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 ISP[3] 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 <u>had consented</u> 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 <u>subscriber</u>.

<u>Response:</u>

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, <u>regardless of age</u>, from providers without a warrant?**

<u>Response:</u>

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?**

<u>Response:</u>

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 subpoenas 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.