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 House of Representatives
December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee:

Thank you for inviting me to testify today on behalf of the Commission concerning the Email Privacy Act (H.R. 699) 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 H.R. 699, 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). H.R. 699 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, H.R. 699 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.