S.607: Keeping Regulatory Agencies Armed, but Not Dangerous

by Greg Nojeim [1]
June 25, 2013

This summer, Congress is expected to consider S.607, legislation by Senators Patrick Leahy (D-VT) and Mike Lee (R-UT) that would amend the 27-year-old Electronic Communications Privacy Act (ECPA) to require government agencies to obtain a warrant before compelling service providers to disclose emails and documents stored in the cloud on behalf of subscribers. The bill would be a huge win for privacy at a time when it is suffering huge losses at the hands of the NSA.

However, some regulatory agencies are seeking an exception that would partially gut the bill. They complain that since they have no warrant authority, S.607 would limit their ability to conduct investigations. In letter [2] dated April 24, 2013, the SEC argued that regulatory agencies should have the power to obtain court orders requiring service providers to disclose the content of communications stored on behalf of third parties. It would empower the IRS, EPA, FCC, FEC, CFPB and every other regulatory agency to obtain communications content without meeting the probable cause standard the bill would establish, making governmental authority in *civil* investigations exceed its authority in *criminal* investigations. The FBI would need a warrant if it wanted to read your email for a murder investigation, but the IRS wouldn't need a warrant to read your email in a civil tax investigation to assess whether, for example, you took a deduction that weren't entitled to take. This should not be.

ECPA already prohibits regulatory agencies from obtaining newer emails from third party service providers; the Leahy-Lee bill would only extend that rule to older email and other stored documents. Furthermore, most large communications service providers follow the Sixth Circuit ruling in U.S. v. Warshak, which determined that the Fourth Amendment protects email. They already require warrants for all email regardless of age. Creating an exception to the warrant requirement in S. 607 for civil investigations would upset, not preserve, the status quo.

It would also turn civil investigations into fishing expeditions. Unlike the target itself, third party service providers are in no position to assess the relevancy or sensitivity of the materials they hand over. As a result, they will overproduce by turning over everything in the subject's account, and the subject of the investigation would have no opportunity to review the data and contest overbroad or abusive requests. Especially in the age of cloud storage, this could result in huge amounts of irrelevant but sensitive data being disclosed during an investigation.

For this very reason, courts in civil proceedings consistently rule that civil subpoenas for email and other content stored in the cloud should be served directly on the party that sent or received the email or created the content. Courts can compel individuals and companies to consent to the disclosure of their data or can impose other sanctions on non-compliant targets. Current rules also enable administrative agencies to use subpoenas to compel service providers to disclose subscriber identifying information. This allows the agency to determine the existence of possibly relevant information, so it can then serve a subpoena on the subscriber to actually obtain the content.

The SEC apparently does not feel these powers, which would be preserved under S.607, are sufficient. It argues that people who violate the law frequently do not retain copies of incriminating communications. However, regulatory agencies already have the power to protect data against destruction: They can require an ISP or any other service provider to preserve any evidence in its possession under 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.

The SEC also complains that individual account holders sometimes delete responsive emails. But, when this happens, regulatory agencies can issue administrative subpoenas to any ISP or service

provider to compel disclosure of account information. This tells the agency what services an individual or entity used, and when it used each, making it impossible for the target to claim that it has no responsive records.

Finally, the SEC claims that an unavailable target may not to provide emails in response to Commission subpoenas. However, in some cases such emails can be turned over by a different party. In bankruptcy proceedings, for example, the trustee may disclose the records of bankrupt entities.

Of course, the main problem with the SEC's proposal is not that it is unnecessary. It would diminish privacy by exposing personal and proprietary information that has nothing to do with the investigation at hand. S.607 provides the privacy protections users demand for the documents they email or store in the cloud, while preserving the legal framework already in place that allows agencies to conduct thorough, efficient and fair investigations. Agencies like the SEC and the IRS are already armed with substantial investigative authorities; we don't need to make them any more dangerous to privacy than they already are.

For more information, see our report [3].

Links:
[1] https://www.cdt.org/personnel/greg-nojeim
[2] https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf
[3] https://www.cdt.org/files/pdfs/Regulatory-Agencies-Access-Stored-Communications.pdf