KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY
& TECHNOLOGY

Statement of Chris Calabrese
Vice President, Policy
Center for Democracy & Technology

Hearing before the U.S. Senate Judiciary Committee on "Reforming the Electronic Communications Privacy Act"

September 16, 2015

Chairman Grassley, Ranking Member Leahy, and members of the Committee:

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We applaud the Committee for holding a hearing on the Electronic Communications Privacy Act (ECPA) and urge the committee to speedily pass S.356, "Electronic Communications Privacy Act Amendments Act of 2015."

Every day, whistleblowers reach out to journalists (and members of this Committee), advocates plan protests against government injustice and ordinary citizens complain about their government. All of these activities are crucial to our democracy. They also all rely on our long-held constitutional guarantee of private communications, secure from arbitrary access by the government. This is true whether the communication happens in the form of a letter, a phone call or, increasingly, an email, text message or over a social network. But as our technology has changed, the legal underpinnings that protect our privacy have not always kept up.

The foundational value that ECPA reform seeks to uphold, as embodied by S.356, is the right to privacy for the content of our communications, even as technology evolves. In the face of an outdated statute, the courts have stepped in, creating key legal precedents and strong limits on access. But that patchwork is not enough on its own. It continues to lag behind technological change and harms smaller businesses that lack an army of lawyers. Reform efforts also face a concerted assault from civil agencies that seek to use statutory changes as a tool to gain new powers.

The Committee has consistently sought to solve these problems through strong reform measures, passing legislation nearly identical to S.356 in both 2012 and 2013. CDT continues to believe that a legislative solution – passage of S.356 – is the best way to advance a modest but critical privacy protection.

Support for privacy reform is deep and abiding. More than one hundred technology companies, trade associations, and public interests groups have signed onto ECPA reform principles.[1] Signatories include nearly the entire tech industry, span the political spectrum and represent privacy rights, consumer interests, and free market values. The companion bill in the House also enjoys widespread support, with more than 290 cosponsors – including a majority of Republicans and Democrats.

The Need for Reform

In 1986, when ECPA was written, few Americans owned computers and even fewer used email. Hard drives were small. Service providers offered little storage capacity and the storage they did sell was expensive. The World Wide Web didn't exist. Neither did cloud computing or broadband or social media or smartphones. The little data that was stored was kept on local computers.

Obviously that is not the world we live in today. Decades after the beginning of the Internet Age we store a vast array of sensitive communications with third parties — emails, text messages, work documents, pictures of our children, and love letters. Under ECPA they receive widely varying degrees of protection – most of which are inadequate and out of touch with consumer expectations.

These changes in technology – the rise of remote storage and cloud computing, the digitization of almost all communication – have two main implications for ECPA. First, they create serious inconsistencies in how similar communications are treated and the reasonable expectation of privacy they deserve. Second, they have disrupted the fundamental balance created in ECPA between privacy rights, law enforcement interests and the needs of innovators.

An Inconsistent Law

It can be helpful in understanding the conflicting standards and illogical distinctions that plague the current statute by considering the technological reality at the time of the passage of ECPA.

In 1986, Congress created two categories of providers and accorded users of those services different levels of protection. Legislators defined an electronic

[1] *About the Issue: ECPA Reform*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

communications service (ECS) as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[2] It was aimed at protecting the nascent use of email. Today, ECSs typically include any service that allows users to communicate with each other whether by email, text message, social network or other means. Under ECPA, those communications are protected by a warrant for the first 180 days after they are sent and are thereafter accessible with a subpoena. That 180-day rule is an outdated reflection of the fact that in 1986 hard drive capacity was incredibly expensive and no one contemplated long-term storage. The assumption was that if a user left an email on a server that long, it was abandoned and merited a lower privacy protection.

The second category of service under ECPA is a remote computing service (RCS), defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[3] Today, this would likely cover a cloud-based service accessed solely by an individual user, such as a Dropbox account. Under ECPA, RCSs receive only the protection of a subpoena. In 1986, RCSs tended to be major companies handling data for other major companies. As such, records in RCS storage appeared more like business records, and hence lawmakers granted them subpoena protections.

