April 9, 2014

The Honorable Mary Jo White
Chair
U.S. Securities & Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chairman White:

A large and diverse coalition of American businesses, trade associations, and public interest groups from across the ideological spectrum supports reform of the Electronic Communications Privacy Act (ECPA). Bi-partisan reform legislation is pending in both Houses of Congress (S. 607 and H.R. 1852). ECPA reform is important both to privacy advocates and to U.S.-based Internet and communications companies, who have been leaders in the development of the innovative cloud and web-based email services that are revolutionizing how businesses and individuals store and share private and proprietary data. In this time of widespread concern about government intrusions on privacy, ECPA reform would assure businesses and the public that their electronic communications and documents stored in the cloud receive the same protections as postal mail and letters stored at home or in the office.

For the past year, the Securities and Exchange Commission has opposed reform of the ECPA. Recent statements by senior SEC staff and your testimony in the House have confused us about the source of the SEC's opposition. We have asked the SEC for recent examples of the type of access to communications that the SEC believes would be cut off by pending ECPA reform bills. So far, we have received none. (Below we discuss the one older case that the SEC cited to Congress, which we have shown does not actually support the Commission's position.)

Nevertheless, we would support an amendment to clarify and codify the principle of technology neutrality that we believe should guide ECPA reform: that the SEC and other regulatory agencies can use the courts to compel account holders to retrieve and disclose content stored in the cloud on the same terms as agencies have always used to compel entities under investigation to compile and disclose content stored locally.

The premise of ECPA reform is to make it clear that data stored in the cloud receives no less privacy protection than data stored locally. Conversely, it has always been the intent of ECPA reform that data stored in the cloud should receive no more protection than data stored locally. When S. 607 was being marked up by the Senate Judiciary Committee, we supported an amendment to make it clear that corporate email, stored by a company, would be available with a subpoena served on that company. The added amendment we propose would make it clear that any Internet user's data stored in the cloud could be obtained with a subpoena served on that Internet user, who could be compelled to retrieve the data from any third party provider.

The SEC is not a criminal justice agency and has no authority to obtain warrants. But the SEC has always had substantial powers to subpoena documents in the possession or control of its targets or other persons who may have sent or received communications relevant to the SEC's investigations. ECPA reform was never intended to interfere with the authority of the SEC to use subpoenas to compel individuals or companies to disclose the communications they sent or received regardless of how they are stored. We are willing to work with you to make that crystal clear. On the other hand, we cannot reform ECPA by giving the SEC a power that it is now widely agreed even criminal justice agencies should not have - the power to compel third party service providers to disclose contents with a subpoena.

We are offering compromise language even though we believe the SEC has made contradictory or misleading statements about its current and past practices.

In your letter last year to the Senate Judiciary Committee, you stated that ECPA reform would block the SEC from obtaining data directly from third party service providers. It is our understanding, however, that the SEC is not currently receiving content from third party service providers and has not been obtaining such content from third party providers since 2010, when the Sixth Circuit held in *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that a warrant rather than a subpoena is required to compel a service provider to disclose the content of communications held on behalf of its customers.

On March 4, 2014, members of the ECPA reform coalition met with senior SEC staff, in order to understand the SEC's concerns, and we asked for examples of the SEC's obtaining data from service providers with a subpoena. Senior staff confirmed that the SEC is not currently using subpoenas to obtain content from third party providers. However, your testimony on April 1 before a House subcommittee contradicted this, as you suggested again that the SEC is currently using subpoenas to obtain content directly from third party providers. We would repeat our request for specific examples.

Even before *Warshak*, we understand that there were few cases in which the SEC obtained an email through an ECPA subpoena to the individual's Internet service provider. In your letter last year, you cited only one. We believe the case referred to is *SEC v. Familant and Greene*.[1] Your letter stated that, absent ECPA authority to subpoena the ISP in that case, the SEC would not have obtained "this critical piece of evidence." This is the only example the SEC has cited on the record in opposition to the bill.

Contrary to the assertion in your letter, the record in the case shows that the email in question was not the critical piece of evidence. A review of pleadings and other evidence reveals that the SEC had a cooperating witness whose testimony was far more damaging than a single email.

Moreover, it is simply incorrect that the SEC could have obtained the email only by a subpoena to the third party service provider. In fact, the SEC could have obtained the email

[1] Center for Democracy & Technology, "The SEC Wants New Authority to Access Emails, But the One Case Cited by the Agency Suggests That New Powers Are Not Needed and Would Pose Serious Risks if Granted" (July 15, 2013) https://www.cdt.org/files/pdfs/cdt-sec-case-analysis.pdf.

through other means and made no effort to do so. As you noted in your letter, the SEC had issued a subpoena to Mr. Greene for his personal emails almost a year before it subpoenaed the ISP. The SEC can enforce its subpoenas on individuals by bringing an action in federal district court. However, a review of court records shows the SEC never sought to enforce its subpoena against Mr. Greene, and this fact has been confirmed with Mr. Greene's counsel.

