The SEC Wants New Authority to Access Emails, But the One Case Cited by the Agency Suggests That New Powers Are Not Needed and Would Pose Serious Risks if Granted

July 15, 2013

The Securities and Exchange Commission is objecting to a long-overdue reform of the Electronic Communications Privacy Act (ECPA). The SEC is arguing that civil regulators, instead of continuing to serve subpoenas on the targets of their investigations, as they traditionally have done, should have the power to obtain documents directly from Internet companies providing storage services on behalf of their customers.

However, the sole case the SEC cited to support this argument actually shows that the need for new authority is greatly overstated, if not totally unjustified. Indeed, the case cited by the SEC illustrates precisely the risk of indiscriminate production of personal emails that we have warned about.

Background – S. 607 and the Letter from the SEC Chair

The bill at issue is S. 607, the ECPA Amendments Act, bipartisan legislation that will stop the government from reading emails and other private documents stored online without obtaining a warrant. In a letter dated April 24, 2013,[1] the SEC chair requested that the bill be amended to create new authority for administrative and regulatory agencies. CDT has separately explained why the approach sought by the SEC is unnecessary and would overturn decades of administrative practice that ensures smooth but fair compliance with regulatory subpoenas.[2]

The One Case Cited by the SEC Falls Apart upon Close Inspection

In this memo, we take a close look at the one case cited in the SEC letter, which says that the use of a subpoena served directly on an individual's ISP was the only way to obtain a critical email. Although the letter from the SEC chair does not identify the case, we believe it is *SEC v. Len A. Familant and Paul V. Greene.*[3] A look at the full record suggests that the piece of evidence cited may not have been critical. Moreover, the record in the case shows that a subpoena served on the individual's ISP was not the only way to obtain this one email.

The case involved InPhonic, a once high-flying online retailer of cell phones and wireless plans. The SEC probably first became concerned about InPhonic after the company itself, in April 2007, informed the SEC that it was restating its financial results for the second and third

---

[1] Mary Jo White, Chair, Securities and Exchange Commission, Letter to Senator Patrick Leahy (April 24, 2013), https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf, hereafter *SEC Letter*.

[2] Greg Nojeim, Center for Democracy & Technology, *S.607: Keeping Regulatory Agencies Armed, but Not Dangerous* (June 25, 2013), https://www.cdt.org/blogs/greg-nojeim/2506s607-keeping-regulatory-agencies-armed-not-dangerous.

[3] Complaint, *Securities and Exchange Commission, Plaintiff, V. Len A. Familant and Paul V. Greene, Defendants,* 2012 WL 256012 (D.D.C.). We believe this is the case because the letter from the SEC says that one of the individuals in the case sent himself an email stating that "the fake credits that were negotiated with" the company were being used "to hit certain quarterly numbers." That exactly quotes an email of defendant Greene as cited in the *SEC v. Familant and Greene* complaint. Complaint ¶ 47.

quarters of 2006, having incorrectly recorded revenue.[4] In May 2007, the company made a further filing with the SEC, warning that none of its financial results from 2006 should be relied on, for a variety of reasons, including "improperly recognized revenue."[5] In June 2007, the company made a third filing with the SEC indicating that its chief financial officer was resigning and that the company was restating its financials for all of 2006.[6] By November 2007, the company had filed for bankruptcy.[7] While the SEC states that the "defendants had carefully concealed their scheme," it seems clear that there was a huge blinking sign pointing directly at the company. The fraud at issue, so-called "round trip" transactions, is a common form of misconduct and one frequently the subject of SEC enforcement actions.

An Extensive Investigation and an Available Target Who Cooperated with Discovery

The SEC issued its Formal Order of Investigation on May 2, 2008 (probably after a period of informal investigation). It thereupon conducted an extensive inquiry over the course of three and a half years. That investigation included subpoenaing witnesses for sworn testimony. In particular, the SEC obtained two days of testimony from a Mr. Greene, who was president of APC, a company that sold telephones to InPhonic. The SEC subpoenaed and received detailed business and accounting records directly from InPhonic. Moreover, according to a court filing from Greene's attorneys, "The Commission also subpoenaed and received records from Mr. Greene."[8]

At some point, possibly as part of a broader subpoena to Mr. Greene, the SEC sought documents from Greene's personal email account. (Like many Americans, Greene used a popular, free online email service to create a personal email account separate from his business account.) After waiting a year, the SEC issued a subpoena directly to the Internet company where Greene had his personal email account, and that company complied without notifying Greene. (A practice that leading email service providers have since rejected, as discussed below.)

