Nothing to See in This Story about the Electronic Communications Privacy Act

posted on: Monday, September 21, 2015

Check out [this story](#). In it, we learn this:

Andrew Ceresney, director of the Division of Enforcement at the [Securities and Exchange Commission](#), [told](#) the Senate’s Committee on the Judiciary at a hearing on Wednesday morning that the pending [Electronic Communications Privacy Act Amendments Act](#) would impede the ability of the SEC and other civil law enforcement agencies to investigate and uncover financial fraud and other unlawful conduct. Ceresney testified that the bill, intended to modernize portions of the Electronic Communications Privacy Act which became law in 1986, would frustrate the SEC’s efforts to gather evidence, including communications such as emails, directly from an Internet services provider.

So. Let’s talk about what’s really at issue here. We’re not talking about emails collected from companies with their own domain names and servers. If a company maintains its own emails for its own purposes, the company is not a “provider of electronic communication service” under the ECPA and those emails are subject to SEC subpoenas just like its other documents.

But take, say, Google and Yahoo, among many others. They are providers of electronic communication services. Here’s what 18 U.S.C. § 2703(a) says about them:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

In plainer English, the SEC may require Google to disclose the contents of its customer’s emails if the emails have been in storage for 181 days. For newer emails, the government must have a search warrant, which the SEC can’t get as a civil enforcement authority.

For the SEC, the ECPA typically comes up when it is investigating people who are not using corporate email addresses. For example, Ponzi schemes and prime bank frauds are often going to be run on hotmail.com, not citigroup.com. The problem for the SEC is, people running Ponzi schemes tend to have few issues with deleting incriminating emails. And Google isn’t obligated to keep those deleted emails for any particular time period. So if some guy defrauds a bunch of people and then...
quickly deletes the emails explaining how the fraud happened, there’s not a lot the SEC can do about it. So it is very, very rare when the SEC is successful in using the ECPA to get emails from “providers of electronic communication service.” And so . . . when Andrew Ceresney tells the Senate Judiciary Committee that amendments to the ECPA could impede civil law enforcement’s ability to uncover financial fraud and other unlawful conduct, he’s sort of right. I might make the same argument if I were in his shoes. But he’s also saying something that is almost inconsequential. If the ECPA is not amended, the SEC will have a very hard time getting a hold of useful g-mails. If the ECPA is amended, it will have a very hard time getting a hold of useful g-mails. Just about every other issue in data privacy and securities enforcement is more significant than this one.