These distinctions make little sense today. Emails and other content are stored indefinitely and data held by RCSs are clearly as private as those by ECSs. It is often hard to glean in which category a particular service belongs. If a user stores a document remotely so she can later edit the document, does it move from RCS to ECS storage when she permits others to edit it as well? It also leads to wildly uneven results. The same communication could be protected by a warrant if stored on a home computer, a subpoena when stored as draft in an inbox, a Title III super warrant when in transit, a warrant for the first 180 days in an inbox and then a subpoena after that.[4]

Further, this one distinction only scratches the surface of the confusion over ECPA. Even basic questions over what type of stored records ECPA applies to can be confusing, given the limited definition of electronic storage. Nor does the statute contain basic protections like a suppression remedy for illegally obtained information or reporting requirements for how often communications are shared with the government.

---

[2] 18 U.S.C. § 2510(15) (2012).
[3] *Id.* at § 2711(2).
[4] Orin S. Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

These problems have not gone unnoticed. Starting in 2007, CDT began working through its Digital Privacy and Security Working Group ("DPSWG") to find common ground on a solution to some of ECPA's problems. In 2010, we announced the formation of the Digital Due Process (DDP) coalition, consisting of nine companies and twelve trade associations, think tanks and advocacy groups. DDP supported four key principles for reforming ECPA – one of which was the warrant for content fix at the heart of S.356. DDP has blossomed today into a broad coalition of more than a hundred groups and companies, including major technology companies, advocacy organizations from the right and the left and grassroots organizations representing millions of members.[5]

Congress has recognized the need for reform, as well. This Committee held a hearing on the issue in 2010 and voted out of committee legislation either identical or similar to S.356 in both 2012 and 2013. The House of Representatives has also weighed in. The companion bill to S.356, H.R. 699, "The Email Privacy Act," is the most cosponsored bill in the House with more than 290 cosponsors including a majority of both the Republican and Democratic caucus.

The federal courts and the tech industry have also attempted to fill the void left by the lack of reform. In 2003, in *Theofel v. Farey-Jones*, the Ninth Circuit clarified confusion in the statute regarding when an email was in electronic storage and rejected the Justice Department's distinction between opened and unopened e-mail.[6] Most significantly, in 2010, in *U.S. v. Warshak*, the Sixth Circuit ruled that people have a reasonable expectation of privacy in email content and that it should only be accessed with a search warrant.[7]

The *Warshak* decision was a watershed. While it technically only applied in the Sixth Circuit, the difficulty in determining where a particular user was located and the persuasiveness of the court's reasoning led most, if not all, major technology companies to adopt a warrant standard for all stored content. Even more significantly, it cast into question the constitutionality of a significant portion of the statute and made the need for reform even more urgent.

---

[5] For a full list, see *Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

[6] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).

[7] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

The Balance in ECPA

At the time of its passage, the goal of ECPA was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement,"[8] and to support the development and use of new types of technologies and services.[9] Congress wanted to encourage the innovation represented by these new technologies and realized that would not be possible if the privacy of users was not protected.[10]

ECPA accomplished that goal by creating a familiar framework – a high level of protection for the content of communication and a lower protection for business records or abandoned communications. Notably, this framework was prescient in recognizing that 3rd parties could and would hold sensitive information that merited warrant protection.

Since this initial balance was struck, we have seen a technological revolution and the result has been a statute that is now much less protective of privacy and hinders innovation.

A short (and probably incomplete) list of the communications content that I store with third parties today 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.

The striking thing about this list is how pedestrian it is. Most Americans could create a similar list; some would likely be able to add many more categories. Yet all of this is protected under a legal framework that is dramatically out of date.

---

[8] H.R. REP. NO. 99-647, at 19 (1986).

[9] S. REP. NO. 99-541, at 5 (1986) (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").

[10] *Id.*; H.R. REP. NO. 99-647, at 19.

Protections are largely reliant on a handful of court decisions and strong government access policies from technology companies.

The need for reform of ECPA to support innovation is equally striking. This Committee is familiar with the importance of cloud computing. Businesses all over the world are looking to cloud-based services for their information management needs in order to save money on equipment and to achieve better computing reliability and data security. Cloud-based services allow companies to expand their computing capacity quickly, which is particularly valuable for start-up businesses and entrepreneurs. Such services give employees the flexibility to share information and collaborate. The global software as services market is expected to reach $106 billion by next year.[11] American companies have been the global leaders in this area, and it has been an engine for U.S.-based innovation, economic growth and job creation.

