KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

REGULATORY AGENCIES DO NOT NEED ADDITIONAL AUTHORITY TO ACCESS STORED COMMUNICATIONS

May 30, 2013

S. 607, the Leahy-Lee bill, would amend the Electronic Communications Privacy Act (ECPA) to require government agencies to obtain a warrant in order to compel service providers to disclose email and other documents stored on behalf of subscribers. Currently, ECPA requires a warrant for email less than 180 days old, but allows the government to use a subpoena, served on the service provider, to compel disclosure of email more than 180 days old. Current law also allows use of a subpoena to compel disclosure of other documents stored online regardless of age (calendars, drafts, documents being stored or shared privately for collaboration in the cloud). The Sixth Circuit has held ECPA unconstitutional to the extent that it allows access to email from a service provider with less than a warrant, and most large providers have already applied that rule nationwide.

Some federal regulatory agencies, led by the SEC, have complained that, since they have no warrant authority, codifying the warrant requirement would limit their ability to conduct investigations. However, ECPA already prohibits regulatory agencies from obtaining newer email from third party service providers; the Leahy-Lee bill will only extend that rule to older email and other stored documents regardless of age. Moreover, with respect to both older and newer email, regulatory agencies already have substantial power to identify user accounts, freeze those accounts to prevent destruction or alteration, and use subpoenas served on the account owner to force disclosure.

I. The SEC Proposal

In a letter dated April 24, 2013, the SEC Chair argued that regulatory agencies should be given the power to obtain court orders requiring service providers to disclose the content of communications stored on behalf of third parties. See https://www.cdt.org/files/pdfs/Leahy-ECPA-Letter-FINAL.pdf. The SEC wants to get documents from service providers without giving the target an opportunity to cull the records for relevancy, assert any privileges, or otherwise raise any objections. The third party service providers, of course, would be in no position to assess relevancy or privilege but rather would be compelled to disclose everything they hold regardless of relevancy or sensitivity. The SEC proposal is not limited to that agency alone. If it were to be adopted it would likely be

extended to all regulatory agencies - the IRS, EPA, FTC, CFPB and hundreds of others.[1]

II. The SEC Proposal Would Fundamentally Alter Civil Regulatory Investigations

Until recently, most businesses stored most of their records locally. (We're not referring here to bank records, payroll data, or transactional records held by third parties. The focus of ECPA reform is on one-to-one communications such as email and documents that used to be stored on local servers.) As individuals and businesses embrace cloud-based services for reasons of cost, flexibility, convenience, and security, huge amounts of personal and proprietary data are being stored indefinitely in the Internet "cloud." As part of this revolution, distinctions are blurring between what is stored locally and what is stored remotely. American companies have been global leaders in development and adoption of cloud-based computing.

The SEC proposal would exploit this development to reap a windfall for government power, by allowing civil regulatory agencies to directly access sensitive private and proprietary content without giving the record subject the opportunity to review the data and contest overbroad or abusive requests.

III. The SEC Proposal Will Result in Inefficiencies and Overproduction of Irrelevant and Privileged Data

When data was stored locally, government agencies could compel compliance with their subpoenas, but the target had the first opportunity to compile its records, review them, select the relevant data, and assert any privileges. The same rules applied whether documents were stored in file cabinets on site, in off-site storage, on the company's local network, or on the network of its cloud provider.

However, if disclosure demands could be served directly on service providers, all of this careful vetting and compiling of data would go out the window. Service providers could not know what is relevant to an investigation and what is not, and what is privileged and what is not, nor should they be put in the position of having to decide. Instead, service providers would be forced to overproduce, turning over to the government all of the target's documents whether or not they are relevant. This might include personal emails an employee may have exchanged with his spouse, trade secrets, and correspondence with company lawyers. Especially in the age of cloud storage, this could result in huge amounts of irrelevant but sensitive data being disclosed to the government.

IV. The Courts Have Effectively Enforced Civil Subpoenas Against Account Owners

Recognizing these risks and inefficiencies, courts in civil proceedings have consistently ruled that civil subpoenas for email and other content stored in the cloud should be served directly on

[1] See U.S. Department of Justice, "Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities," http://www.justice.gov/archive/olp/rpt_to_congress.pdf (identifying approximately 335 subpoena authorities held by various federal entities under current law).

the party that sent or received the email or created the content.[2] Moreover, the cases have proved that courts can compel individuals and companies to consent to the disclosure of their data or can impose other sanctions on non-compliant targets. See, e.g., Mintz v. Mark Bartelstein & Assocs., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Defendants may request documents reflecting the content of Plaintiff's relevant text messages, consistent with the SCA, by serving a request for production of documents on Plaintiff pursuant to Rule 34. … Of course, Plaintiff may raise privacy or other objections to any Rule 34 document request … ."); O'Grady, 139 Cal. App. 4th, 1423, 1446 (2006) ("Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions.").

