



September 16, 2015

The Honorable Chuck Grassley
Chairman, Senate Judiciary Committee
224 Dirksen Senate Office Bldg.
Washington, D.C. 20001

The Honorable Patrick Leahy
Ranking Member, Senate Judiciary Committee
224 Dirksen Senate Office Bldg.
Washington, D.C. 20001

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

**RE: Senate Judiciary Committee Hearing on “Reforming the
Electronic Communications Privacy Act”**

Dear Chairman Grassley and Ranking Member Leahy:

We write to thank you for holding this hearing on reforms to the Electronic Communications Privacy Act of 1986 (“ECPA”), and specifically the legislation pending before this committee, S. 356, the Electronic Communications Privacy Act Amendments Act.¹

We hope this hearing will drive new momentum behind desperately needed—and overwhelmingly popular—ECPA reforms. Almost a quarter of the Senate has sponsored the ECPA Amendments Act and more than 300 House members have done the same with that chamber’s bill. Clearly, Americans at all points on the political spectrum support the basic premise that our email—just as with a handwritten love letter—should not be read by the government absent a warrant, supported by probable cause.

This premise should not be controversial, and we urge the committee and Congress to act swiftly in enacting these important reforms.

The ACLU has commented repeatedly on the need to bring our electronic communications privacy laws in line with modern technology. Specifically, we have explained how information privacy law must finally grapple with the dramatic growth of third-party cloud computing, where our most essential and sensitive electronic communications—like email, online word processing and instant messaging—are stored in remote data centers, where they may receive significantly less privacy protection.

¹ The House version of this bill is H.R. 699, the Email Privacy Act. We refer to the Senate legislation as the ECPA Amendments Act, and both S. 356 and H.R. 699 together in this letter as “ECPA reform legislation.”

For instance, under existing law—based on technical architecture that predates even the World Wide Web—emails older than 180 days or that have been opened can be accessed under a legal standard significantly lower than the warrant requirement for emails that are unopened or have been in electronic storage for fewer than 180 days.²

The incongruity in such a rule is not lost even on law enforcement. “I think there’s no doubt that there are going to be certain modifications made [to ECPA],” said president of the FBI Agents Association in 2013. “I also know that it’s the position of the Department of Justice that the 180-day distinction is an artificial one.”³

The ACLU has testified repeatedly on the need for ECPA reform, and how basic American values—like the right to be left alone, the presumption of innocence until proof of guilt, the right to equal treatment under law, the right to criticize government without fear of retaliation, and many others—are served by a warrant requirement before law enforcement can access our most sensitive electronic communications.⁴

Today, we offer brief additional comments responding to some of the arguments offered by critics of ECPA reform legislation. Specifically, we note:

- ECPA reform legislation will retain law enforcement’s ability to obtain electronic communications in emergencies, and we urge Congress to resist imposing a mandatory disclosure regime that could be used to short circuit due process in non-emergencies.
- Civil agencies will suffer no injury to their investigative authority through ECPA reform. Indeed, agencies like the Securities and Exchange Commission (“SEC”) should *not* be able to demand electronic communications from third parties with an administrative subpoena. Civil agencies do not have criminal investigative powers, and they should not be able to obtain emails, which could then be used in a parallel criminal investigation, under a standard lower than probable cause.

² 18 U.S.C. 2703(a)-(b) (2012). If the government entity provides notice to the subscriber or customer, it can access email content with an administrative, trial or grand jury subpoena, or with a court order under § 2703(d), which requires only a showing of specific and articulable facts that the emails are relevant and material to an ongoing criminal investigation. Notice may be delayed under 18 U.S.C. § 2705 (2012). ECPA also permits government entities to access electronic communications records without notice using, depending on the records sought, a § 2703(d) order or subpoena. 18 U.S.C. § 2703(c)(1)-(2) (2012).

³ The Communicators (C-SPAN television broadcast Apr. 14, 2013), *available at* <http://www.c-span.org/video/?311872-1/communicators-grover-norquist-laura-murphy>.

