes, promoters first try to boost the price of a stock with false or misleading statements about the company. These schemes often occur on the Internet where it is common to see messages urging readers to buy a stock quickly. After "pumping" the price of the stock up, fraudsters seek to profit by selling, or "dumping," their holdings of the stock into the market. Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose money.

⁶ For example, in FY2014, the SEC brought actions stopping Ponzi and pyramid schemes that had raised more than \$2 billion from investors, filed more than 60 actions involving market manipulation schemes, and charged more than 85 individuals and entities with insider trading violations.

Subscribers receive – and have in the past received – notice and an opportunity to challenge a Commission subpoena to an electronic communications provider before any materials are turned over, which is the process all nine Supreme Court Justices deemed constitutional in *Patel*. Indeed, from a privacy perspective, this process, in some ways, is preferable to the process for obtaining a warrant. While a court may issue a warrant after an *ex parte* proceeding in which the subscriber does not participate, a court may compel compliance with a subpoena only after a contested proceeding in which the subscriber may participate.

While significant focus has been placed on the ruling in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), which is the decision of just one court of appeals, the *Warshak* case did not involve an administrative subpoena in which the procedures described in *Patel* were followed but instead involved a grand jury subpoena. More specifically, the subscriber in *Warshak* did not receive notice or an opportunity to appear before a neutral decisionmaker before the emails were turned over by the provider. Of the few courts that have cited *Warshak*'s Fourth Amendment holding, none has applied it to administrative subpoenas, which is not surprising since *Warshak* does not discuss them. But to the extent its holding could be construed to cover administrative subpoenas, *Patel* would now control.⁷

3. Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses and/or anything else you did not have a chance to respond to that was discussed at the hearing.

Response:

As I stated in my testimony, the SEC agrees that modernizing ECPA makes sense and fully appreciates the important privacy interests. Our goal is simply – but crucially – to preserve a mechanism for the SEC to obtain electronic communications from ISPs in certain limited circumstances as part of its civil enforcement of the federal securities laws, while also recognizing the privacy interests implicated. Towards that end, there are a few points I would like to highlight for members of the Committee as they consider the Electronic Communications Privacy Act Amendments Act of 2015 (S.356).

The content of electronic communications is extremely important in SEC investigations. Electronic communications among individuals often provides critical evidence in SEC enforcement matters. Access to the content of electronic communications enables the SEC to obtain direct and powerful evidence of wrongdoing that is unavailable by other means, particularly against individuals, who, time and again, put detailed information about misconduct in their emails and, time and again, have deleted their emails, claimed damaged hardware or fled the country.

As currently drafted, S.356 would require government entities to procure a criminal warrant in order to obtain the content of electronic communications from an ISP. Because the SEC is a civil law enforcement agency, it cannot obtain criminal warrants. Thus, if S.356 is

⁷ On May 26, 2011, then Attorney General Holder sent a letter to multiple Members of Congress indicating that the government believed *Warshak* was wrongly decided.

passed in its current form, the SEC will be unable to obtain evidence critical to its investigations even in situations where we know the subscriber deleted or failed to produce his emails or fled the jurisdiction and we believe that the ISP has the communications. This would create an unprecedented digital shelter for electronic communications that does not exist for paper documents and that would allow wrongdoers to shield an entire category of probative evidence from civil law enforcement. Such a harmful effect on law enforcement would assist wrongdoers, harm the public, and is not necessary to advance privacy protections.

There are various ways to modernize ECPA that protect individual subscriber privacy and fully comport with the Constitution without frustrating legitimate law enforcement. As noted in my testimony, the Committee could amend ECPA to include language that would: (1) require civil law enforcement agencies to attempt, where possible, to seek electronic communications directly from a subscriber first before seeking them from an ISP; and (2) should seeking them from an ISP be necessary, give the subscriber or customer notice and the opportunity to challenge the request in a judicial proceeding. If the legislation were so structured, an individual would have the ability to raise any privilege, relevancy, or other objections with a court before the communications were provided by an ISP, while civil law enforcement would still maintain a limited avenue to access existing electronic communications in appropriate circumstances from ISPs. Such a proceeding – which would require the SEC to obtain an order from the same federal courts that would decide whether to issue a criminal warrant – would offer protections not available to subscribers subject to a warranted search, who receive no advance notice and have no opportunity to be heard by a judge before communications may be required to be provided.⁸

One important point that was not discussed at the hearing is that in its current form, S.356 would endanger the SEC's ability to obtain critical evidence even in cases where an individual's privacy interests are not at issue because the individual has consented to the release of their electronic communications. There have been multiple instances since the *Warshak* decision where ISPs have resisted SEC subpoenas for the contents of electronic communications even though the subscriber had consented to the ISP providing the information to the SEC, in which case there is no privacy interest implicated. Under the proposed amendment, the SEC would likely be unable to require the ISP to provide the electronic communications even where they are undisputedly relevant to the SEC's investigation or in situations where the subscriber has consented to their production. Such an outcome would obviously unnecessarily impede the SEC's ability to investigate and uncover wrongdoing without protecting any individual subscribers' privacy interests.

In sum, amending ECPA so that a criminal warrant is required in all cases would unquestionably harm the ability of the SEC to uncover financial fraud and other unlawful conduct. While updating ECPA to enhance privacy protections is appropriate, there are multiple ways to do it that comport with the Constitution and address privacy and other interests without unnecessarily undermining civil law enforcement. We would welcome the opportunity to work with Congress to update ECPA in a way that strikes an appropriate balance between privacy and law-enforcement interests.

⁸ To be clear, such a proceeding would not authorize the SEC or its representatives to enter private property and take documents or other records. A court order compelling compliance with a request for electronic communications under this procedure would simply require the ISP to produce the communications to the SEC.

Written Questions of Senator Patrick Leahy,
 Ranking Member, Senate Committee On The Judiciary
 For Andrew Ceresney
 Director, Division of Enforcement, U.S. Securities Exchange Commission
 Hearing on “Reforming the Electronic Communications Privacy Act”
 September 16, 2015

1. You testified that, notwithstanding *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), and its application in the Sixth Circuit, the SEC continues to believe that it has legal authority to obtain the content of an individual’s electronic communications through third-party service providers without a warrant. Despite this assertion, you also testified that the SEC has not sought to exercise that authority in the five years since *Warshak* was decided.
 - a. When was the last time that the SEC issued a subpoena to a third-party service provider for the contents of email communications?

Response:

As you note, following the Sixth Circuit’s *Warshak* decision in December 2010, the SEC refrained from exercising its ability to obtain subscriber emails from an ISP through an administrative subpoena and has continued to do so out of deference to ongoing legislative discussions about ECPA reform. Although it would be constitutional for us to obtain such emails from an ISP pursuant to a subpoena, as confirmed by the Supreme Court’s recent decision in *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), after the decision in *Warshak*, the only instances in which we have sought to do so pursuant to a subpoena are where the subscriber has consented to the production. Prior to *Warshak*, the SEC exercised its authority under ECPA to seek the contents of email communications from ISPs through administrative subpoena in appropriate cases.

- b. Please explain the legal basis for the SEC’s position that it has the authority to compel the disclosure of an individual’s electronic communications from a third-party service provider without a warrant.

Response:

The legal basis for the Commission’s position is the long line of Supreme Court precedent governing disclosure of information requested by administrative subpoenas, which clearly holds that the Fourth Amendment does not require a warrant in all circumstances, and that administrative subpoenas, which are not self-enforcing, comply with the Fourth Amendment. Indeed, the Supreme Court recently reaffirmed this black letter law in *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015). In *Patel*, the Supreme Court held that obtaining information through a subpoena is constitutional if the subpoenaed party is “afforded an opportunity to obtain precompliance review before a neutral decisionmaker.” *Id.* at 2452, citing *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) and *Camara v. Municipal Court of City and County of San*

Francisco, 387 U.S. 523, 545 (1967). The Court discussed at length the use of administrative subpoenas, which allow a subpoenaed party to “move to quash the subpoena before any search takes place,” at which point a neutral decisionmaker “would then review the subpoenaed party’s objections before deciding whether the subpoena is enforceable.” *Id.* at 2453. The Court noted that “[p]rocedures along these lines are ubiquitous,” and it confirmed that searches following the application of such procedures are constitutional. *Id.* at 2453–54. While *Patel* is a 5-4 decision, all nine Justices agreed that it was constitutional for an agency to obtain information through the use of a subpoena process that gives subpoenaed parties an opportunity to have any objections heard by a neutral decisionmaker, such as a federal judge. *Patel* did not break new ground; it reaffirmed well-established Fourth Amendment principles [which the SEC adheres to when seeking to compel compliance with its subpoenas to suspected wrongdoers].

One such principle is that the bedrock constitutional protection offered by the Fourth Amendment is a requirement that a search be reasonable. U.S. Const. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”). Reasonableness, however, does not mean that every search must occur pursuant to a warrant. *Patel*, 135 S. Ct. at 2452–53; *see also id.* at 2458 (Scalia, J., dissenting) (“[T]he only constitutional *requirement* is that a search be reasonable.”); *Florida v. Jimeno*, 500 U.S. 248, 250 (1991). *Patel* and other cases hold that searches are not unreasonable simply because they follow a subpoena, which “commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands.” *United States v. Bailey*, 228 F.3d 341, 348 (4th Cir. 2000).

Under this law, if the Commission seeks electronic communications content from a provider after being unable to obtain that content from the subscriber or through other channels, and the subscriber has notice and opportunity to challenge the subpoena before any content is turned over, the Fourth Amendment has been fully satisfied. While one court of appeals held that obtaining content was not constitutional when authorities did not obtain a warrant, that case did not involve an administrative subpoena and the subscriber did not have the opportunity to obtain precompliance review from a judge or other neutral decisionmaker. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).⁹ Imposing a warrant requirement that is applicable only to requests for electronic communications content – and that precludes civil law enforcement agencies from ever obtaining such content – distorts the Fourth Amendment and ignores established Supreme Court law that administrative subpoenas are a constitutional method of obtaining information so long as the procedures discussed in *Patel* are followed.

c. Please provide examples of specific cases in the past five years in which you have obtained the contents of email via a subpoena to the subscriber.

Response:

The staff obtains emails in almost all SEC investigations. Typically, in the case of corporate email addresses, this is accomplished by seeking relevant emails directly from the

⁹ On May 26, 2011, then Attorney General Holder sent a letter to multiple Members of Congress indicating that the government believed *Warshak* was wrongly decided.

company. If relevant emails are held in a personal email account, the staff typically will seek the relevant emails from the individual subscriber. These requests to individual subscribers regularly occur in our investigations, especially in cases involving unregulated entities. In many instances, the individual subscriber will provide emails in response to our requests and there is no need for additional action. However, if a subscriber claims that he is unable to provide relevant emails because they are no longer in his possession, or Commission staff has reason to believe that additional relevant communications exist, the staff may request that the individual consent to the relevant emails being produced by the ISP.