Currently, ECPA does not provide a solid legal foundation to continue this growth. When businesses contract out to cloud providers, there is a strong argument under ECPA that those cloud providers are offering the services of an RCS and hence the information they store is only protected by a subpoena. Contrast that with the full protection of a warrant offered when someone saves information on her own personal computer. As Fred Humphries, Vice President of U.S. Government Affairs at Microsoft said, "Our goal is simple: the law should treat data stored in the cloud as closely as possible to data that we previously stored in our homes or in our offices."[12]

At the same time, law enforcement's ability to collect information has grown astronomically. It's not just access to the content of communication. Everything we do online – and increasingly offline through our mobile devices – also produces metadata. Our location, with whom we are communicating, our friends and social networks – all of it is accessible to law enforcement under a variety of legal standards, most of which are lower than a warrant backed by probable cause. While increased protections for metadata are not part of S.356, it is important to keep this cornucopia of new information in mind when considering any reform effort. The reality is that we currently live in a golden age of surveillance where the government has access to copious amounts of

---

[11] Louis Columbus, *Roundup of Cloud Computing Forecasts and Market Estimates, 2015*, FORBES (Jan. 24, 2015), http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/.

[12] Microsoft Corporate Blogs, *A day of action to demand ECPA reform*, MICROSOFT (Dec. 5, 2013), http://blogs.microsoft.com/on-the-issues/2013/12/05/a-day-of-action-to-demand-ecpa-reform/.

information about all of us. S.356 is just a level set in one area, returning privacy protections to the content of communications while we continue to see erosions in many others.[13]

Law enforcement has not denied the need for reform in this area. At a hearing earlier this year, FBI Director James Comey said about ECPA, "There is an outdated distinction. For email, over 180 days, I think, under the 1980s statute is treated as something that you could in theory obtain without a search warrant. We don't treat it that way. We go get a search warrant from a Federal judge no matter how old it is. So a change wouldn't have any effect on our practice."[14] Similarly, in a past hearing on reforming the ECPA, the Department of Justice agreed "that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened."[15] Given this acknowledgement that a problem exists – and the reality that there is a constitutional infirmity in the statute protecting all stored communications – it is frustrating that some in law enforcement continue to resist commonsense reform.

The Legislation

The "Electronic Communications Privacy Act Amendments Act" (S.356) does not fix all the problems described above, but it does remedy the constitutional infirmity identified by *Warshak* and provide a strong, consistent and easily administered legal protection for the content of communications.

The key to the protections in S.356 can be found in Section 3. It amends ECPA so that the disclosure of the content of email and other electronic communications by an ECS or RCS is subject to one clear legal standard – a search warrant issued based on a showing of probable cause. The provision eliminates the confusing and outdated "180-day" rule. Section 3 also requires that

---

[13] For more on the golden age of surveillance, see Peter Swire, *Going Dark or a Golden Age for Surveillance?*, CDT.ORG (Nov. 28, 2011), https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/.

[14] *Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary*, 113th Cong. 69 (2014) (statement of the Hon. James B. Comey, Director, Federal Bureau of Investigation).

[15] *ECPA Part 1: Lawful Access to Stored Content: Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Elana Tyrangiel, Acting Assistant of Attorney General, Department of Justice Office of Legal Policy).

the government notify the individual within either 3 or 10 days if their information was disclosed.

Section 3 also reaffirms current law to clarify that the government may use an administrative or grand jury subpoena in order to obtain certain kinds of electronic communication records from a service provider, including a customer's name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

Lastly, the section contains a rule of construction regarding government access to internal corporate email. It states that nothing in the bill precludes the government from using a subpoena to obtain email and other electronic communications directly from a company when the communications are to or from an officer, agent or employee of a company.

Section 4 permits delayed notice under the same standard as current law. A court may extend the delay periods for a period of up to an additional 180 or 90 days at a time (depending on whether an investigation is criminal or civil). Law enforcement may also obtain an order barring providers from disclosing the existence of a warrant.

