CENTER FOR DEMOCRACY & TECHNOLOGY

07/07/15

Issue Brief: No special powers for civil agencies under ECPA

Under the Electronic Communications Privacy Act (ECPA) of 1986, law enforcement agencies can force service providers (such as email service providers) to turn over digital content (such as email or social networking messages) that is more than 180 days old.[1] This outdated law creates bizarre results for the digital age: law enforcement needs a warrant to obtain physical papers in a drawer or files on a computer hard drive, regardless of age, but only a subpoena to obtain online messages and documents held in the "cloud" that are older than six months.

A large and diverse coalition of American businesses and civil society groups spanning the political spectrum has called for an update to ECPA.[2] This coalition, of which CDT is a founding member, supports a clear and consistent warrant standard for government access to digital content held by service providers, regardless of whether the content is more than 180 days old – with appropriate exceptions for emergency situations. Rep. Yoder's bipartisan "Email Privacy Act," as well as Sen. Lee's bipartisan "ECPA Amendments Act" would make this crucial reform to ECPA.[3]

SEC wants a new warrantless snooping power

In letter to Senate Judiciary Committee, 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.[4] The SEC is a civil agency and lacks authority to issue warrants, relying instead on subpoenas for investigations. The SEC argues that ECPA reform should allow civil agencies to obtain digital content from service providers without a warrant. However, the SEC's request for a warrantless snooping power is unnecessary and troubling:

- **Every civil agency may receive the new warrantless snooping power.** The SEC has requested that all federal civil law enforcement agencies be granted the power to compel emails and other content from service providers without a warrant.[5] That means the Internal Revenue Service (IRS), Environmental Protection Agency (EPA), Consumer Financial Protection Bureau (CFPB), and potentially many more agencies would have new authority to demand a target's emails from service providers without going directly to the target. If state and local agencies are also included, the number of government offices with warrantless access to individuals' email would be quite large.

- **Civil agencies can get emails from users with a subpoena.** 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.[6] In addition, ECPA

[1] 18 U.S.C. 2703(a)-(b).
[2] Digital Due Process, Who We Are, available at http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last accessed Jul. 2, 2015).
[3] H.R. 699, 114th Cong. (2015). S. 356, 114th Cong. (2015).
[4] See Letter from the Honorable Mary Jo White to Senator Patrick Leahy, Apr. 24, 2013, available at https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf.
[5] See Letter from the Honorable Mary Jo White to Senator Patrick Leahy, Apr. 24, 2013, pg. 3, available at https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf.
[6] See, e.g., *FTC v. Sterling Precious Metals, LLC*, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013).

already allows civil agencies to issue preservation orders – without court approval – that direct service providers to freeze a user's account, preventing destruction or alteration of evidence, while a motion to compel is being pursued.[7] ECPA reform would not change any of these existing powers for civil agencies. What the SEC wants is a new authority to circumvent users and court processes and instead demand emails from third party service providers.

- **The SEC does not obtain emails from service providers.** The SEC's demand for authority to obtain digital content from service providers without a warrant would be an expansion of the agency's practice since at least 2010. The SEC Chair recently testified that the agency does not obtain digital content from service providers.[8] 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* case in 2010, in which the Sixth Circuit held that the government violated the Fourth Amendment by compelling a service provider to turn over emails without a warrant.[9]

- **Forcing disclosure by service providers would erode privacy.** 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. This would include information that is irrelevant to the agency's investigation, and potentially information that is protected under the target's attorney-client privilege, since the service provider would not filter out this information. As a result, individual privacy would be damaged and the risk of government abuse would increase.

Alternative: Clarify civil agencies' powers to subpoena targets

Rather than granting civil agencies 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.

This clarification should be part of ECPA reform legislation that requires government to use a warrant to obtain a user's content from service providers. Coupled with the evidence preservation authority already in ECPA, civil agencies would preserve the power they need to complete investigations.

Warrant protection for emails and other content stored with third parties has massive support in Congress, as well as among businesses, civil society, and the public.[10] Requests for a new, unnecessary, and invasive warrantless snooping power should not stand in the way of ECPA reform.

END

For more information, please contact Chris Calabrese, CDT Vice President for Policy, at ccalabrese@cdt.org or 202-637-9800.

[7] 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.
[8] Dustin Volz, *SEC Reveals It Doesn't Use Email Snooping Power It Defends*, National Journal, Apr. 16, 2015, http://www.nationaljournal.com/tech/sec-reveals-it-doesn-t-use-email-snooping-power-it-defends-20150416.
[9] See Letter from the Center for Democracy & Technology et al. to the Honorable Mary Jo White, Apr. 9, 2014, pg. 2, available at https://cdt.org/files/2014/04/SEC-ECPA-reform.pdf.
[10] See Mark Stanley, *A Majority of the House Now Supports ECPA Reform*, Center for Democracy & Technology, Jun. 18, 2014, https://cdt.org/blog/a-majority-of-the-house-now-supports-ecpa-reform.