- d. Please provide examples of specific cases in the past five years in which you were unable to obtain the contents of email via a subpoena to the subscriber, and due to your decision not to seek contents from providers, you were unable to bring a case.**

Response:

As noted in my testimony, the SEC has refrained from seeking electronic communications from third-party providers under the administrative subpoena provisions of ECPA in recent years out of deference to ongoing legislative discussions concerning ECPA reform. Because we have not obtained such emails, and therefore have no knowledge of the contents of those emails, there is no basis for the SEC to determine whether the inability to bring a case was due to the decision not to seek the contents of the emails from providers. For similar reasons, it would be difficult to determine how many of the cases we have brought in the past few years would have been stronger or filed earlier had we been able to obtain relevant electronic communications from third-party providers. There have, however, been numerous cases in which we were unable to obtain potentially relevant electronic communications because the subscriber deleted relevant emails from their personal accounts, claimed to have damaged hardware and thus could not produce relevant emails, or fled the SEC's jurisdiction.

- 2. You testified that since *Warshak* was decided five years ago, the SEC has not sought to enforce a subpoena to a third-party service provider for the contents of email communications in deference to Congress. Will the SEC continue to “defer” to Congress until ECPA reform legislation is enacted into law?**

Response:

While the SEC has voluntarily refrained from exercising its authority to obtain electronic content of a subscriber from an ISP through an administrative subpoena absent subscriber consent out of deference to the ongoing legislative discussions about ECPA, it remains constitutional for us to do so under the current version of ECPA. It is a matter of concern for our enforcement program that we have not exercised that authority. Going forward we will continue to reassess our approach based on the needs of our Enforcement program.

3. You testified that it no longer makes sense to provide less privacy protection to emails that are more than 180 days old and to emails that have been opened. The Electronic Communications Privacy Act currently requires the government to obtain a warrant before compelling the disclosure of email less than 180 days old. 18 U.S.C. § 2703(a). Is the SEC seeking the authority in civil investigations to obtain email, regardless of age, from providers without a warrant?

Response:

The SEC agrees with the general consensus that the age of an email should not dictate the method by which the government may obtain a copy of the email.

4. Because the cost of electronic storage has plummeted over the past two decades, service providers now store years of email or other documents for their customers. The full contents of an email account could reveal an enormous amount of information about an individual – much of which may be entirely irrelevant to the investigation. Please explain the process that was undertaken when, prior to the *Warshak* decision, the SEC obtained a subpoena for the contents of an individual's stored electronic communications from a third-party service provider. In particular, please answer the following questions:
- a. Did the SEC typically obtain the entire contents of the email account? Were its requests limited by date range or other factors? If so, how often?

Response:

The SEC's information requests are designed to obtain information relevant to the investigation. Almost all requests for documents are limited by date range and other factors. Accordingly, the SEC typically did not request the "entire contents" of an email account from an ISP, except in [rare] situations in which the subscriber asked that the SEC do so to avoid the subscriber's need to conduct a relevancy review or where the entire contents of an email account were relevant to a particular investigation. Just as with subpoenas for paper documents, if an individual believed that the SEC's requests were too broad or sought information irrelevant to its investigation, the individual was provided notice and had the opportunity to raise these objections to SEC staff and, if necessary, before a neutral decisionmaker before the material was provided to the SEC.

- b. How was the information received from service providers stored, and who had access to it?

Response:

Electronic evidence obtained by the SEC is generally received in an electronic format that is designed to be imported into the discovery tools used by the staff. Access to the electronic evidence in these tools is limited to the individual members of the enforcement staff conducting the investigation.

c. How was this data searched or sorted for relevance to the pending investigation?**Response:**

The SEC uses commercially available tools to store and review evidence produced in an investigation. These tools provide various methods for searching and filtering data to reduce the overall review time and to increase the likelihood of finding relevant evidence. For example, these tools provide the ability to search by keyword, by date, and by the sending or receiving party.

d. What controls were in place to protect the security of this information?**Response:**

All SEC information technology systems are protected with multiple layers of security, both technical and process oriented. These include robust firewalls, intrusion detection and prevention systems, and access control systems, all in support of a comprehensive security management framework based off of NIST SP 800-53 rev4. Data at rest also is encrypted on all user laptops.

In every SEC investigation, the access to evidence is limited to the individual members of the enforcement staff working on the investigation. Moreover, the Division of Enforcement has adopted policies and conducts training intended to ensure that particularly sensitive data, including data that contains personal identifying information, is treated appropriately.

e. Was the information that was deemed irrelevant to the investigation deleted? If so, when?**Response:**

The Division of Enforcement is required to maintain its records consistent with a records schedule approved by the National Archives and Records Administration, and that schedule governs what investigative materials may be discarded and when. Nevertheless, the SEC staff only uses information relevant to the investigation in connection with its investigatory activities.

- 5. In a prior committee markup of the ECPA Amendments Act, the Judiciary Committee added a provision making clear that agencies can continue to issue subpoenas to corporations for the contents of their employees' email. This recognizes that corporations do not have the same privacy interests as individuals. How important is this corporate email provision to your agency?**

Response:

The SEC's ability to obtain emails from corporations by subpoena is critical to its enforcement efforts. As the primary form of business communication, emails routinely serve as a key component of the evidence reviewed by the staff during investigations and introduced as evidence in the SEC's litigated matters. That said, while a provision along the lines of what you reference would be helpful, it would not address the concerns I raised in my testimony with the proposed ECPA reform bill.

- 6. Please explain the process by which your testimony was approved by the Commission, including whether your testimony was approved by the agency's commissioners.**

Response:

The written statement I submitted to the Senate Judiciary Committee for its September 16, 2015 hearing was provided on behalf of the full Commission. The Commission approved my written statement by the Commission's seriatim process. *See* 17 C.F.R. § 200.42. Under the seriatim process, the Commission votes on a matter without convening a meeting of the five Commissioners. A matter circulated for disposition by seriatim consideration is not considered final until each SEC Commissioner reports his or her vote to the Commission's Secretary or has reported to the Secretary that the Commissioner does not intend to participate in the matter. The Commission voted unanimously to approve my written statement submitted to the committee.

Questions for the Record
Senator Mike Lee
ECPA Hearing
September 16, 2015

Andrew Ceresney, Director of Division of Enforcement, SEC

1. **In April of this year, Chair Mary Jo White testified before the House Appropriations Committee that the SEC is not issuing subpoenas to third-party service providers for content. However, in your written testimony, you suggest that you have recently obtained information from service providers without a warrant.**
 - **For clarity's sake, in the past few years, has the SEC compelled the sharing of content from a service provider with something less than a warrant?**

Response:

Following the Sixth Circuit's *Warshak* decision in December 2010, the SEC voluntarily refrained from exercising its authority to obtain subscribers' electronic communications content from an ISP through an administrative subpoena and has continued to do so out of deference to ongoing legislative discussions concerning ECPA reform. Recently the only instances in which we have sought email content from an ISP pursuant to an administrative subpoena are situations where the subscriber has provided consent, and thus no privacy interest was implicated. In some of those circumstances, the ISP has refused to produce the email content despite the consent of the subscriber. It would, however, be constitutional for us to obtain email from an ISP pursuant to an administrative subpoena under the current version of ECPA. It is a matter of concern for our enforcement program that we have not exercised that authority. Going forward we will continue to reassess our approach based on the needs of our Enforcement program.

2. **In its 2014 annual report, the SEC noted that it brought a "record number of cutting edge enforcement actions." In that same report, the SEC said that it brought "more cases than ever before," including "a number of first-ever cases that span the securities industry."**
 - **Given the "record number" of enforcement actions and "first-ever cases" brought, why is the SEC claiming that the ability to subpoena records from third-party providers is critical?**

Response:

The fact that the SEC has been successful in enforcing the securities laws and has brought a record number of enforcement actions in recent years without exercising our authority to compel the production of electronic communication content from ISPs does not mean that we would not be able to protect investors more effectively if we could do so in certain cases. This was an important tool for us pre-*Warshak*, particularly in cases such as Ponzi schemes, market

manipulation and insider trading. And while we cannot know what evidence we have been unable to obtain since we began voluntarily refraining from exercising our authority, there are current investigations that would be advanced by use of that ability, including instances where subscribers deleted relevant emails to avoid production to the SEC or fled the SEC's jurisdiction. In addition, having the authority to subpoena records from ISPs – whether or not we use it – is important, because it incentivizes individuals to comply with subpoena requests if they know that the SEC has another means of obtaining the materials should they refuse to comply or not comply in full.

3. In your testimony, you suggest that we allow the SEC, the IRS and the Consumer Financial Protection Bureau to force email providers to turn over emails as long as you ask the target of the investigation first and allow the target to object in court. In other words, if you or any of these agencies wanted to investigate me, you could read my birthday greetings to my mother, my love notes to my wife, or my correspondence with my doctor unless I hired a lawyer and appeared in court.

- **So instead of the government having the burden to establish a case, the burden is on the citizen to give reasons why his or her emails are private. Is that your agency's position?**

Response:

The SEC is seeking an appropriate mechanism for obtaining electronic communications from an ISP in instances where the communications are relevant to an investigation of wrongdoing and we are unable to obtain them from the subscriber for various reasons. There are multiple ways to modernize ECPA that would protect the legitimate privacy rights at issue and allow subscribers to raise relevancy and other objections without impairing the SEC's ability to enforce the federal securities laws and putting investors at risk. We believe providing the subscriber notice of a request and an opportunity to challenge the request in a judicial proceeding would be appropriate, as I noted in my testimony. Under such a procedure, which has been consistently reaffirmed by the Supreme Court across the decades, the burden would be on the SEC to establish that its request for the electronic communications is appropriate under a standard determined by Congress.¹⁰

The obligation placed on an individual under such a process would be no more onerous than responding to a subpoena for paper documents where similar steps are required to avoid producing documents. If the SEC serves an individual with a subpoena for paper documents that the individual believes requests irrelevant information, the individual can either, comply with the subpoena and provide the documents, ask the SEC staff to review the scope of the subpoena, ignore the subpoena and force the SEC to seek enforcement of the subpoena in a judicial proceeding, or move to quash the subpoena in a judicial proceeding. Unless accord is reached

¹⁰ The SEC's requests for documents are designed to obtain information relevant to its investigations. The SEC staff is not interested in irrelevant documents, such as birthday cards, love notes or correspondence with personal doctors, whether they are in paper or electronic format. To the extent these documents are included in the electronic communications that an ISP may provide in response to an SEC request, there are a number of ways to address this issue, including, in appropriate circumstances, allowing the subscriber to review the communications before they are provided to the SEC.

with SEC staff, an individual is required to appear at a judicial proceeding (and hire a lawyer if he chooses) in order to avoid producing the information requested.

4. Chair White testified that the SEC has not been issuing subpoenas to third party service providers, in the wake of the Sixth Circuit's ruling in 2010 that warrants are required for content.