S.356 also grants new authority to assist government investigations. In cases where there has been a delay, Section 4 requires that service providers notify the government in advance when that time period expires and they intend to notify a customer about the warrant. Current law requires no such advance notice. The purpose of this provision is to ensure that the government has an opportunity to protect the integrity of its investigation and, if warranted, to ask a court to delay the notification, before such notice is given. It also doubles the period for which notice to a user of law enforcement access to communications content can be delayed. Finally, it adds civil discovery subpoenas to the list of subpoenas that can be used to compel disclosure of subscriber identifying information, placing all subpoenas on the same footing

S.356 is also noteworthy for what it does not do. It does not impact national security powers under the Foreign Intelligence Surveillance Act – a rule of construction in Section 6 makes this clear. It does not affect the traditional exceptions that allow law enforcement to access communications without a warrant – exigency, consent and the other exceptions found in 18 USC 2702. Nor does it interfere with the existing process that allows providers to work with the National Center for Missing and Exploited Children to identify and help prosecute child pornography under 18 USC 2258A.

This simple change to the law – treating searches of an individual's inbox the same way we treat searches of her home – is profoundly important to personal privacy and American business while not unduly interfering with law enforcement's ability to protect public safety.

Issues of Special Note

Opponents of S.356 have identified two areas of concern – access by civil agencies and the handling of emergencies. I will address each in turn.

Civil Investigation Carve Out

In a letter to this Committee in April 2013, the Chair of the Securities and Exchange Commission (SEC) stated that a warrant requirement would block the SEC from obtaining digital content from service providers.[16] The SEC is a civil agency and lacks authority to issue warrants, relying instead on subpoenas for investigations. The SEC argued that ECPA reform should allow civil agencies to obtain digital content from service providers without a warrant. However, the SEC's request for new authority is unnecessary and troubling.

The scope of this request is very broad. While the SEC has only requested that all federal civil law enforcement agencies be granted the power to compel emails and other content from service providers, ECPA's provisions have always applied to all government – including state and local agencies.[17] But even if this authority was somehow limited to federal agencies, it would mean that the Internal Revenue Service (IRS), Environmental Protection Agency (EPA), Consumer Financial Protection Bureau (CFPB), and potentially many more agencies would have a new authority to demand a target's emails from service providers without going directly to the target of an investigation.

An effective and time-honored method to access these types of communications in civil investigations already exists. Civil agencies can already obtain digital content with a subpoena issued directly to the target of the investigation – such as a user who sent or received emails. Civil agencies can enforce these subpoenas on individuals in court, and courts can order the user to disclose the data sought under the subpoena.[18] In addition, ECPA already allows civil

---

[16] *See* Letter from the Hon. Mary Jo White, Chair, Securities and Exchange Comm'n, to Sen. Patrick Leahy, Chair, Sen. Judiciary Comm. (Apr. 24, 2013), *available at* https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf.

[17] *See id*. at 3.

[18] *See, e.g.*, FTC v. Sterling Precious Metals, LLC, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013).

agencies to issue preservation orders – without court approval – that direct service providers to prevent deletion of information from a user's account, thereby preventing destruction or alteration of evidence, while a motion to compel is being pursued.[19] ECPA reform would not change any of these existing powers for civil agencies.

In reality, what the SEC is seeking is a new authority. The SEC Chair recently testified that the agency does not obtain digital content from service providers.[20] The SEC has also provided no evidence – despite repeated requests – that it has ever sought content from service providers since the *U.S. v. Warshak* in 2010.[21]

If granted, the authority the SEC seeks would result in a significant erosion of privacy. There are many more potential violations of civil law than criminal law – creating more potential predicates to investigate an individual. If civil agencies are empowered to serve subpoenas on service providers for a target's communications, the service provider may disclose the target's entire account – often years of email communications. This would most likely include information that is irrelevant to the agency's investigation, as well as information that is protected under the target's attorney-client or other privilege, since the service provider would not filter out this information. Finally information gathered as part of a civil process could be shared for use in a parallel criminal investigation – creating a major backdoor to the protections in the bill.[22]

---

[19] 18 U.S.C. § 2703(f). Evidence preservation orders can be issued at early stages of an agency's inquiry, even before launching a formal investigation.

[20] Dustin Volz, *SEC Reveals It Doesn't Use Email Snooping Power It Defends*, NAT'L J. (Apr. 16, 2015), http://www.nationaljournal.com/tech/sec-reveals-it-doesn-t-use-email-snooping-power-it-defends-20150416.

[21] *See* Letter from the Center for Democracy & Technology et al. to the Hon. Mary Jo White, Chair, Securities and Exchange Comm'n 2 (Apr. 9, 2014), *available at* https://cdt.org/files/2014/04/SEC-ECPA-reform.pdf.