In one recent case involving an administrative agency, FTC v. Sterling Precious Metals, LLC, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013), the court stated:

> The undersigned finds the *Flagg* court's reasoning to be persuasive. In the present case, the FTC is not asking for information proprietary to the web host. Rather, it only requests that compartmentalized information relevant to the operation of Sterling's website. As a customer of its web host, Sterling surely has the contractual right to obtain that data. Accordingly, that information is within its control under Rule 34 and must be provided to the FTC. Moreover, the Court notes that in this context, complying with the request would not impose any great burden on Sterling. Accordingly, the FTC's motion will be granted as to Request 17. Sterling may either obtain the information from its web host and then turn it over to the FTC, or alternatively, provide the FTC with written consent to obtain its code from the relevant party(ies).

The ECPA reforms in the Leahy-Lee bill, S. 607, would preserve that approach. S. 607 would also preserve current rules allowing administrative agencies to use subpoenas to compel service providers to disclose subscriber identifying information. This allows the government to determine the existence of possibly relevant information, so that subpoenas can be then served on the subscribers to actually obtain the content.

V. SEC Already Has Substantial Powers to Preserve, Identify and Obtain Electronic Data

The SEC letter understates the powers already available under ECPA to the SEC and other regulatory agencies. The letter notes three concerns, all of which are already addressed under current law:

---

[2] *Flagg v. City of Detroit,* 252 F.R.D. 346 (E.D. Mich. 2008) (finding that a Rule 34 request for production of documents served on a party for any materials in its custody *or control* was the "more straightforward path" to discovery of messages stored by a service provider). See also *O'Grady v. Superior Court,* 139 Cal. App. 4th 1423 (2006) http://www.internetlibrary.com/pdf/OGrady-Apple-Cal-Crt-App.pdf:

> Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure storage, and who should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent. This does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted.

- Persons who violate the law frequently do not retain copies of incriminating communications;
- They may choose not to provide e-mails in response to Commission subpoenas;
- Individual account holders sometimes delete responsive e-mails.

A. Regulatory agencies already have the power to protect data against destruction

ECPA authorizes any governmental entity, including a regulatory agency, to require an ISP or other service provider to preserve any evidence in its possession to prevent deletion of the data while access is being litigated. 18 USC 2703(f). These preservation demands can be issued by any agency, in any kind of matter, without even a showing of need or relevance, and they can be issued at the earliest stages of an investigation.

B. Regulatory agencies already have the power to prove that a target has an account

ECPA already allows any regulatory agency to issue administrative subpoenas to any ISP or service provider to compel disclosure of account information (everything except the contents of communications). S. 607 would not affect this authority. The information that can be obtained with an administrative subpoena includes dates of service, types of service utilized, and records of session times and durations. With this information, the agency can get a good picture of what services an individual or entity used and during what time periods, including when the person accessed his account, making it impossible for the individual to claim, in response to a subpoena, that he has no responsive records.

C. The records of bankrupt entities can be disclosed by the trustee

In Chapter 7 and Chapter 11 bankruptcies, the bankruptcy trustee acquires control over all the assets of the bankrupt entity and has full power to access the email accounts of the bankrupt corporation and to comply with any subpoenas for email or documents stored electronically by the bankrupt entity.[3]

Armed with data preservation plus evidence of the usage of an account, the government can then use the same methods it uses to compel compliance with any of its subpoenas for any information in the possession or control of a target.

[3] As the Supreme Court said in *Commodity Futures Trading Comm. v. Weintraub,* 471 U.S. 343, 352-53 (1985), "The powers and duties of a bankruptcy trustee are extensive. Upon the commencement of a case in bankruptcy, all corporate property passes to an estate represented by the trustee. … Moreover, in reorganization, the trustee has the power to 'operate the debtor's business' unless the court orders otherwise. … Even in liquidation, the court 'may authorize the trustee to operate the business' for a limited period of time. … [I]t is clear that the trustee plays the role most closely analogous to that of a solvent corporation's management." In Weintraub, the Court held that the bankruptcy trustee has the power to waive the attorney-client privilege of the corporation. Surely, the trustee also has the power to turn over corporate email in response to a subpoena (and to waive or assert any privileges in those records on behalf of the corporation).

Summary

Allowing regulatory agencies to obtain court orders against service providers for the content created by third parties is unnecessary and would diminish privacy, threaten proprietary information, and impose an immense burden on those service providers.

For more information, contact Greg Nojeim, CDT, gnojeim@cdt.org, 202-407-8815.