- **If the authority to compel the production of content from third-party service providers on something less than a warrant is critical, why hasn't the SEC sought this authority from Congress before now?**

Response:

As a general matter, Section 21 of the Securities Exchange Act has provided authority for the SEC to obtain content from third-party service providers since 1934. In 1986, Congress placed certain limitations on the Commission's authority to obtain content in electronic storage from third-party service providers as part of the Electronic Communications Privacy Act. As the existing statutory structure currently provides for this authority, it was unnecessary for the SEC to seek authority it already possessed.

With respect to the recent efforts by Congress to update the Electronic Communications Privacy Act, the SEC's specific involvement began in 2013 when a bill was introduced that would strip the SEC and other civil regulatory agencies of an important enforcement tool that has historically been available to investigate potential civil violations of federal law. For the past approximately two and a half years, Chair White has sought changes to ECPA modernization bills under consideration by Congress. Specifically, in April 2013, days after being sworn in as Chair of the SEC, Chair White sent a letter to then Senate Judiciary Chairman Leahy that stated, among other things:

While I appreciate your efforts to update the privacy protections for e-mail and other electronic communications for the digital age, I am concerned that [ECPA reform] bill as currently constituted could have a significant negative impact on the Securities and Exchange Commission's enforcement efforts. For the reasons set forth below, I respectfully ask you to consider the negative impact that the legislation in its current form could have on the Commission's ability to protect investors and to assist victims of securities fraud, and would be interested in discussing with you a modest change in your proposal that would continue to address privacy concerns while also providing the Commission the authority it needs to effectively discharge its critical functions.

A copy of that letter was included in my testimony submitted to the Committee.

Since that time, Chair White has discussed ECPA-related issues both in Congressional hearings and in meetings with members of Congress in both chambers. In addition, SEC staff has provided technical assistance to multiple interested members of Congress or their staffs pursuant to requests that they received. All of these efforts have been aimed at finding an acceptable a solution that balances the need to update the protections contained in ECPA and accommodate

privacy concerns while allowing law enforcement agencies, in limited circumstances, the opportunity to obtain electronic content from third-party service providers through judicial process after first seeking the content from the individual subscribers.

- **Why haven't you attempted to take a noncompliant third-party service provider to court to compel disclosure and to get the court to uphold your interpretation of privacy rights?**

Response:

We have voluntarily declined to seek content from service providers or exercised our authority to compel compliance with a subpoena, which would initiate a contested proceeding regarding that subpoena, out of deference for the ongoing legislative discussions about ECPA reform. While we disagree with the assertions that a court order arising out of that process presents any sort of constitutional problem, we recognize that Congress has been actively considering reforming these aspects of ECPA for several years. It is a matter of concern for our enforcement program that we have not exercised our authority. Going forward we will continue to reassess our approach based on the needs of our Enforcement program.

5. **One of the major concerns you listed in your testimony was that targets of investigations will destroy emails rather than turn them over. But you already have authority under ECPA to compel providers – with no judicial process – to preserve accounts or provide backup preservation. In the second half of 2014 alone, Google received over 4,000 preservation demands affecting over 17,000 users/accounts.**

- **Why aren't preservation requests sufficient for government agencies to ensure that responsive evidence is preserved?**

Response:

The SEC's authority to require providers to preserve evidence under ECPA is significantly limited. The statute only authorizes the SEC to require an ISP to preserve electronic communications for a maximum of 180 days.¹¹ More importantly, preservation alone is not the issue. Preservation by ISPs means little if the SEC has no ability to obtain the evidence and use it in its investigations or at trial. Indeed, depriving the SEC of the ability to obtain electronic communication content from third-party service providers likely would further incentivize wrongdoers to delete or destroy relevant communications or corresponding hardware, knowing that the SEC would be unable to otherwise obtain the information.

¹¹ 18 U.S.C. § 2703(f)(2) provides that a government entity may request that a provider retain evidence for a period of 90 days, which may be extended for an additional 90 days upon a renewed request.

Questions for the Record
“Reforming the Electronic Communications Privacy Act”
September 16, 2015
Senator Sheldon Whitehouse

Mr. Andrew Ceresney

In your testimony, you stressed that the SEC’s inability to obtain the content of customer communications from third-party providers threatens to undermine the SEC’s enforcement efforts. Please provide as many examples as possible of past instances where content obtained from a third-party provider was essential evidence in an SEC investigation.

The authority to obtain electronic communications from third-party providers is critical to the SEC’s ability to investigate wrongdoing and to protect investors from fraud and other misconduct affecting the financial markets. We need this authority because fraudsters and other wrongdoers routinely use email and other electronic communications when violating the securities laws and, in some cases, delete, destroy, or refuse to provide these communications during the SEC’s investigations. In some of these cases, obtaining these communications from the third-party provider may be the only way the SEC can get this crucial evidence, particularly if the subscriber does not respond to a subpoena or flees the jurisdiction. The following examples demonstrate instances where SEC investigations significantly benefitted from an ability to obtain electronic communications directly from ISPs.

- **Insider Trading**: During an insider trading investigation, the suspected tipper produced emails pursuant to a subpoena but there appeared to be gaps in his production. As a result, with notice to the subscriber, we requested and obtained the suspect’s personal emails from the ISP under ECPA. The ISP’s subsequent production contained emails missing from the subscriber’s production, including the alleged tip, which became the centerpiece of our successful action against the tipper and tippee.
- **Market Manipulation**: In an investigation into market manipulation by a foreign stock promoter, we could not obtain emails with valuable information about the scheme because the individual lived in a foreign jurisdiction. After noticing that the company’s principals occasionally used personal email addresses for work-related communications, we subpoenaed the ISPs under ECPA (with notice to the subscriber). The resulting emails provided key communications about the fraud, including discussions establishing knowledge in planning the scheme and demonstrating control of the companies being promoted. The information was unavailable from other sources because the principals apparently used personal email addresses for certain sensitive communications regarding the scheme. In addition, the email content was unobtainable without a subpoena to the ISP because under the foreign jurisdiction’s law, we could not compel the principals to produce the information. Ultimately, we charged a variety of defendants for their roles in the scheme.

- Financial Fraud: In an action involving a scheme to artificially inflate the financial results of a public company, we obtained a key email through a subpoena to the ISP (with notice to the subscriber), which was sent after the individual had failed to produce the relevant emails for nearly a year. This evidence was particularly important because, as alleged in the complaint, the defendants carefully concealed the scheme. At the time the SEC subpoenaed the ISP, the individual had failed to produce his personal e-mail in response to a document subpoena we had issued almost a year earlier. Thus, absent the authority to subpoena the ISP directly, we likely would not have obtained this critical evidence.

In addition to past cases, there are also ongoing investigations that we believe would significantly benefit from the ability to obtain electronic communications from ISPs. These include investigations where individuals have deleted relevant emails from their personal email accounts to avoid their production to the SEC, cases where individuals have failed to produce emails from their personal accounts and refused to provide consent to obtain the communications from ISPs, and cases where individuals reside in foreign jurisdictions where we cannot subpoena their communications from them directly.

**Questions for the Record
Senator Mike Lee
ECPA Hearing
September 16, 2015**

Victoria Espinel, President and CEO, BSA – The Software Alliance

1. I appreciate the stress that companies feel while trying to balance compliance with U.S. warrants and their obligation to foreign customers. It is an important issue that should be dealt with at some point, while making sure we first secure the privacy rights of our own citizens.
 - How would an extraterritorial application of ECPA, such as what the LEADS Act contemplates, affect the privacy rights of US citizens?

Response: Today, there is no statutory basis to apply a warrant issued under ECPA extraterritorially, to reach emails stored overseas. Yet the Government has taken the position that it can use an ECPA warrant to seek emails stored abroad, regardless of whether those emails are stored on behalf of a U.S. person or a foreign national. That position jeopardizes the privacy rights of U.S. citizens, because it invites law enforcement agencies in other countries to reach into the U.S. and access emails stored here.

The LEADS Act would strengthen the privacy rights of U.S. citizens by creating a statutory framework that creates a legal basis for the U.S. Government to obtain emails stored outside of the United States, but only in limited circumstances. This sets an international precedent that law enforcement agencies should seek data stored outside their country in limited scenarios, such as when there is a sufficient nexus between their country and the subscriber whose emails they seek.

The LEADS Act also embraces other reforms to ECPA that are included in S. 699, your bipartisan ECPA Amendments Act, such as requiring a warrant for all email content regardless of its age, and requiring the Government notify a subscriber when her email is obtained with an ECPA warrant. The reforms in the ECPA Amendments Act, and the LEADS Act, greatly strengthen the privacy rights of U.S. citizens. BSA therefore supports both the ECPA Amendments Act and the LEADS Act. The bills complement each other and will improve the privacy rights of U.S. citizens and the economic opportunities of our most successful companies.

**Questions for the Record
United States Senate Committee on the Judiciary
Hearing on
“Reforming the Electronic Communications Privacy Act”**

September 16, 2015

Response of
Richard Littlehale
Assistant Special Agent in Charge
Technical Services Unit
Tennessee Bureau of Investigation

Questions of Chairman Chuck Grassley

Special Agent Littlehale, in your testimony you described the many different ways in which the current ECPA regime poses problems for state and local law enforcement. Do you have any additional, real-life examples that illustrate these problems?

Response: Let me offer two additional examples of real-world problems faced by investigators working today’s digital crime scene. I have picked two that illustrate some of the issues discussed in other questions for the record set forth below. It is worthy of note, given much of the discussion in the hearing, that in both of these cases, law enforcement obtained a search warrant, and in both cases, they were frustrated by delayed and obstructionist responses from the service providers.

Case #1: The first example illustrates the problems that law enforcement has with service providers pre-litigating the warrant, and with delayed response:

In December 2014, the police department in a large city obtained a search warrant for stored messages from a deceased victim’s account with a smartphone application provider during a capital murder investigation. The warrant called for a response within 15 days of receipt. No response was immediately forthcoming, and after a second service of the search warrant, six months after service, the investigators received a response that stated in pertinent part:

“[service provider] has additional responsive data that we can produce in a supplemental production; this data includes the contents of messages that were on [service provider’s] servers as of January 19, 2015 (the messages that are on [service provider’s] servers are limited to the messages that were not successfully delivered to the intended recipient – in this case, the target facility identified in the Search Warrant). Some of this data is responsive to this warrant (data between November 22, 2014

through December 26, 2014) but [service provider] is unable to date-limit this message content and accordingly are requesting a new or amended warrant that includes language reflecting the use of a “taint team”, a group of law enforcement’s technical experts who will review the messages and seal any content that exceeds the scope of the Warrant.

An example of this language is:

Law enforcement personnel will review the information stored in the accounts and files received from [service provider] employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant as specified. Law enforcement personnel will then seal the original duplicate of the accounts and files received from [service provider] employees and will not further review the original duplicate absent an order of the Court.

The law enforcement agency refused to seek a fresh warrant and asked the prosecutor to intervene by threatening legal action. Only at that point did law enforcement receive the proceeds the original warrant sought.

