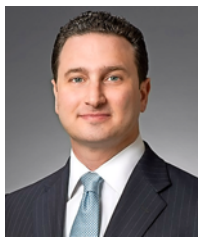
Bloomberg Law

Securities Regulation & Law Report™

PRIVACY

An Uneasy Relationship: The SEC and the Electronic Communications Privacy Act

BY SUSAN KAY LEADER, PETER I. ALTMAN, ERICA ELIZABETH ABSHEZ AND KELLY ANN HANDSCHUMACHER

Imagine this hypothetical scenario. You're an analyst at a hedge fund. You cover the technology sector and recommend investments to a portfolio manager. Last month, you received an email from your firm's general counsel informing you that the SEC had sent the firm a document request regarding trading activity in a publicly traded technology company that you started covering last year. Your firm had since taken a large position in that company. The SEC has requested all emails and instant messages your firm has regarding that technology company. A representative from the firm's information technology company has extracted all Microsoft Outlook communications from your computer, which is company property. You've learned from your friend in the compliance department that the firm intends to conduct keyword searches on those communications and turn them over to the SEC in the next two weeks. Though you feel sure that all of the investments you recommended to your portfolio manager were based on public information—and not material non-public information—you've read stories about Wall Street analysts being hauled off to jail for participating in insider trading.

And then yesterday, you came home from work to find an express mail envelope with a subpoena demanding the production of *all* of the emails you sent or received during the last year through Google's Gmail service. You've contacted a lawyer to help you with this and are waiting to hear back. While contemplating what you're about to go through (or, you hope, perhaps this investigation won't be a priority for the new administration—you've heard government enforcement might slow down under the Trump Administration), you wonder if you have to comply. The SEC already has your communications from work and you don't think it is fair to have your communications with friends and family reviewed by the government. You are pretty sure you never discussed work matters over Gmail, but you think you might have spoken about technology sector trades you made in your personal brokerage account with your college buddy who works at a technology

Susan Kay Leader is a partner, Peter I. Altman is senior counsel, Erica Elizabeth Abshez is an associate and Kelly Ann Handschumacher is a law clerk at Akin Gump Strauss Hauer & Feld LLP. All are members of the firm's litigation practice in Los Angeles.

 ISSN 0037-0665

startup. You also wonder what the SEC can get its hands on if you refuse to turn over your emails—can it go to Google and ask for your Gmail communications?

The SEC's Right to Electronic Communications Under Current Laws

The answer to this question involves the evolving intersection between the Fourth Amendment and federal privacy statutes—namely, the Electronic Communications Privacy Act of 1986, known as ''the ECPA.'' The SEC has two choices for getting access to your personal email communications: (1) subpoenaing the communications from you directly; or (2) subpoenaing your internet service provider (''ISP,'' and in the above hypothetical, Google). If you don't turn them over, the Stored Communications Act (''SCA'') section of ECPA governs how the SEC can request Google—via administrative subpoena—to divulge an individual's emails that were sent through, or stored in, Gmail.

An administrative subpoena is easy for the SEC to issue. Once the Division of Enforcement obtains a formal order of investigation, which is granted after minimal internal review by senior officers in the agency's regional offices, it obtains nationwide subpoena power. Such subpoenas need not be based on probable cause or approved by an independent judge—the core protections afforded by the Fourth Amendment for searches and seizures by the criminal authorities—and are subject to largely deferential review by a federal judge if challenged by the subpoena's recipient. *See United States v. Powell*, 379 U.S. 48, 57-58 (1964) (judicial enforcement of administrative subpoena contingent on whether (1) the inquiry is being conducted for a proper purpose; (2) the subpoena was issued in accordance with the required administrative procedures; and (3) the information sought is relevant to that legitimate purpose).

On its face, the SCA permits the SEC to subpoena an ISP such as Google both for subscriber information and contents of certain emails. Subscriber information includes your name, address, records of session times and durations, length of service and types of services used, telephone or instrument number, IP address, other identity information, and means of payment for service, including credit card or bank account numbers. Your subscriber information may seem insignificant in the abstract—particularly when compared to the contents of your emails—but such information can provide the SEC with valuable leads to other investigative threads such as telephone and bank records that it might not have otherwise known to access.