Since the case cited in your letter contradicts the claim that the SEC needs direct access to third party providers in order to obtain critical evidence, we asked senior SEC staff at our meeting on March 4 if they could provide to us other cases pre-*Warshak* where the SEC had obtained content from a service provider with a subpoena. They declined to provide us with any other cases. We think that such cases, if any, were extremely rare, since the cloud phenomenon only emerged a couple of years before *Warshak* (and has accelerated considerably since 2010).

As far as we know, in the more than three years since *Warshak* was decided on constitutional grounds, neither the SEC nor any other civil agency has tried to compel a service provider to disclose the content of stored communications with a subpoena.

Further not only would the use of subpoenas by the SEC to compel disclosure by third party service providers constitute an expansion of access beyond what the SEC had as a practical matter after *Warshak* and even before *Warshak* (that is, before cloud services emerged), and not only would it not comport with the constitutional basis for *Warshak*, but it would open the door to potential abuse. For example, in a parallel investigation by the SEC (civil) and Department of Justice (criminal), the SEC could obtain information with a subpoena and then share it with DOJ, allowing the DOJ and other criminal agencies to circumvent the warrant process.[2]

Forcing disclosure by service providers raises other pitfalls, including the risk of violating an individual's attorney-client privilege if personal email was used to communicate with a lawyer (exactly what one would expect a person to do rather than use email in the workplace for example). The SEC staff was particularly dismissive of the privilege issues, asserting at one point that privileges are "our problem [the SEC's], not yours." While the SEC claims it has a process in place to insure that investigators did not review privileged emails this practice turns the concept of privilege on its head by allowing the government, not the affected party, to make a determination about privilege. Moreover, there is no such process referenced in the SEC's Enforcement Manual.

Despite our concerns with the SEC's conflicting statements, we propose an amendment to ECPA that would make it clear that the SEC or any other agency can use its subpoena power to compel an individual to retrieve and disclose any data held with a third party. A copy of the amendment is attached. We have worked with Chairman Leahy's office on this amendment. We believe that it would fully clarify the principle of technology neutrality -- that ECPA cannot be used to shield data in the cloud from ordinary discovery techniques.

---

[2] James B. Stewart, "A Dragnet at Dewey & LeBoeuf Snares a Minnow," The New York Times (March 14, 2014) http://www.nytimes.com/2014/03/15/business/an-underling-among-the-officials-accused-of-fraud-at-dewey.html?hp&_r=0.

This amendment would work in conjunction with authorities already in ECPA. ECPA already provides the SEC with a powerful tool to prevent the destruction or alteration of evidence while a motion to compel is being pursued: 18 USC 2703(f) authorizes any agency to issue, with no pre-approval, a preservation order directing a service provider to preserve the contents of any account it has. This order can be issued at the earliest stages of the SEC's interest in an individual or entity, even before a formal investigation has been opened. It can be used in conjunction with other provisions in ECPA allowing the SEC to serve subpoenas on email service providers and third parties to obtain subscriber identifying information and thus to confirm where a person has accounts.

Then, knowing where a person has accounts, and ensuring that the data is preserved, the SEC can issue a subpoena to that person (the target of its investigation or any other person who has sent or received email relevant to an investigation). Using the authority spelled out in the attached amendment, the SEC could proceed in a regular proceeding to compel production of any email in that account. Under cases such as *FTC v. Sterling Precious Metals, LLC,* 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013), the court could order the account holder to disclose the data, or, if the person claims to be no longer able to retrieve the data, the court can order the account holder to give consent, and the service provider could then disclose the contents.

We urge you to consider this amendment. Taken together with the preservation tool available to the SEC, we believe that it would fully preserve the access to electronic evidence that the SEC has today, while assuring businesses and the public that their electronic communications and documents stored in the cloud receive appropriate protection.

For follow-up, you can contact Jim Dempsey, Vice President for Public Policy at CDT, 202-xxx-xxxx (cell) or jdempsey@cdt.org.

Sincerely,

American Civil Liberties Union
Americans for Tax Reform
Center for Democracy & Technology
Heritage Action for America

cc: Luis A. Aguilar, Commissioner
Daniel M. Gallagher, Commissioner
Kara M. Stein, Commissioner
Michael S. Piwowar, Commissioner
Andrew J. Ceresney
Anne K. Small
Timothy B. Henseler
Joseph K. Brenner