Here, after a delay of six months, the service provider acknowledges that they have additional evidence that is responsive to the warrant, but refuses to provide it unless law enforcement obtains a new warrant setting forth a complicated review procedure identified by the service provider, all so that the service provider doesn’t have to take the time to separate evidence from non-responsive data themselves. The decision of whether or not to employ a taint team rests properly with law enforcement in consultation with the prosecution, not with a company that holds evidence. If law enforcement should have employed a taint team and did not, the defense will have ample opportunity to raise the issue if criminal charges are brought. This type of pre-litigation of warrants is precisely the sort of burden that lengthens investigative timelines and complicates the job of investigators unnecessarily.

Case #2: This is another example of non-compliance, pre-litigation of the warrant, combative responses, and in this case, an absurd demand that law enforcement supply precisely the information that law enforcement was seeking in order to narrow their request:

A law enforcement agency investigating a murder that occurred in December 2014 identified a pre-paid smartphone in May 2015 as being relevant to the case. Investigators needed to identify an unknown person who was associated with a telephone number that was associated with the phone. A judge issued a search warrant calling for the smartphone manufacturer/cloud service provider to provide subscriber information for a specific telephone number for a single month.

The service provider responded that the telephone number was associated with multiple customer accounts, and requested the relevant “account email address, or full name and telephone number, and/or full name and physical address of the

subject [account].” The investigators responded that they could not provide the requested information because that was precisely the information that they were seeking in order to identify their unknown user, and asked the provider to comply with the original warrant, stating:

“If there is more than one subscriber, then provide information for all subscribers associated with phone number xxx-xxx-xxxx, from December 1, 2014, through December 31, 2014. This is not an unreasonable request and we expect [service provider] to comply with the search warrant – as is.”

The service provider responded:

We have reexamined this matter. However, we have not been in a position to provide you with account information due to the fact that there is not enough account identifying information provided in your warrant. In this regard we are not in the position to identify any account based solely on the telephone number due to the potential number of accounts pertaining. We need an individual's full name, physical address and/or email address in addition to the telephone number in order to identify any account which may be associated with the individual in question. Further, your warrant does not provide us with any information which will assist in identifying any account which may be associated with this individual. If you would be kind of to provide us with either a name, email address and/or physical address for the individual who is the subject of this warrant. We will conduct searches to establish if there is an account associated with these details, and if so provide the results to you. We trust this clarifies the position for you at this time and we look forward to receiving the further identifying details from you should you be kind enough to provide them.

Here, the service provider admits to having responsive information... in other words, the compliance personnel can see multiple accounts associated with the telephone number in question. Despite being in possession of this evidence, the provider has decided that it will not provide the range of subscribers that have used the number in question, because law enforcement’s request is not specific enough to identify a particular subscriber. The provider renews their insistence that law enforcement provide precisely the information that law enforcement does not have in order to receive the evidence called for in the warrant.

Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses, and/or anything else you did not have a chance to respond to that was discussed at the hearing.

Response: One term that I heard repeated in the hearing was a familiar assertion of those who insist that law enforcement has all the access to evidence we need: that we

live in the “golden age of surveillance,” when law enforcement has access to an endless buffet of data. I certainly agree that a steadily increasing amount of evidence relevant to any criminal investigation exists in the digital world, and that digital evidence can be of enormous value to investigations. It is also true, however, that we now have access to less and less of that evidence; we are allowed to look at the buffet, but even with a search warrant in hand, all too often, we go hungry.

Imagine a person who wishes to communicate with another person without the government having access, and wants to exchange pictures and other materials and keep those private as well. Fifty years ago, those communications would be subject to interception on any available means of communication available to the public, and any enciphering of the information would have had to be manual and subject to decryption by experts. A cache of pictures could be buried in the woods, locked up in a bank, or hidden behind a false wall, but would be subject to discovery by a diligent enough search. Now, that person can put all of those communications and materials on a mobile device that fits in a pocket, and if the person chooses the device carefully, they can give the device to the police for a week with the expectation that their secrets – or the evidence of their criminal conduct – cannot be accessed.

That sounds more like the Golden Age of Privacy to me. If we continue to allow technological advancement without any consideration of the importance of collecting digital evidence in criminal investigations, it will place law enforcement at an unprecedented disadvantage in gathering the evidence we need to do the job the public expects us to do.

Questions of Senator Mike Lee

1. **Mr. Littlehale, when you testified before the House Judiciary Committee in 2013 about the emergency issue, you said that some “providers make a decision never to provide records in the absence of legal process, no matter the circumstances.” But Google, Facebook, Microsoft, and Yahoo! have all put out transparency reports that show that they do respond to emergency requests and provide responsive data the majority of the time.**
 - **Do you acknowledge that the largest service providers usually do voluntarily disclose content in response to an emergency request?**

Response: It has been my experience, and the experience of the state and local investigators with whom I am acquainted, that larger service providers will sometimes respond to emergency requests under the existing provision in ECPA. How often and how quickly they respond varies widely from case to case and provider to provider (and even from call-taker to call-taker). It is fair to say that in my experience, most large providers will usually provide records on an emergency basis for a child exploitation investigation, for example, or in response to a child abduction. The same is not

necessarily true for other situations which those of us in law enforcement would consider life-threatening emergencies.

I wouldn't use the word "usually" across the range of cases and providers, therefore, and even when the providers do provide an "emergency" response, what that means in terms of investigative latency also varies. Turnaround times of an hour or two for basic information on an emergency basis are normal for some large and small providers, but emergency responses in the four to eight-hour range are distressingly frequent, and even longer delays occur regularly with providers who do not adequately staff their compliance office.

Better data about the number of requests and the timeliness of service provider response in emergencies would be a welcome addition to this conversation; at present, law enforcement does not have a central mechanism to collect that data, and generally concentrates on the emergency itself rather than on data collection.

Most providers have a policy that is more restrictive than the statute; that is, they state a willingness to provide records in an emergency in a set of cases smaller than the range authorized by 18 United States Code Sec. 2072(b)(8), which permits voluntary disclosure "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." Some will provide emergency response in cases involving a danger to children, for example, or will only provide emergency access to non-content records.

It is worthy of note that the service providers who publish transparency reports often claim a certain number of emergency requests that they have rejected. It does not necessarily follow that those emergency requests were objectively flawed, but rather that the service provider chose not to respond to them. Without an independent examination of the facts, it is irresponsible to suggest that all of those cases were not true emergencies.

Service providers routinely require law enforcement to include language in legal process and other measures beyond what the Constitution and laws require. For example, when one Circuit issues a particular ruling raising the bar for access to a particular category of records, some service providers routinely extend that ruling to law enforcement in other parts of the country not bound by the decision.

- **Can you identify the service providers that have a policy of categorically rejecting emergency requests in the absence of compulsory legal process? If not, why not?**

Response: I have generally avoided naming specific service providers in my testimony because I do not want to publicly highlight forms of communication that are

particularly problematic for law enforcement, whether by virtue of policy, practice, or technology. It may be that the time will come when that practice is no longer practical in this area, as has become the case with developers of certain forms of encryption.

All of that said, I am personally aware of law enforcement officers who have attempted to obtain records on an emergency basis and been told by service providers that they agree that an emergency exists, but that the provider will not provide records in the absence of process. Some of those providers are among the “larger” companies in the market.

An example from a large provider’s compliance manual might be helpful. The following quote was included with an example provided by a colleague; the compliance manual in effect at the time of the example stated “If we receive information that provides us with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, **we may provide** information necessary to prevent that harm, if we have it.” Isn’t the implication of “we may provide” that in some instances, when there is “an exigent emergency involving the danger of death or serious physical injury to a person,” they might not provide it on an exigent basis? There is the justification for a mandatory disclosure provision in a nutshell.

2. In your written testimony, you discuss the need for law enforcement to have immediate access to evidence when the officer determines that an emergency exists.

- **What limits would be placed on such an emergency exception? Would it be entirely up to the discretion of the officer making the request?**

Response: The statute should contain a statutory definition of emergency that an officer must identify as having been satisfied in a declaration to the service provider. This definition should be broad enough for an officer to require accelerated response when the circumstances lead that officer, in his or her informed professional opinion, to believe that a person is in danger. Once the guidelines were established, it would be up to the officer to require an expedited response through a declaration.

The definition must be clearer than it is now, and the officer is in the best position to evaluate the facts and whether or not they qualify. What about the case of someone missing under suspicious circumstances, for example? What about a murderer on the run...how many people does someone have to kill before they are judged an unreasonable danger to the public? How specific does law enforcement’s evidence of a specific intent to harm others, rather than simply an intent to flee capture, have to be? Right now, those questions are entirely in the hands of call-takers without any public safety experience.

Any effort to reform this provision in ECPA should retain voluntary disclosure as an option for officers who are less familiar with this type of interaction with service providers, and who are willing to allow the service provider to retain responsibility for declaration of an emergency disclosure as a result.

- **Wouldn't this create powerful incentives for law enforcement to compel the disclosure of content in situations where a statutory emergency (i.e. risk of serious bodily harm or death) doesn't truly exist?**

Response: The incentive is only powerful if one is predisposed to think that law enforcement routinely circumvents limitations placed on their authority. Yes, law enforcement is often frustrated by the lack of timely responses by service providers in routine cases, and yes, when those delays prevent access to evidence, there are often have very real impacts on investigations and public safety. To the extent that there are missteps in this area, they are generally based on a misunderstanding of what constitutes an emergency, not on a deliberate attempt to avoid seeking legal process.

- **Do you think a suppression remedy would be appropriate to ensure content obtained in a falsely claimed emergency isn't used in a later investigation or prosecution?**

Response: No, a statutory suppression remedy would cause over-deterrence. Existing administrative sanctions are sufficient to deter unsupported exigent requests. One might also ask why the sanction would be exclusively on the law enforcement side. Shouldn't Congress create a civil cause of action against a service provider if their delay or negligence in responding to an emergency demand causes harm to someone? Or are the existing remedies that the common law provides sufficient to deter willful or negligent noncompliance by service providers?

3. You have suggested that Congress ought to statutorily mandate time limits for service providers to respond to legal process, but judges routinely prescribe deadlines for compliance.

- **Are state judges ill-equipped to be serving this function? Do service providers routinely ignore judge-imposed deadlines?**

Response: Judges routinely impose deadlines in areas where they are given the discretion to do so by rule or statute, such as in discovery. The rules for most state judges in this area are less clear. In some instances, state statutes provide some guidance, and in others the judges are willing to place a deadline in a search warrant or other order.

In my experience, and the experience of my colleagues, yes, service providers large and small routinely disregard judge-imposed deadlines placed on routine legal demands unless they are being actively litigated. Such disregard, and the reasons it often goes unanswered, can be largely explained by the fact that state prosecutors and judges are already generally overburdened by their caseload. The only remedy for this problem is to set aside time for a show cause hearing, and that requires the judge and the

prosecutor to litigate an issue which is often moot by the time a hearing could be held, either because the provider has finally responded to the process, or because the investigation has progressed in a different direction.