The SCA allows the SEC to subpoena the following categories of documents from ISPs:

- emails that are older than 180 days;
- emails that are considered to be in remote computing storage, regardless of whether they are older than 180 days, provided the SEC sends you notice of the subpoena; and
- basic subscriber information, which the SEC can access without giving you notice.

Hold on, you're thinking. You just skimmed Google's webpage describing how it handles government subpoenas, which states: ''Google requires an ECPA search warrant for contents of Gmail and other services based on the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure.'' How can Google refuse to comply with what seems to be a statutory mandate to provide contents of emails that are more than six months old?

The answer to that question lies at the next proverbial intersection—this time, between the Fourth Amendment and recent attempts by federal courts to apply ECPA to modern technology. ECPA (including the SCA), which was passed in 1986, bolstered individual privacy protection in the face of then evolving technology. Stop and consider that for a moment: federal courts today are charged with making decisions regarding data privacy through the framework of a federal statute drafted more than 30 years ago. Needless to say, technology has evolved since 1986—the year IBM announced its first laptop computer, which weighed 12 pounds and had a fraction of the computer power contained in the smartphones used by billions of people today.

It should come as no surprise, then, that the terms of the SCA rely on distinctions that no longer fit with modern use of technology and associated expectations of privacy, including the aforementioned 180-day line drawn with respect to the age of electronic communications. For example, the proliferation of cloud storage is particularly troubling for digital privacy rights under the current iteration of ECPA, given that many companies, including Google, offer cloud storage for emails and other electronic communications and that cloud storage holds such communications indefinitely.

These issues came to a head in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). There, the Sixth Circuit Court of Appeals held that government agents violated a defendant's Fourth Amendment rights when they compelled his ISP to produce the content of his emails without first obtaining a warrant based on probable cause. Though the decision was made in the criminal context—and not the civil regulatory context—it influenced legislation to reform ECPA and gave ISPs at least some ground to refuse to turn over content to regulators without a warrant.

In the words of outgoing SEC Chair Mary Jo White, *Warshak* ''greatly impeded the SEC's ability to serve administrative subpoenas on ISPs absent the consent of the subscriber.'' Concern over *Warshak* led the SEC, as a matter of practice, to no longer seek to compel production of the contents of emails from ISPs. Indeed, since *Warshak*, the SEC has not subpoenaed the contents of emails from ISPs, regardless of whether the emails were older than 180 days. *Warshak* has also allowed Google and other ISPs to take the position that they will not share the contents of communications without a warrant based on probable cause.

Proposed Reform of ECPA

In the wake of *Warshak*, further technological changes to the way electronic communications are transmitted, processed and stored (including through cloud-based storage), as well as ever-changing public expectations of privacy in electronic communications, have led to a reform movement focused on strengthening and clarifying privacy rights in ECPA. This reform movement had bipartisan support in the last Congress, and from technology companies such as Google, Apple, and Amazon, and legal interest groups like the American Civil Liberties Union (''ACLU'').

  SRLR ISSN 0037-0665

Prior to the election last November, bills in both the House and the Senate proposed a major change to how the government may require an ISP to disclose the contents of electronic communications. Specifically, the Electronic Communications Privacy Act Amendments Act of 2015 (the ''ECPA Amendments Act,'' S. 356, and identical H.R. 283) and the Email Privacy Act (a related bill in the House, H.R. 699), both would have required, in relevant part, a court-approved search warrant for access to the content of any electronic communications and records (eliminating any time-based distinction). This proposed warrant requirement to access content would, in effect, codify *Warshak*, a result that would leave the SEC and other civil regulators out in the cold with respect to accessing contents of electronic communications without the consent of the subscriber. Both proposed bills still would have allowed the SEC to access subscriber information pursuant to a subpoena.

Though the House passed the Email Privacy Act *unanimously* with 419 yea votes on April 27, 2016, neither its bill nor the version considered by the Senate were enacted into law. But the push for ECPA reform in Congress continues. In January 2017, Congressmen Yoder (R-KS) and Polis (D-CO) reintroduced the Email Privacy Act (H.R. 387) for the 115th Congress. While this reintroduction shows continued bipartisan support of ECPA reform, it remains to be seen whether the Trump Administration will push this as a high priority agenda item for the new Congress.