⁴ See, e.g., The Electronic Communications Privacy Act, Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 113th Cong. (2013) (testimony of Catherine Crump); The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (2010) (testimony of Laura W. Murphy, et al.).

- The concern expressed by the SEC that ECPA reform would lead to the destruction of evidence is misplaced. Agencies would fully retain their authority under 18 U.S.C. § 2703(f) (2012) to issue a preservation order. Once issued, such an order would prevent third party communications providers from deleting or altering relevant material. The agency would then have the power to go to court to force the subscriber to turn over responsive material, much as in private civil litigation.⁵

We address each point in turn below.

1. ECPA Reform Retains the Emergency Exception, Which Should Not Be Expanded to Mandate Disclosure of Electronic Communications

Under both current law and the ECPA reform legislation, law enforcement has the ability to go to a communications provider and ask for the voluntary disclosure of electronic records and communications. This power is limited by the law’s requirement that a provider only disclose material in response to such a request if the provider “in good faith, believes that an emergency involving danger of death or serious physical injury” requires disclosure.⁶

Some now seek to make disclosure *mandatory* for providers receiving emergency requests for electronic records and communications.

There are compelling reasons to give providers the discretion to resist law enforcement requests when they believe such requests to be improper. First, there is an incentive for law enforcement to push the envelope and to use the authority to avoid seeking judicial review of a request.⁷ Not only does this create obvious civil liberties concerns, but it could lead to a “the sky is falling” dynamic where increasingly skeptical providers are more resistant to law enforcement requests in bona fide emergencies than they otherwise would be.

⁵ Both S. 356 and H.R. 699 include a rule of construction that expressly preserves the ability of civil agencies to use administrative subpoenas to seek records directly from the “originator, addressee, or intended recipient” of the communications. This has the added benefit of, much as in civil litigation, preserving the ability of the sender or recipient of the communications to review for privilege or attorney work product. See S. 356, 114th Cong. § 3 (2014) (adding a new § 2703(h) to preserve agency administrative subpoena power).

⁶ 18 U.S.C. § 2702(b)(8), (c)(4) (2012). Indeed, the standard by which providers may disclose communications and records was lowered in 2006 in the USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 107(b)(1)(B), 120 Stat. 192 (2006) to allow disclosure with a “good faith” belief.

⁷ This concern is not theoretical. In a comprehensive 2010 investigation, the inspector general at the Department of Justice found that, in the years following the 9/11 attacks, the FBI repeatedly misused so-called “exigent letters” and other informal requests to compel the production of telephone records and other material. In many cases, the FBI presented the request as exigent when it was not, in fact, an emergency. In other cases, the FBI failed to provide the relevant details and the providers just assumed that the requests were exigent. Dep’t of Justice, Office of the Inspector General, A Review of the Federal Bureau of Investigation’s Use of Exigent Letters and Other Informal Requests for Telephone Records 257-72 (2010) (detailing the IG’s findings with respect to improper FBI use of exigent letters and other informal requests in violation of § 2702’s emergency exception).

Additionally, mandatory emergency disclosure coupled with the potential for thieves to impersonate law enforcement when “dialing for data” poses serious privacy concerns. Recognizing the danger of thieves calling service providers and asking for customer records under false pretenses, Congress enacted the Telephone Records and Privacy Protection Act of 2006,⁸ which makes it a federal felony, punishable by up to 10 years in prison, to use “pretexting” to obtain call records.⁹ Tellingly, the statute includes heightened penalties if the records are used to facilitate cyber-stalking, one of the primary concerns driving the legislation.¹⁰

It is precisely in these cases—emergency requests by individuals claiming to be law enforcement—where communications providers must be given the discretion to resist the request. Providers should be free, and should be encouraged, to deny requests when they believe the requester is not a member of law enforcement or where a requester’s status cannot be determined. This is particularly important given the unique time pressures and heightened emotion attendant in an emergency request.

Finally, emergency requests are (thankfully) quite rare—on the order of a couple of hundred requests a year, versus tens of thousands of subpoenas and search warrants.¹¹ Providers comply with the vast majority—indeed more than they do formal process. In those cases where providers do not comply, it is often because they do not have any responsive records. And, where providers do not comply because they do not believe a genuine emergency exists or they suspect pretexting, denying the request is the right outcome for both privacy and public safety.