As we have explained elsewhere, the SEC had full authority, which S. 607 would not alter, to require the company providing Greene's personal email service to preserve all his email, to be

---

[4] http://www.washingtonpost.com/wp-dyn/content/article/2007/04/03/AR2007040301708.html. Such an admission invariably raises eyebrows, at the least. That very same day, a plaintiffs' law firm announced that, prompted by the company's SEC filing, it was considering filing a securities lawsuit on behalf of InPhonic's shareholders. http://globenewswire.com/news-release/2007/04/04/357636/116785/en/Investor-Notice-The-Rosen-Law-Firm-Announces-Investigation-of-Securities-Claims-Against-Inphonic-Inc.html.

[5] http://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_07-cv-00930/pdf/USCOURTS-dcd-1_07-cv-00930-0.pdf.

[6] http://www.cfo.com/article.cfm/9282110/c_9279593. The company admitted that it had failed to "maintain effective controls over the recordation, accuracy and completeness of activations and services revenue and related accounts receivable;" "maintain effective controls over the determination and accuracy of equipment revenue and related accounts receivable;" "maintain effective controls over the accuracy and completeness of consumer product rebate liabilities;" and "maintain effective controls over the accuracy and completeness of costs."

[7] http://www.washingtonpost.com/wp-dyn/content/article/2007/11/08/AR2007110802164.html.

[8] SEC v. Greene, Motion to Stay Discovery, 2012 WL 2282347 (June 5, 2012).

sure he didn't delete anything incriminating while the government sought to enforce the subpoena against Greene.[9] The SEC also had extensive powers, which S. 607 would not alter, to determine what private email accounts Greene had.[10] We have found nothing to indicate that the SEC used either of those existing authorities. Moreover, as we have also noted, SEC had very substantial powers to compel an individual to comply with its subpoena. We have found no indication that the SEC sought to enforce against Greene its subpoena demanding that he disclose email in his personal email account. There is no indication whether Greene raised any constitutional or statutory privileges or would have if the SEC had sought to enforce its subpoena. Instead, according to the SEC, after a year went by, the SEC issued a new subpoena directly to Greene's personal ISP and obtained an unstated quantity of email, one of which it cited in its complaint and press release and in the April 2013 letter from the SEC.

Not the "Critical" Piece of Evidence

However, an analysis of *SEC v. Greene* reveals that the one email cited by the SEC may not have been as critical to the investigation as the SEC claims. If anything, what was critical was the testimony of an APC employee who apparently cooperated with the SEC. This individual was identified in the complaint as "the APC Employee," but it is clear from subsequent filings that he was critical the SEC's case. This same APC Employee is cited 9 times in the SEC compliant, and emails to or from the APC Employee at his corporate address constitute 12 of the 42 exhibits relied on by the government in its opposition to Greene's motion for summary judgment. (Two of the other exhibits are the transcripts of the APC Employee's two days of testimony.)

Apparently, it was the APC Employee who said that that an APC accountant told him "That is fraud," and the APC Employee who said that, when he told that to Familant, Familant responded by supporting the illicit activity.[11] It was APC Employee who said that "Familant encouraged [him] to hide its billing for phony services."[12] And the APC Employee said that "Familant assured [him] that InPhonic would … pay APC's invoices for phony repair services,"[13] The APC Employee also seems to be the source for the allegation that "Greene directed him to create tracking sheets …. [that] showed the specific amounts by which APC was overbilling."[14] These and other conversations apparently recounted by the APC Emploee are among the numerous pieces of evidence of misconduct by both targets, regardless of the email obtained via subpoena for Greene's personal account.

---

[9] 18 U.S.C. § 2703(f). See CDT, Regulatory Agencies Do Not Need Additional Authority to Access Stored Communications (May 30, 2013), hereafter CDT Report, at p. 4 https://www.cdt.org/files/pdfs/Regulatory-Agencies-Access-Stored-Communications.pdf.

[10] 18 U.S.C. § 2703 (c). CDT Report, note 9 above, at p. 4.

[11] Complaint, ¶ 24.

[12] Complaint, ¶ 24.

[13] Complaint, ¶ 24.