[22] For example, Form 1662 of the Securities and Exchange Commission, which is designed to be used with all SEC civil subpoenas, expressly states:

> The Commission often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors. There is a likelihood that information supplied by you will be made available to such agencies where appropriate. Whether or not the Commission makes its files available to other governmental agencies is, in general, a confidential matter between the Commission and such other governmental agencies.

SECURITIES AND EXCHANGE COMMISSION, SEC 1662 (09-14), http://www.sec.gov/about/forms/sec1662.pdf.

Rather than granting civil agencies a new authority to subpoena service providers, Congress could instead clarify and codify agencies' power to obtain digital content from targets. This would be consistent with the principle of technology neutrality – civil agencies can use courts to force targets to respond to subpoenas for digital content stored in the "cloud," just as they can with content stored on a computer hard drive or physical documents stored in a safe.

Changing Rules for Emergency Exceptions

Under ECPA, electronic communications providers cannot give content and sensitive user information to the government absent a court order, subpoena or warrant. However, the law does contain an exception so that in an emergency situation involving danger of death or serious bodily harm, the provider may disclose content and user records to law enforcement absent the legal process that would otherwise be required.[23] Because these requests receive no independent judicial oversight, providers have discretion to assess whether the request is proper and should be fulfilled absent the required legal process. As ECPA reform legislation continues to gather strong support, some have called for a new provision that would change this rule to mandate compliance with any emergency request for user data or content. Such a change is unnecessary, and would raise significant privacy and security problems.

Although most emergency requests are appropriate and receive speedy compliance, there are enough instances where requests are deemed improper that misuse of the emergency authority should not be ignored. Providers' authority to evaluate the legitimacy of these requests is a crucial check against this type of abuse. For example, in 2014, Google rejected 94 out of 342 requests.

The government has previously abused its ability to engage in emergency requests. A 2010 Department of Justice Inspector General report stated that the Inspector General "found repeated misuses of [the FBI's] statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions."[24] Based on this, the Inspector General report recommended Congress consider "appropriate controls" on the FBI's ability to obtain records in emergency situations. With mandatory compliance and no judicial oversight, such abuses could become more frequent.

---

[23] *See* 18 U.S.C. §§ 2702(b)(8), (c)(4).

[24] *See* OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 268 (Jan. 2010), *available at* https://oig.justice.gov/special/s1001r.pdf.

Right now, emergency requests are very rare. America's largest Internet and electronic communications companies only receive a small number of requests. For example, Google only received 342 emergency requests[25] and Microsoft only received 475 requests[26] throughout all of 2014. In comparison, Google received 20,280 subpoenas and search warrants and Microsoft received 12,364 similar requests during that same year.

In the event that a provider denies a request for an emergency disclosure without legal process, the government still has options available. Law enforcement can revise its request to obtain content or data if appropriate justification has not been provided. Additionally, government entities may also seek information through ECPA's mandatory disclosure provisions without delay. In all judicial districts, a magistrate is available for after-hours requests that require immediate action, and Rule 41 of the Federal Rules of Criminal Procedure stipulates for telephonic search warrants to be obtained at all hours.

Requiring providers to comply with any emergency request would also endanger data security by interfering with providers' ability to assess the validity of requests. Data thieves regularly attempt to take customer information by posing as law enforcement and demanding that data be provided pursuant to an emergency. Congress criminalized this activity because of the serious threat it poses.[27] Providers must have the capability to ensure that requests are not fraudulent and prevent disclosure of user data to unauthorized third parties. Mandating disclosure in response to all emergency requests and removing discretion to appeal for clarification, additional information, or a more secure method of disclosure would undercut providers' ability to protect users' sensitive information.

The current system for disclosure of user information and content pursuant to emergency requests absent a court order works effectively. It protects both public safety and user privacy and security, and should not be changed. Providers take seriously both safety needs and their users' privacy rights. Voluntary disclosure that assesses government requests allows them to effectively protect both.

---

[25] *See Google Transparency Report: Security and Privacy*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US/.
[26] *See Microsoft Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.
[27] *See* 18 U.S.C. § 1039 (2012).

We thank the Committee for holding a hearing on this important issue and urge you to act swiftly to mark-up S.356, "Electronic Communications Privacy Act Amendments Act of 2015."