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 that 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 certainty 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.