[14] Complaint, ¶ 31.

Further evidence that Greene's personal email account was not critical is found in the government's list of exhibits offered in response to Greene's motion for summary judgment. [15] Of 42 exhibits offered by the government, only four are to or from Greene's personal account. Of those, two are to or from InPhonic accounts, so they were not under the sole control of Greene and were available to the SEC from InPhonic (or its bankruptcy trustee). A third was an email to the APC Employee, who appears to have cooperated with the government.

That leaves the one email, sent by Greene from his APC account to himself at his personal account in which he outlined plans to bring a lawsuit against InPhonic in connection with the fraudulent transactions. Greene may have withheld that email because he considered it privileged. Indeed, less than 2 weeks after Greene sent the email to himself, his attorney sent InPhonic a draft complaint along the lines in Greene's note to himself, suggesting that Greene did in fact take the matter up with his attorney in what were likely privileged communications. If indeed Greene thought that his personal email was privileged or otherwise protected, it is very troublesome that the SEC, rather than litigate the issue, took an end run around the judicial process and went to the third party ISP, which was going to be totally unaware of, and unable to assert, any claims of privilege.

The Case Illustrates Precisely the Kind of Indiscriminate Access to Personal Email That We Fear

It is particularly troubling that the kind of email account that the SEC wants to force intermediaries to disclose is a personal account. Like many Americans, Greene had a corporate email address under his company's domain name and a personal email address with a popular free email service. Greene apparently cooperated with the SEC's subpoena for his corporate email. However, we have found no indication that the SEC tried to compel Greene to turn over relevant communications in his personal account. Greene was legally available. He responded to the SEC subpoena for testimony, showing up and giving testimony over the course of 2 days. He also cooperated with the government request for his corporate email account, apparently turning over responsive corporate email, both email that he wrote and received and email to and from other of his employees - email that was extensively cited by the government.

Understandably, perhaps, Greene was reluctant to turn over his private account. But this was not an investigation where time was of the essence. The formal SEC investigation lasted at least three and a half years (from May 2008 until January 2012). Rather than invoking its substantial powers to have Greene held in contempt, the SEC went directly to Greene's personal ISP, placing that company in an impossible position.

As we have warned, Greene's personal email provider had no ability to decide what was relevant and what was not. We do not know how much personal email was turned over to the SEC, but it could have been voluminous, covering many years of Greene's life. To find the one email cited by the SEC, investigators may have received and reviewed thousands and thousands of personal emails completely unrelated to the investigation. The email service provider had no ability to sort through those emails; it was basically required to turn over everything it had within the requested time range. This is precisely what we fear from a regulatory agency carve-out to S. 607: indiscriminate access to personal emails without an opportunity to assert relevance, privilege or other protections.

[15] See Index of Exhibits to SEC's Statement of Material Facts Subject to Genuine Dispute, filed in Support of the SEC's Opposition to Motion for Summary Judgment.

The SEC's Problem Isn't With S. 607 – It's With the Constitution

There is another telling detail in the SEC's letter. The letter states that the subpoena for Greene's personal email account was issued "pre-*Warshak*." *Warshak* is the December 2010 decision of the Sixth Circuit Court of Appeals holding, in the SEC's own words, "that use of a subpoena or court order [other than a warrant] to obtain the contents of email stored with an ISP violates the Fourth Amendment's prohibition against warrantless searches." S. 607 would codify the Warshak rule and remove any uncertainty about its national application.

However, the critical point is this: After *Warshak* was decided on Constitutional grounds, the major email service providers (including the one used by Greene) decided that they could no longer comply with subpoenas for the content of communications stored on behalf of their customers. That is, even before S. 607 was introduced, it was clear to the SEC and other regulatory agencies that they would no longer be able to obtain email from third party service providers. In essence, the SEC is asking Congress to overturn *Warshak*. However, since *Warhak* is constitutionally based, that is not something Congress can do.

Conclusion

In the one case cited by the SEC for the proposition that regulatory agencies should have the power to compel email service providers to turn over communications stored on behalf of their customers, the SEC already had the authority to compel the target of its investigation to turn over his email. Instead, the SEC went directly to an Internet company and forced it to disclose what may have been voluminous private correspondence unrelated to the investigation. This is not the kind of practice that Congress should endorse.

For further information, contact Greg Nojeim, Center for Democracy & Technology, gnojeim@cdt.org.