Please do not mistake this for evidence in support of the conclusory and unsupported “law enforcement will always find another way” argument. In fact, even if law enforcement does find another way to work the case, it often imposes delays, takes additional resources, and impacts the overall quality of the prosecution. “Well, you were able to scratch and claw your way most of the way there, even though you didn’t have access to the digital evidence,” isn’t a reasonable burden to place on law enforcement.

The difficulty in finding the time to pursue show cause orders – and the reason why they are not sought more often – is effectively illustrated by some simple figures from a large American urban court system: in one urban county, as of October 2015, there are 18,535 pending felony cases across 22 felony courts. These courts average 843 pending cases at a time, and each court has 3 prosecutors assigned. It shouldn’t be a surprise that cancelling court to hold a show cause hearing is not the most attractive option to secure service provider compliance for those judges and prosecutors.

Questions of Senator Amy Klobuchar

The Justice Department, and in particular the Federal Bureau of Investigations (FBI), often works in concert with local law enforcement.

- **How can we enhance cooperation between law enforcement at the federal level?**

Response. There are already a number of mechanisms in place for information-sharing among law enforcement agencies at all levels of government. In the area of digital evidence collection from service providers through ECPA, state and local law enforcement’s most pressing needs are for technical and legal assistance in securing the evidence that we need for our cases. We depend on the FBI, the Department of Justice, and other federal partners to provide us with advanced technical assistance and the support of compliance infrastructure through the federal system in cases where our local courts and mechanisms

A particularly important part of this support system that deals with digital evidence is the National Domestic Communications Assistance Center. Congressional support for the NDCAC’s mission of facilitating federal, state, and local access to electronic evidence. In addition, supporting programs to ensure that federal agencies have the funding and mandate to assist state and local law enforcement, and to ensure that federal law enforcement shares any and all technological solutions available to ensure state and local access to electronic evidence, will also foster interagency cooperation.

- **Are there notable differences in the collection of electronic information through ECPA at the federal level compared to the local level? If so, what can be done to ensure uniform processes for all law enforcement agencies?**

Response. Generally speaking, the legal demands used are similar, and the interaction with service providers is similar. One area of difference is the fact that the federal government has already implemented electronic systems for exchange of routine process, greatly improving response time. Any efforts to increase the availability of these systems to state and local law enforcement, and/or to develop them further to accommodate the wide range of requests and legal demands, would be a huge service to the state and local law enforcement community.



October 7, 2015

**Responses of Richard Salgado, Director, Law Enforcement and Information Security
Senate Judiciary Committee
Hearing on "Reforming the Electronic Communications Privacy Act," September 16, 2015**

Question for the Record from Senator Grassley

Q1: In 2014, Apple implemented a new operating system that employed a system of encryption that effectively prevented it from providing certain user content in response to a judicially-authorized search warrant or otherwise bypassing a user's passcode. I understand that Google does not currently employ such a system. Does Google intend on implementing an Apple-like encryption system or will Google continue to employ strong encryption technology that still allows law enforcement to access platforms and devices with court authorization?

A: As I mentioned in the hearing, keeping user data secure is important to Google and to the people who use the services Google offers. Encryption is a valuable tool in the suite of tools that Google can use to secure information that users have shared with Google. There are many types of encryption, and, depending on the product, one type of encryption may be more appropriate than another to keep the information secure while also providing the underlying services. It is important that Google, and companies that handle the data of Americans, have the ability to use technological means to combat the serious threats to the nation's networks; it would be shortsighted to hamstring the ability of network operators to employ key security defenses to protect the nation's data.

Since 2011, Google's Android operating system has allowed an Android user to secure the data on the device with the key in the control of the user, much as users have been able to do with computers and laptops of all sorts for many years now. The newest version of the Android operating system, known as Marshmallow, continues this approach and makes it easier for those with Android phones to secure their devices to protect against the event that the phone is lost or stolen. The data on the device, as well as the device itself, is in the control of the owner. The device and the data are available to investigators from the user in response to court authorization no less than any other item or data that a user may have in his or her unique possession.

Many former national security officials, current government officials, and security experts believe that this type of device encryption is important to protect the public from identity theft, privacy invasions and other crimes:

- *"We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."*

Mike McConnell (former NSA Director)
Michael Chertoff (former DHS Secretary)
William Lynn (Former Deputy Secretary of Defense)
[Washington Post op-ed](#) on 7/28/15

- *"If consumers cannot trust the security of their devices, we could end up stymieing innovation and introducing needless risk into our personal security. In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers."*

Terrell McSweeney
FTC Commissioner
[Huffington Post op-ed](#) on 9/3/15

- *"The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage."*

The [President's Review Group on Intelligence and Communications Technologies](#)
on 12/12/2013

Question for the Record from Senator Leahy

Q1: In its testimony, the SEC asked Congress for the authority to obtain the contents of electronic communications from third-party service providers without a warrant. How do you respond to this proposal? What are the implications of requiring providers to go into their users' accounts to look for and produce communications and documents that are responsive to a civil investigation?

A: There are several reasons why civil administrative agencies should not be granted the power to compel service providers to disclose the content of user communications.

First, granting civil agencies the power to compel service providers to disclose the content of communications stored with the provider by users would run afoul of the Constitution. The reasoning in *United States v. Warshak*, concluding that the Fourth Amendment protects the content of communications stored with a service provider, is persuasive. The SEC has set out an abstraction from which, it contends, one could draft a special Fourth Amendment carve-out. Even assuming that there is a way to draft a bespoke rule for the SEC that passes constitutional muster, this is the sort of exercise that Chief Justice Roberts warned against in in [Riley v. California](#), 134 S.Ct. 2473 (2014). In that decision, Chief Justice Roberts wrote that a regime with various exceptions and carve-outs "contravenes our general preference to provide clear guidance to law enforcement through categorical rules." *Riley*, 134 S.Ct. at 2493.

Second, there is no need to create a carve out of this constitutional doctrine for civil administrative agencies. The SEC and the thousands of other administrative agencies in the United States have ample authority to obtain communications of targets and witnesses without also granting them powers reserved to criminal and national security authorities.

As I discussed in my responses to questions posed by Senator Whitehouse, civil administrative agencies can issue subpoenas to the targets or witnesses to obtain their records. There is no need for a provider, or even a court, to get involved. If the recipient of the subpoena is intransigent or uncooperative, the administrative agency has a broad array of tools to compel compliance. Civil agencies can always enforce subpoenas when a person fails to produce responsive documents and secure a court order. If a target or witness subsequently fails to produce responsive material pursuant to that court order to do so, the judge may impose sanctions, which could include the denial of counter-claims, adverse inferences as a result of the target's intransigence, fines, default judgments, and even jail time. As Andrew Ceresney, who testified for the Securities Exchange Commission noted, the intransigence of a witness can be discovered by issuing subpoenas to others.

It is thus not surprising that when asked at the hearing if there were cases that were affected by the inability of the SEC to obtain content from providers, Mr. Ceresney gave no examples. This in spite of the fact that the the SEC and all other civil administrative agencies have never had the authority the SEC now seeks. Previously, in [an April 2013 letter to Senator Leahy](#), the SEC discussed what it purported to be an example of a case where the lack of authority to delve into the constitutionally protected online accounts of others negatively impacted an investigation. In that letter, SEC Chairman Mary Jo White asserted that "absent ECPA authority to subpoena the ISP directly, the Commission would not have had in its possession this critical piece of evidence." Upon closer analysis, [this example was debunked](#).

Third, a provider will make a very poor substitute for the user in searching for and selecting documents to produce. The provider will likely have little knowledge about the case in order to determine what communications are in and what are outside the scope of the legal process, and no ability to determine what materials are privileged, are trade secrets or confidential, or subject to special handling rules like health information. As in any civil case, it should be the witnesses

who are responsible for finding and producing the documents over which they have control. There is no reason that there should be a different rule for documents a witness has stored online than for documents stored by the witness at home. Even in cases where the user consents to disclosure, providers should not be forced into becoming discovery vendors for parties in civil litigation.

Finally, it is worth noting that there are thousands of civil administrative agencies in the United States with some flavor of subpoena power. Each no doubt has a case to make as to why the authority the SEC seeks would be useful. Granting such authority to these agencies would be a significant expansion of power for all of these agencies, large and small, at the expense of the Fourth Amendment. We would never grant civil administrative agencies the power to convert landlords into police officers to search for documents in the basement of a home, and we should tolerate that no less with the same documents stored online.

Question for the Record from Senator Lee

Q1: In his testimony, Mr. Littlehale described the difficulties that law enforcement agencies encounter when making emergency requests to service providers. In particular, he noted that the determination of an emergency is left to the providers rather than with those agents on the ground and that the response rate is too low or too slow.

- **Do you believe that an emergency exception that would compel compliance from service providers is necessary?**

A: No. The current emergency authorities codify important checks and balances that ought to be preserved by Congress. Moreover, users expect Google to scrutinize requests for communications content that otherwise are not reviewed by a judge to ensure that statutory criteria for emergency situations (i.e. danger of death or serious physical injury to any person) are met.

In his testimony, without identifying any providers, Mr. Littlehale asserts that some "providers make a decision never to provide records in the absence of legal process, no matter the circumstances, as baffling as that may sound in the light of day." Vis a vis the largest Internet companies in the world, including Google, it is clear that this is not the case. The transparency reports published by Google, Facebook, Microsoft, and Yahoo!, each disclose data about the number of emergency requests received and the percentage of cases where responsive data is provided. Google takes emergency requests under ECPA very seriously, and those requests receive the highest priority.

It is not a little ironic to hear a representative of local law enforcement agencies express misgivings about statutory authority sought by and granted to the government by the USA PATRIOT Act of 2001. Prior to the PATRIOT Act, the Stored Communications Act had no

express carve out for emergency situations at all. The PATRIOT Act actually expanded the ability of government to get stored information, including content, in emergency situations. Congress struck the right balance in granting providers the discretion to reject requests that did not meet the statutory criteria for emergencies, and it should decline the invitation to weaken the core protections of S. 356 by amending the emergency provisions under ECPA in ways that do not comport with the Fourth Amendment.

- **Does it make sense for the service provider to be able to decline a request in an emergency? Why?**

A: Yes. The current statutory provision has proven to work well, and there is no need to convert this into a new authority, which necessarily would have very little pre-disclosure oversight to prevent abuse. Google has set up a 24/7 emergency request system to respond to life and limb emergencies wherever in the world the emergency may happen. The requests are handled immediately as they come in by trained specialists. We take this very seriously. As our Transparency Report shows, Google is able to help in the majority of requests, 80% in the last reporting period, that come to us through this authority.

Of course, there are situations in which a provider will not disclose the contents of communications or customer records in response to a request that is purported to be an emergency. For example, the service provider may not have any responsive data. For [Microsoft](#), according to its transparency report, this accounts for more than 26% of requests for which no data is provided in the U.S.; Microsoft simply doesn't have any responsive data to provide.