2. A Warrant Exception for Civil Agencies Subverts the Whole Purpose Behind a Warrant, and Would Swallow the Warrant Rule for Law Enforcement

In April 2013, SEC Chair Mary Jo White sent a letter to this committee raising concerns with ECPA reform legislation.¹² In it, the SEC chair warned against the consequences of amending ECPA to eliminate the artificial distinctions current law sets up with respect to, for instance, requiring a probable cause search warrant for emails that are less than 180 days old but a lower standard of cause for emails that are older than 180 days.

Chairwoman White noted that the SEC has, historically, relied on its administrative subpoena authority to access emails *from a third party communications provider* (a key distinction) that are

⁸ Pub. L. No. 109-476, 120 Stat. 3568 (2007)

⁹ 18 U.S.C. § 1039(a) (2012).

¹⁰ § 1039(d).

¹¹ See Ctr. For Dem. & Tech., Issue Brief: Weakening ECPA Reform by Altering Emergency Exception Rule Unnecessary and Problematic (2015), <https://cdt.org/insight/issue-brief-weakening-ecpa-reform-by-altering-emergency-exception-rule-unnecessary-and-problematic/>.

¹² Letter from Mary Jo White, Chair, Sec. and Exch. Comm’n, to the Honorable Patrick Leahy, Chairman, S Judiciary Comm. (April 24, 2013), *available at* <https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf>.

older than 180 days. White then noted a 2010 court case, *United States v. Warshak*,¹³ which, quite rightly, held that emails are protected by the Fourth Amendment's prohibition against unreasonable searches and seizures. White stated that ECPA reform would "codify *Warshak* [nationwide], permitting federal government entities to obtain the content of emails from ISPs only if it were to obtain a warrant pursuant to the Federal Rules of Criminal Procedure."¹⁴

This is a feature, not a bug. In point of fact, the SEC should *not* be able to compel the disclosure of email content from a third party service provider under an administrative subpoena, just as it has never been allowed to use a subpoena to demand an email that has been in storage for less than 180 days. While that distinction may have made intuitive sense in 1986, it makes little to no sense today, when cloud storage is cheap and many of us retain a decade of email in one remotely stored Gmail account.¹⁵

Additionally, the SEC is a civil agency. It does not have federal criminal law enforcement power. Just as it cannot secure an arrest warrant for the target of an investigation, it cannot secure a valid search warrant based on probable cause (to believe that a *crime* has been committed). And if ECPA protects emails stored for less than 180 days from access without a warrant, there is no technical or legal reason today why it should not protect all emails.

The SEC claims that it would be unduly burdensome to rely on a parallel criminal investigation at the Department of Justice to secure warrants for material held by third party ISPs for two reasons. One, the Department of Justice may only issue warrants in its own cases, not those brought by the SEC. And, two, sometimes the Justice Department does not feel the evidence warrants the opening of a parallel criminal investigation.¹⁶

But, again, both of these are features, not bugs. The SEC serves a regulatory function and it may seek only civil redress against the targets of its investigations. It would be both troubling and incongruous for the DOJ to be doing the bidding of the SEC. And, if the DOJ cannot establish the predicate facts for a finding of possible *criminal* wrongdoing, not opening an investigation is the right outcome for both civil liberties and government efficiency.

¹³ 631 F.3d 266, 288 (6th Cir. 2010).

¹⁴ *Id.* at 1-2.

¹⁵ Precisely the opposite assumptions informed the structure of ECPA as it stands today. Emails left in the primordial cloud of 1986 were presumed to be "abandoned" by the user because, given the high cost of storage, it made little economic sense to keep emails anywhere but on one's personal computer. See Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. Penn. L. Rev. 373, 376 (2014) ("The incredible growth of stored records renders ECPA's structure exactly backwards for the operation of modern computer networks.").

¹⁶ *White Letter*, *supra* note 12, at 2.

