

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 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.

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.

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