In some situations, a government agency may make a request where there is no "emergency involving danger of death or serious physical injury to any person" and there is time to secure legal process. At Google, we take seriously our obligation to protect users' privacy. Unfortunately, at times government investigators try to invoke the emergency disclosure requests because it is easier than getting legal process, with the checks that come with it, even though legal process is available in a timely manner. It's not unusual, when we turn down an emergency request because of the lack of a life or limb emergency, that we receive legal process shortly thereafter.

By granting providers the right to disclose when they believe there is such an emergency, but not an obligation to disclose when the authorities assert there is, we help ensure that law enforcement uses legal process as the preferred means to obtain user data, and the emergency process only in true exigent circumstances.

To the extent a government investigator prefers to compel the disclosure, delay in securing legal process should not be an issue. In every federal judicial district, a search warrant is a telephone call away. [Federal Rule of Criminal Procedure 41\(d\)\(3\)](#) permits a magistrate to respond to a telephonic request for a warrant any time, including after-hours where it is inconvenient to go to court or in an exigent situation where time is of the essence or evidence could be lost.

Governmental entities avail themselves of this option and consequently obtain user data in a timely manner when exigent circumstances exist.

- **What is Google's response rate to emergency requests? What reasons could a service provider have for not complying?**

A: In November 2013, Google began including information about emergency requests in its [bi-annual transparency report](#) covering government demands for user data. Other service providers, including Facebook, Microsoft, and Yahoo, also now include information about emergency requests in their transparency reports.

This data helps shed light on the volume of emergency requests that service providers receive, which is very low in comparison to the total number of compulsory legal demands that service providers receive under ECPA. In the second half of 2014, for example, Google received 171 emergency requests affecting 272 user accounts in the U.S. That figure represents less than 2% of all compulsory legal demands issued to Google by authorities in the U.S. As I mentioned above, Google voluntarily disclosed data in response to 80% of those emergency requests. (By comparison, Google disclosed data in response to 78% of compulsory legal demands in the U.S. in the second half of 2015.)

Further information about Google's handling of emergency requests appears in the table below. (Some of the reasons why a service provider may not comply with an emergency request are discussed in response to the previous question.)

| Timeframe | Emergency Requests | Users/Accounts Impacted by Emergency Requests | Percentage of Cases Where Data Provided |
|----------------------|---------------------------|--|--|
| July - December 2014 | 171 | 272 | 80% |
| January-June 2014 | 171 | 241 | 65% |
| July-December 2013 | 153 | 217 | 78% |
| January-June 2013 | 119 | 175 | 81% |

- **In what ways can the response time be improved in cases where an emergency exists?**

A: As noted above, emergency requests receive the highest priority. We strive to respond to emergency requests in about an hour. Of course, some are resolved much faster, and others may be more complex and take longer to close out, but they all receive immediate attention when sent through the emergency system.

Q2: Several witnesses have discussed the slow response rates from service providers as reasons to hold up codifying a warrant-for-content standard.

- **Why are response rates perceived as being slow?**

A: It is difficult to speculate why law enforcement agencies perceive that service providers are slow to respond to legal demands; it's likely that response times vary among companies that receive ECPA legal process just as it would with companies that receive non-ECPA process. The substantial increase in law enforcement demands to service providers like Google may fuel this perception. Since 2009, government requests for user data issued to Google in criminal matters in the U.S. alone have increased 179%. Notwithstanding this fact, Google responds to law enforcement demands in a timely manner.

Judges of course can prescribe deadlines for compliance that are tailored to the exigencies and gravity of particular cases, as well as the need for the underlying evidence. If service providers are uncooperative or otherwise non-compliant, law enforcement agencies can take remedial actions with a court to enforce such deadlines. Taking that discretion away from judges and trying to craft a one-size-fits-all statutory deadline makes little sense.

Slow response rates can be attributable to factors that are beyond the control of service providers. For example, when Google receives legal process that is overbroad, vague, ambiguous, illegible, riddled with typographical errors, or issued without proper authority, that will invariably slow our response time in responding to that process, and of course takes resources away from properly issued process. Moreover, a single legal request can ask for information covering multiple products and concern multiple account holders, and may require engineering resources, each of which obviously increases the time and resources necessary to respond. Finally, law enforcement agencies often demand nondisclosure to users without proper nondisclosure orders. That, too, leads to delay.

- **What is Google doing to improve response times?**

A: Google is always looking for ways to improve the process, while making sure that we are not compromising the quality of review to protect users. We do this in many ways. For example, as the volume of requests increases, we increase the number of legal specialists to handle them. As you might expect, we also are able to take advantage of the technical expertise of the company to offer faster and more secure ways for government agencies to submit requests and receive responses.

The huge number of agencies, with different technical competencies and legal authorities, make it impossible to have a single approach for all. Nonetheless, we have been able to reduce response time even as volume has grown. Time varies between legal process, of course, as some are more urgent than others and some have shorter deadlines than others. In addition, after hearing the testimony of Mr. Littlehale, we reached out to make sure that if any of his perceptions applied to Google, we find ways to address them.

Q3: The administration witnesses on the first panel spent a great deal of time talking about how onerous it would be to face a warrant requirement for email content. Yet, they have been operating for years under a bright-line, warrant-for-content standard.

- **In what ways would enacting the warrant requirement laid out in the ECPA Amendments Act change the ability of these agencies to gather information?**

A: It would change nothing at all. As you note, civil agencies have been operating under a bright-line, warrant-for-content standard since 2010, when the Sixth Circuit Court of Appeals opined in *United States v. Warshak* that ECPA is unconstitutional to the extent it does not require a warrant for all content. Even before then, going all the way back to 1986 when ECPA was passed, the civil agencies could not get email that was unread and fresh from providers, per the limitations in the statute.

There is no evidence to suggest that *Warshak* decision, or the limits in ECPA before that, have prevented civil agencies from investigating cases. In its [2014 annual report](#), the SEC notes that it brought a "record number of cutting edge enforcement actions." In that same report, the SEC said that it brought "more cases than ever before", including "a number of first-ever cases that span the securities industry." It did so, as [Chairman White testified](#) earlier this year, without issuing subpoenas for content from providers under ECPA.

Warshak is effectively the law of the land today. It is embraced by companies and observed by governmental entities. In many ways, S. 356 is a modest effort to codify the status quo and implement the Sixth Circuit's conclusion that the Fourth Amendment requires a warrant in all cases where the government seeks to compel a provider to disclose communications content from a company covered under ECPA.

Question for the Record from Senator Franken

Q1: I am interested in better understanding the various circumstances in which Google satisfies government requests for user data. The statistics I've seen indicate that Google receives more than 20,000 requests per year from government agencies in the United States, and is able to provide at least some data in response to approximately 80% of these requests. Of course, not all of these requests are for content or are accompanied by

criminal warrants. Please describe the range of requests typically received. How often does Google voluntarily comply with requests based on an exception for emergencies?

A:

Range of Requests

Google receives a broad array of government demands seeking user data, which includes demands for basic subscriber information (which is defined in the statute, such as name, account creation information, associated email addresses, phone numbers), other non-content data (e.g. the IP address associated with a YouTube video upload, records of who a user emailed and who emailed the user) and content (e.g., the body of Gmail messages).

Approximately 60-70% of US demands for user data that Google receives are subpoenas, through which the government can obtain basic subscriber information. About 10% are court orders through which the government can seek basic subscriber information and often the more detailed non-content information. Another 20-30% are search warrants, through which government can seek the non-content information as well as content. Not all warrants require production of content. We also receive a small number of orders issued under pen register and trap and trace statutes, and an even smaller number under wiretap authorities.

Since 2014, we have also reported data about the volume and type of national security demands that we receive. We look forward to the effective date of the USA Freedom Act, under which we will be able to increase the granularity of those reports, and we greatly appreciate your leadership in ensuring the enactment of these provisions.

Emergency Requests

In November 2013, Google began including information about emergency requests in its [bi-annual transparency report](#) covering government demands for user data. Other service providers, including Facebook, Microsoft, and Yahoo, also now include information about emergency requests in their transparency reports.

This data helps shed light on the volume of emergency requests that service providers receive, which is very low in comparison to the total number of compulsory legal demands that service providers receive under ECPA. In the second half of 2014, for example, Google received 171 emergency requests affecting 272 user accounts in the U.S. That figure represents less than 2% of all compulsory legal demands in the U.S. received by Google. Moreover, Google voluntarily disclosed data in response to 80% of such emergency requests. (By comparison, Google disclosed data in response to 78% of compulsory legal demands in the U.S. in the second half of 2015.)

Further information about Google's handling of emergency requests appears in the table below.

| Timeframe | Emergency Requests | Users/Accounts Impacted by Emergency Requests | Percentage of Cases Where Data Provided |
|----------------------|---------------------------|--|--|
| July - December 2014 | 171 | 272 | 80% |
| January-June 2014 | 171 | 241 | 65% |
| July-December 2013 | 153 | 217 | 78% |
| January-June 2013 | 119 | 175 | 81% |

Responses of Federal Trade Commission Daniel Salsburg to Questions Submitted for the Record

Hearing on “Reforming the Electronic Communications Privacy Act”
Senate Committee on the Judiciary
September 16, 2015

Questions from Chairman Grassley

1. The Commission's statement for the record describes a series of types of cases that would be affected in the future if there is no mechanism to compel the disclosure of content from providers—including cases involving anticompetitive and deceptive business practices, consumer protection, and other fraud enforcement actions. Can you describe these, and other, scenarios in more detail, including how often these types of enforcement actions arise?

The Commission’s testimony recommended that ECPA reform legislation include a mechanism that would enable civil law enforcement, using judicial process and approval, to seek a court order requiring that a target’s provider produce content when the target has failed or refused to provide the content directly to the Commission. The Commission’s testimony noted that this authority would be necessary in cases against fly-by-night scammers — especially those based abroad — as well as cases against targets that refuse to respond to the agency’s CIDs or discovery requests.

The Commission frequently targets complex consumer frauds that are causing substantial injury to the public and in which the targets have an incentive to hide their involvement in the fraud, destroy incriminating records, and hide or deplete assets. In such cases, the Commission will typically seek temporary restraining orders. For instance, in FY2014, the Commission sought temporary restraining orders in 20 of the 50 federal court consumer protection actions it filed. Moreover, in numerous instances, the Commission has sued foreign defendants who may seek to evade their discovery obligations. For example, in 2014, the Commission filed 10 federal court actions against foreign defendants.

Even in future cases that do not concern consumer fraud – such as competition matters involving alleged conspiracies in which the defendant fails or refuses to produce internal documents – content that the defendant stores with a cloud service provider may be evidence that is central to the enforcement action.

2. Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses, and/or anything else you did not have a chance to respond to that was discussed at the hearing.