Finally, the SEC's claimed exception would not be limited to the SEC. Most government agencies have some form of administrative subpoena power,¹⁷ and the scope of that power is vast.¹⁸ The rationale articulated in the SEC's letter would permit the use of administrative subpoena power by any other civil agency that possesses it to secure emails from a third party provider under a standard less than probable cause, and to then provide these emails to criminal investigators in a parallel investigation.

This exception would swallow the proposed rule—that, given the modern privacy interests in cloud based communications, they should not be subject to compelled disclosure by the government absent a warrant based on probable cause.

3. Concerns About Spoliation Are Misplaced

Finally, the SEC has pointed to fears that the target of an administrative subpoena would either delete emails or simply fail to fully comply with a subpoena. But, ECPA itself permits the issuance of a preservation order that would prevent third party ISPs from deleting or altering emails or other material in a target's account.¹⁹ The agency itself issues the order, without going through a judge, and may do so at the earliest stages of an inquiry.

Once the preservation order is issued, the agency is fully within its rights to issue a subpoena to the sender or recipient of a relevant electronic communication and demand that it be turned over. The distinction, which is important, is that the individual in control of the communication is the one that must obtain it from her ISP and then deliver it to the agency.

With respect to individuals who fail to fully comply with such a subpoena, the consequences are quite severe, including contempt. Additionally, the SEC has only identified one case where the target of an earlier subpoena failed to disclose a responsive email that was subsequently discovered through a third-party ISP subpoena, and no case post-*Warshak*.²⁰

While we do not discount the possibility that the target of a subpoena would fail to be completely forthcoming with the SEC, the remote threat of such misconduct should not lead Congress to

¹⁷ Dep't of Justice, Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities apps. A-C, *available at* http://www.justice.gov/archive/olp/rpt_to_congress.htm.

¹⁸ Faced with a challenge to an administrative subpoena, federal courts apply a deferential "reasonableness" standard that asks only whether the agency has a legitimate purpose, whether the material is relevant to that purpose, whether the agency already has the information and whether the agency has followed the appropriate internal procedures before issuing the subpoena. *Sec. and Exch. Comm'n v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 741-42 (1984); *United States v. Powell*, 379 U.S. 48 (1964).

¹⁹ 18 U.S.C. § 2703(f) (2012).

²⁰ *See White Letter*, *supra* note 12, at 2; 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>.

create a civil agency warrant exception that would swallow the proposed warrant requirement. That would render ECPA reform stillborn.

The better approach, which is the one taken by both S. 356 and H.R. 699, is to clarify that the SEC and other civil agencies may still demand that individual targets of their investigations be compelled to secure responsive material from third-party ISPs and turn it over to the investigating agency. This has the added benefit of protecting privileged or work-product communications from improper scrutiny by the investigating agency.

4. Conclusion

The internet of 2015 bears little resemblance to that of 1986, when even the advent of dial-up services like CompuServe or AOL was several years away. Today, users store billions of emails—containing the most sensitive information about personal relationships, political affiliations, religious convictions and physical health—in the cloud.

In 1986, Congress was animated by a concern over the direct interception of emails as they moved from a remote storage provider to an individual's personal computer. Today, ECPA reform is compelled by the fact that many of us keep our digital lives in a cloud based email platform, which should be free in its entirety from government scrutiny absent evidence of criminal activity.

We applaud the committee for holding this important hearing, and we urge Congress to move swiftly in enacting these crucial reforms. And we urge Congress to ensure that ECPA advances without controversial amendments, including those that seek to undermine encryption efforts.²¹ Please do not hesitate to call or email Legislative Counsel/Policy Advisor Gabe Rottman at grottman@aclu.org or 202-544-1681 with any questions or comments.

Sincerely,



Karin Johansen
National Political Director



Gabe Rottman
Legislative Counsel and Policy Advisor

²¹ We would oppose any proposal that would remove the protections for strong backdoor-free encryption; require, request or incentivize technology companies or communication providers to weaken encryption to enable greater government surveillance; or incentivize, request or mandate that technology companies retain information or metadata to circumvent encryption efforts.