Thank you for soliciting the FTC's views on ECPA reform. As the federal agency responsible for protecting the privacy and security of consumers' data, we have carefully considered the proposed legislation. The Commission has developed a multifaceted approach to protect consumers' privacy and security: (1) enforcement of a wide range of statutes, including the Fair Credit Reporting Act, Children's Online Privacy Protection Act, and Section 5 of the FTC Act, (2) policy development that provides guidance to companies on best practices they should adopt to enhance privacy and security, and (3) outreach to consumers on how to protect their personal information and mitigate the risk of identity theft. In addition to protecting consumers' privacy and security, protecting consumers from fraud is also an extremely important part of our agency's mission. ECPA reform can help strike the appropriate balance between civil law enforcement interests and the need to protect customers' and subscribers' privacy so long as it: (1) exempts previously public commercial content that advertises or promotes a product or service, (2) exempts content when the customer or subscriber consents to the release of the content to the government, and (3) provides civil enforcement agencies with the ability to seek a court order requiring a provider to produce a target's content when the target has refused or failed to produce the content directly to the agency. As the Commission explained in its testimony, a target should have no reasonable expectation of privacy with respect to government access to previously public commercial content and the consensual release of content. And, a judicial mechanism for other content that a target fails or refuses to produce to the government would provide appropriate privacy safeguards so long as it requires a civil enforcement agency to first seek the content directly from the target, and then to seek a court order with notice to the target.

Questions From Ranking Member Leahy

- 1. You testified that it no longer makes sense to provide less privacy protection to emails that are more than 180 days old and to emails that have been opened. The Electronic Communications Privacy Act currently requires the government to obtain a warrant before compelling the disclosure of email less than 180 days old, 18 U.S.C. § 2703(a). Is the FTC seeking the authority in civil investigations to obtain email, regardless of age, from providers without a warrant?**

Recent ECPA reform proposals would require the government to obtain a criminal warrant in order to compel a provider to produce a customer's email content. Because the FTC is a civil agency without authority to seek a criminal warrant, this sweeping prohibition would prevent the Commission from compelling the production of all email content – even messages in which a customer had no reasonable expectation of privacy with regards to law enforcement access. For instance, a spammer that sends a million messages touting a get-rich-quick scheme or a cure-all remedy has no reasonable expectation of privacy in the content of its spam, but the Commission would be foreclosed under ECPA reform proposals from seeking this content from a provider. These proposals also would require a criminal warrant to obtain email content even when a customer consents to having the FTC obtain the content directly from its provider. For instance, if a victim deleted a message from a target and wanted to authorize the FTC to obtain a copy of the message directly from the victim's provider, the FTC would not be able to do so under proposed ECPA reform legislation. The legislative proposals should include exceptions for previously public commercial content that advertises or promotes a product or service and for content with the consent of the customer or subscriber.

ECPA reform should also include a judicial mechanism that would permit civil law enforcement to obtain a court order compelling a provider to produce electronic content such as email when efforts to obtain the content directly from the target fail. Although the FTC has not proposed a specific judicial mechanism, such a mechanism should require appropriate judicial oversight and due process to protect the privacy rights of the target.

There is no reason for treating content differently based on the length of time it has been in electronic storage. Recent ECPA reform proposals appropriately remove this distinction by imposing a single standard for content held by remote computing service or electronic communications service providers. Thus, if a target fails or refuses to produce relevant email, regardless of its age, the Commission should be able to seek a court order, with notice to the target, demanding that the target's provider produce the content.

- 2. In a prior committee markup of the ECPA Amendments Act, the Judiciary Committee added a provision making clear that agencies can continue to issue subpoenas to corporations for the contents of their employees' email. This recognizes that corporations do not have the same privacy interests as individuals. How important is this corporate email provision to your agency?**

Virtually all businesses use email as a communication method. For this reason, emails among a target's employees frequently provide important evidence of a target's law violations, the scope of injury, and identity of victims. ECPA reform efforts should preserve the Commission's ability to obtain this vital form of evidence.

Questions from Chairman Lee

1. The FTC is the nation's chief privacy protection agency. The ECPA Amendments Act is the most important and popular consumer privacy bill before Congress, and it has been for many years now. It has over 290 cosponsors in the House and 23 Senators have joined me as cosponsors in this chamber.

- **Why is it so difficult for the FTC to endorse a bill that would codify protections that everyone here agrees reflect users' reasonable expectation of privacy?**

The Commission supports ECPA reform, but has commented on specific ways in which recent legislative proposals could be improved. The FTC brings a unique perspective to the ECPA reform process. The FTC is the civil enforcement agency charged with protecting consumers from unfair methods of competition and unfair or deceptive acts or practices. The FTC also has extensive experience in consumer privacy enforcement. Its enforcement actions have addressed practices offline, online, and in the mobile environment. The FTC also works to protect consumer privacy through other tools such as conducting studies and issuing reports, hosting public workshops on a wide range of issues, including the Internet of Things and Big Data, and developing educational materials for consumers and businesses. In all of its privacy work, the Commission aims to protect consumers' personal information and ensure that consumers have the tools necessary to make effective choices about their privacy while at the same time taking advantage of innovative products and services offered in a dynamic marketplace.

Successful ECPA reform requires finding the appropriate balance between protecting privacy and enabling civil law enforcement to obtain the evidence needed to protect the public.

The Commission's testimony highlighted two forms of content that recent ECPA reform proposals would prevent the FTC from obtaining even though customers would have no reasonable expectation of privacy with respect to government access to the content – previously public commercial content that advertises or promotes a product or service and content when the customer has consented to the government obtaining the content.

The Commission's testimony also explained the need to create a judicial mechanism to allow civil law enforcement to obtain content in some circumstances. As more and more content moves from local storage to cloud-based storage, the FTC is likely to encounter situations in which scammers refuse or fail to turn over relevant data stored in the cloud, thereby making it difficult for the FTC to protect consumers. In those instances when a target fails or refuses to

produce content directly to a civil enforcement agency, the agency should be able to seek a court order, with notice to the target, that would direct the target's provider to produce the content directly to the agency.

- **If the FTC can't – without reservation – endorse a bill that's supported across the ideological spectrum, and that merely seeks to codify the status quo as it exists today, doesn't that raise questions about the FTC's credibility to represent the views of consumers on privacy issues?**

The FTC supports the goals of ECPA reform, but believes that current legislative proposals can be modified in ways that both protect consumers' privacy and enable the FTC to continue to perform its critical consumer protection and competition missions in the future when most business data will be stored with third parties. The Commission has worked for almost 20 years to ensure that consumers' privacy is protected; we have brought hundreds of cases to protect consumers' privacy, published detailed reports on a range of privacy issues, and produced valuable consumer education and business guidance. The Commission remains committed to protecting consumers' privacy. We also seek to ensure that the FTC is able to perform its role as a civil law enforcement agency.

2. **The SEC's proposal to compel a third-party provider to disclose all of the content of an email account (going back who knows how far) rather than going to the company or individual directly and asking for only the relevant emails should raise important privacy concerns.**

- **Wouldn't such discovery would result in a lot of unrelated personal material being produced to the SEC and other agencies like the FTC, including medical, financial or attorney-client communications that are wholly unrelated or wholly protected in civil litigation between the parties?**

Long-standing administrative and judicial procedures are capable of addressing the risk that unrelated personal data or privileged material would be improperly accessed if the Commission obtained access to a target's content. As an initial matter, the Commission does not seek unrelated or privileged materials in its investigations. Moreover, there are several procedural safeguards that significantly decrease the likelihood that the Commission would obtain such information. For example, the FTC's internal review process for civil investigative demands (CIDs) requires that they pass through several layers of review before they are ultimately issued by a Commissioner. Once issued, the recipient has several opportunities to seek to narrow the scope of the CID, ranging from a meet and confer requirement contained in the Commission's CID rules to more formal opportunities to object to the CID's scope. The judicial mechanism sought by the FTC to obtain content from a target's provider would include further safeguards by requiring a civil law enforcement agency to seek a court order from a neutral judge with notice to the target. The target would have an opportunity to appear before the judge and explain any concerns about the production of irrelevant personal or privileged materials. If the court were to find that an order directing the provider to produce material was likely to result in the production

of privileged materials or materials that were not likely to lead to the discovery of admissible evidence, it could limit or deny the order altogether.

Federal Bureau of Investigation
Agents Association

September 24, 2015

The Honorable Charles E. Grassley
Chairman
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patrick J. Leahy
Ranking Member
Senate Committee on the Judiciary
Washington, DC 20510

Re: Reforming the Electronic Communications Privacy Act

Dear Chairman Grassley and Ranking Member Leahy:

On behalf of the FBI Agents Association (FBIAA), a voluntary professional association currently representing over 12,000 active duty and retired FBI Special Agents, I write to express the FBIAA's concerns and thoughts regarding issues raised in the hearing held by your committee on September 16, 2015, entitled "Reforming the Electronic Communications Privacy Act." During the hearing, witnesses and Senators raised a number of important concerns about efforts to change the Electronic Communications Privacy Act (ECPA), and the FBIAA believes that legislative efforts to reform ECPA must address these concerns directly, before any ECPA reform legislation should be enacted.

Chairman Grassley, you correctly noted during the hearing that reforming ECPA 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 profession, society's interest in encouraging and expanding commerce, and the dictates of the Constitution." On behalf of the brave men and women defending this Nation as federal law enforcement officers, let me assure you that we share your commitment to adhering to the Constitution and striking the proper balance between privacy and security. It is for this very reason that we think that any ECPA reform legislation must address the serious issues raised at your recent hearing.

The FBIAA is particularly concerned about two major issues regarding the ECPA reform proposals that have been discussed to date:

Post Office Box 320215 • Alexandria, Virginia 22320
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175
E-mail: fbiaa@fbiaa.org www.fbiaa.org

Federal Bureau of Investigation

September 24, 2015

Agents Association

Page 2

1. ECPA reform legislation should ensure that law enforcement is able to access electronic evidence.

As a number of witnesses and Senators noted during your recent hearing, technology has evolved significantly in recent years and has made it necessary for Congress to update the laws surrounding electronic privacy. However, such an effort must address more than the business and privacy concerns of major technology companies. Meaningful ECPA reform must also address the security and law enforcement needs of our citizens by preventing criminals from having unfettered access to secure communications, including crucial warrant exceptions, and requiring that technology companies cooperate with lawful investigations.

Going Dark

An important aspect of the recent technology revolution has been the development of hardware and software that threatens to give criminals secure tools for communication and dissemination of information and materials—tools that can make it impossible to obtain electronic evidence even when such evidence is required to be produced pursuant to a lawful warrant.

Never before in our country's history have criminals and terrorists had access to technology that could allow them to coordinate their efforts nationally or internationally without any ability for law enforcement to legally access the evidence of their conspiracies. Such a scenario—often described as “going dark”—could create new and dangerous risks of crime and terrorism. Accordingly, Congress must address the risks of going dark by ensuring that technology companies allow for lawful access to electronic data.

Warrant Exceptions

Requiring a probable cause warrant for access to all electronic information could add additional delays to the investigation process, and such delays could pose unique risks to investigations that are uniquely time-sensitive. Accordingly, the FBIAA believes that ECPA reform legislation should include explicit exceptions to the warrant requirement for emergencies and investigations of crimes such as child pornography where the time and delays associated with warrants and the risks of notification can jeopardize investigations.

Service Provider Cooperation

ECPA reform legislation that has been considered by Congress to date, such as S. 356, increases administrative burdens on law enforcement by expanding warrant requirements, but does not address the need for internet service providers to deliver timely responses to law enforcement requests. Delayed responses or a lack of communication from internet service providers in response to law enforcement requests can jeopardize sensitive investigations, and Congress should compel these providers to develop reliable and efficient procedures for responding to law enforcement requests for electronic information.

Post Office Box 320215 • Alexandria, Virginia 22320**A Non-Governmental Association****(703) 247-2173 Fax (703) 247-2175****E-mail: fbiaa@fbiaa.org****www.fbiaa.org**

Federal Bureau of Investigation

September 24, 2015

Agents Association

Page 3

ECPA reform should include language requiring that internet service providers develop internal response protocols designating at least one individual as a “24/7” point of contact for law enforcement requests, and requiring that responses to requests be made in a timely manner. Additionally, Congress should clarify the language in 18 U.S.C. § 2709 to make it clear that service providers must provide all relevant electronic communications transaction records when they are properly requested by law enforcement officials.

2. ECPA reform legislation should not create new obstacles for investigations

The FBIAA understands that there are aspects of ECPA that have been rendered obsolete by changing technology and should be revised. However, ECPA reform should not result in the creation of new and unnecessary obstacles for law enforcement officials. In particular, Congress should avoid creating new and risky notification procedures, and should not include provisions that would make it more difficult for law enforcement to obtain electronic evidence housed outside of the U.S.

Notification of Targets

As discussed in our previous communications with your committee and Congress, the FBIAA is concerned that target notification requirements that have been included in ECPA reform bills may threaten the effectiveness of sensitive investigations of criminals and terrorists.

Search warrants are often obtained in the early stages of investigation, and notifying the target of a search warrant about its issuance could allow for the destruction of vital evidence. Requiring notice a few days after a warrant is issued, even with the ability to request a delay, risks administrative and technical errors that could result in targets of an investigations being told of ongoing investigations, a potential threat to public safety. Further, even if a delay order is obtained, limiting the delay to 180 days could undermine investigations that require more than 180 days to complete because targets would be notified of the ongoing investigation. While the orders can be renewed, an accidental failure to do so or a delay due to administrative error would alert the target to the investigation.

For these reasons, the FBIAA believes that changes need to be made to the proposed notification requirements that have been included in ECPA reform bills such as S. 356. Specifically, rather than a presumption of notification, there should be a presumption that notice is not required until an investigation is ended and a court finds that notification would not pose a risk to ongoing investigations.

Access to Evidence Overseas

In the era of cloud computing, electronic evidence held by U.S. companies or persons may be physically stored anywhere around the world. Access to this evidence is essential to investigations of criminal and terrorist enterprises, and U.S. service providers should not be able to refuse to comply with warrants because they have opted to locate their servers outside

Post Office Box 320215 • Alexandria, Virginia 22320**A Non-Governmental Association****(703) 247-2173 Fax (703) 247-2175****E-mail: fbiaa@fbiaa.org****www.fbiaa.org**

Federal Bureau of InvestigationSeptember 24, 2015
Page 4*Agents Association*

of the U.S. To do so would be to create an easy method for criminals and terrorists to evade law enforcement scrutiny and execute their plots to threaten the safety and security of our country. Despite these risks, however, some are seeking to expand ECPA reform legislation to include provisions that would make it more difficult for law enforcement officials to obtain this electronic evidence.

Negotiating cross-border data issues is complicated and delicate, and Congress should not use ECPA reform to circumvent ongoing diplomatic and analytical work being put into cross-border data access. Specifically, ECPA reform legislation should not be expanded to include proposals such as the *Law Enforcement Access to Data Stored Abroad Act* (LEADS Act). The FBIAA believes these proposals have significant flaws, and could make it more difficult to investigate, thwart, and prosecute criminals and terrorists.

We greatly appreciate your consideration of these concerns, which are of critical importance to the federal law enforcement community.

We look forward to continuing to work with you as you explore the impact of ECPA changes on federal law enforcement activities. If you have any questions, please contact me at rtariche@fbiaa.org or 703-247-2173, or FBIAA General Counsel Dee Martin, dee.martin@bgllp.com, and Joshua Zive, joshua.zive@bgllp.com.

Sincerely,

Reynaldo Tariche
President

Post Office Box 320215 • Alexandria, Virginia 22320
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175
E-mail: fbiaa@fbiaa.org www.fbiaa.org



**National Association of
Assistant United States Attorneys**
Safeguarding Justice for All Americans

Board of Directors September 15, 2015

Steven H. Cook
President (E.D. TN)

John E. Nordin II
Vice President
(C.D. CA)

Lawrence J. Leiser
Vice President
(E.D. VA)

Steven B. Wasserman
Treasurer (DC)

Kathleen L. Bickers
Secretary (OR)

J. Gregory Bowman
(E.D. TN)

Allison W. Bragg
(E.D. AR)

Eduardo R. Castillo
(W.D. TX)

Catherine A. Connelly
(W.D. MO)

Karen A. Escobar
(E.D. CA)

Craig W. Haller
(W.D. PA)

Lauren E. Jorgensen
(S.D. FL)

Joseph E. Koehler
(AZ)

David A. Marye
(E.D. KY)

Jessica Natali
(E.D. PA)

Jose Homero Ramirez
(S.D. TX)

Clay M. West
(W.D. MI)

Executive Director
Dennis W. Boyd

Counsel
Bruce Moyer

The Honorable Charles Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Patrick Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Re: September 16 Hearing, "Reforming the Electronic Communications Privacy Act"

Dear Chairman Grassley and Ranking Member Leahy:

In conjunction with your above-referenced September 16 hearing, I write to express our concerns over the foremost Senate proposal amending the Electronics Communications Privacy Act (S. 754) and ask that these comments be included in the record of your hearing.

The "Electronic Communications Privacy Act Amendments Act of 2015," S. 356, represents a troubling and incomplete approach toward updating current law governing one of the premier laws regulating access by law enforcement agencies to private electronic communications. The ECPA balances privacy interests in electronic communications against legitimate law enforcement needs. Enacted more than 25 years ago, the law has fallen behind technology and requires updating, but the better approach remains through a broader, more refined effort than that proposed by S. 356.

As you know, the ECPA currently provides the standards by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communications system. It requires that the Government obtain a court order, based upon probable cause, in order to intercept wireless and data communications. The law also requires that the Government obtain a search warrant in order to compel a third-party service provider to disclose the content of email, or other electronic communications, that the provider maintains in electronic storage and provides exceptions to the warrant requirement in certain

circumstances. For example under current law, the Government does not need a warrant in an emergency situation involving danger of death or serious physical injury, or when a crime is being committed.

The Electronic Communications Privacy Act Amendments Act of 2015, S. 356, proposes new standards governing notice by communications carriers to persons whose records have been made available to law enforcement. We are troubled by the vagueness of its proposed notice of disclosure and delayed disclosure standards and the potential compromise of sensitive law enforcement information that could result. We also are concerned by the silence of the bill in addressing the use of the ECPA to protect and disclose vital phone geolocation information collected and maintained by electronic communications service providers. Our concerns are addressed below.

Notice of Disclosure Requirements

Section 3 of S. 356, in part, requires the Government to notify the individual whose account was disclosed, and to provide that individual with a copy of the search warrant and other details about the information obtained. We are concerned by the bill's requirements regarding the content of the disclosure notice, including disclosure of "the nature of the law enforcement inquiry with reasonable specificity." The meaning of that preceding phrase is unclear and arguably could require the disclosure of a summary of the investigation or the affidavit in support of the search warrant, thereby releasing potentially compromising and sensitive information about the underlying investigation. The Senate report on similar legislation, S. 607 in the 113th Congress, suggested that the required notice included "a copy of the search warrant and other details about the information obtained." The lack of clarity in the current language of section 3 could create considerable confusion and threaten the disclosure of critical law enforcement information.

In addition, we are concerned by the inadequacy and inconsistency of legal process protocols between service providers and law enforcement, upon which disclosure requirements are based, and which are left unaddressed by S. 356. The ECPA also should be amended to confer to law enforcement investigators the authority to determine what constitutes an "exigent circumstance" or emergency situation that requires service providers to disclose the requested information. This would permit law enforcement investigators, who have the training and experience in such matters, to make a more informed judgment that balances privacy and public safety.

Delayed Notice

Section 4 amends section 2705 of the ECPA to provide that the Government may seek a court order to delay notifying an individual of the fact that the Government has accessed the contents of the individual's electronic communications for up to 180 days. Section 4 also requires that service providers

notify the Government of their intent to inform a customer or subscriber of the fact that the provider has disclosed the individual's electronic communications information to the Government at least three business days before the provider gives such notice to the customer or subscriber.

We are concerned by the brevity of the three-day "warning" period from the provider to the Government. Three days is insufficient to assure a timely response from the United States Attorney's Office, including its possible application to a court for an extension of the preclusion of notice. Any warning period should be enlarged from 3 business days to at least 7 calendar days. Any harm, if any, to customers or providers by the additional time required is *de minimus*.

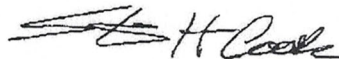
Geolocation Information

We regret that S. 356 is silent on the use of the ECPA to protect and disclose phone geolocation information collected and maintained by electronic communications service providers. This is a critical omission. Access to phone geolocation data is a constant challenge for law enforcement and prosecutors. Its pursuit is time-consuming and wrought with uncertainty (*e.g.*, what showing must be made, under what statute, and what process should be used). Greater clarity is needed, both to bring clarity to the ECPA and companion authorities, as well as the splits among the federal courts in this area. Inconsistent federal court rulings have added to the complexity over what information is subject to privacy protections, under what circumstances, and with what level of legal and administrative constraints.

Legislative reform of the ECPA will remain incomplete unless Congress addresses how and when providers may disclose geolocation information to law enforcement, appropriate warrant or subpoena requirements, and emergency exceptions.

Thank you for your attention to these matters. We look forward to working with the sponsors of S. 356 and other lawmakers to assure that any updating of the ECPA provides the proper balance between privacy and law enforcement interests.

Sincerely yours,

A handwritten signature in black ink, appearing to read "S H Cook". The signature is stylized with a large initial "S" and a cursive "H" and "Cook".

Steven H. Cook
President

cc: Hon. Orrin Hatch
Hon. Jeff Sessions
Hon. Lindsey Graham
Hon. John Cornyn
Hon. Mike Lee
Hon. Ted Cruz
Hon. David Vitter
Hon. Jeff Flake
Hon. Thom Tillis
Hon. Patrick Leahy
Hon. Dianne Feinstein
Hon. Charles Schumer
Hon. Richard Durbin
Hon. Sheldon Whitehouse
Hon. Amy Klobuchar
Hon. Al Franken
Hon. Christopher Coons
Hon. Richard Blumenthal