The SEC's Opposition to Proposed Reforms

It is likely that at least one contributing factor in Congress's failure to pass a version of these popular bills was the SEC's repeated opposition to any addition of a warrant requirement to ECPA. The outgoing SEC leadership—most notably Chair White and former Director of the Division of the Enforcement Andrew Ceresney—championed the agency's interest in not wanting the holding of *Warshak* codified by statute. And even as a new set of leaders takes control at the SEC, including nominated Chairman Jay Clayton, it is likely that the agency will continue to resist the codification of a warrant requirement for ISP subpoenas.

In April 2013, Chair White wrote to Senator Patrick Leahy, then Chairman of the Senate Judiciary Committee, describing the SEC's concerns regarding Senate Bill 607 (the ECPA Amendments Act's predecessor bill in 2013). She wrote of the SEC's reliance on ''the contents of e-mail and other electronic communications'' where ''defendants had carefully concealed their scheme.'' Similarly, when testifying before the Committee on the Judiciary in September 2015, former Director Ceresney stated that ''[e]lectronic communications often provide critical evidence in [SEC] investigations, as email and other message content (e.g., text and chat room messages) can establish timing, knowledge, or relationships in certain cases, or awareness that certain statements to investors were false or misleading.''

Ceresney testified that a warrant requirement (as suggested by *Warshak* and subsequent proposed legislation) would ''frustrate the legitimate ends of civil law enforcement.'' *Id.* ''Because the SEC and other civil law enforcement agencies cannot obtain criminal warrants, [the SEC] would effectively not be able to gather evidence, including communications such as emails, directly from an ISP, regardless of the circumstances.'' Chair White similarly stated that the warrant requirement in the ECPA Amendments Act's predecessor bill would ''effectively foreclos[e] the Commission from obtaining these electronic communications from the ISP[.]'' And in May 2016, Rick Fleming, the SEC's Investor Advocate, wrote to Senators Charles Grassley and Patrick Leahy, stating that ''[i]n its current form, the [ECPA] Amendments Act of 2015 (S. 356) would . . . inhibit the SEC in its mission of protecting investors and promoting confidence in the U.S. capital markets.''

The SEC's stated view of the proposed ECPA reforms has surely influenced lawmakers' view of these reforms. Indeed, Senator Dianne Feinstein explicitly stated that if there were to be a vote on the ECPA Amendments Act, ''my vote would be 'no.' To pass a bill that the SEC is not going to support and believes hamstring their actions, is not something I'm willing to do.''

The SEC's Proposed Modifications to Legislation and an Evaluation of the SEC's Position

ECPA's reform pits the SEC's drive for efficiently and effectively gathering information in its investigations against data privacy rights. While, without reform, ECPA ostensibly permits the SEC to exercise broad subpoena powers, the fact is that given *Warshak*, civil regulators are unable to subpoena a broad swathe of digital information without subscriber consent. In Ceresney's words, the proposed bills that codify *Warshak* ''would create an unprecedented digital shelter—unavailable for paper materials—that would enable wrongdoers to conceal an entire category of evidence from the SEC and civil law enforcement.'' Such an ''unprecedented shelter'' would be problematic given that the SEC's only recourse would be subpoenaing digital communications from potential wrongdoers—individuals who are more likely to erase emails, fail to tender important emails, assert damaged hardware, or refuse to respond to the subpoena at all. As Ceresney explained, ''unsurprisingly, individuals who violate the law are often reluctant to produce to the government evidence of their own misconduct.'' This would undercut the SEC's ability to compel online communications efficiently and effectively, potentially risking entire investigations. Thus, it is understandable that the SEC is against a reform that would remove its ability to go directly to ISPs for the contents of a subscriber's communications.

At the same time SEC officials criticized efforts to reform ECPA, they have also suggested modifications to bills moving through Congress. These modifications attempt to place the SEC in a position better than it is in under the current *Warshak* landscape. In his testimony before the Senate, Ceresney suggested the possibility of allowing the SEC to obtain contents of communications, while ''afford[ing] a party whose information is sought from an ISP in a civil investigation an opportunity to participate in judicial proceedings before the ISP is compelled to produce the information[.]'' Alternately, the SEC has suggested ''requiring civil law enforcement agencies to obtain a court order and satisfy a judicial standard comparable to the one that governs criminal warrants.''

Yet the SEC's proposed modifications are inherently problematic. Given that the SEC routinely shares infor-

mation it receives via subpoena with criminal law enforcement authorities, a broad subpoena power might overwrite any warrant requirement in ECPA. Moreover, a notice requirement on such a subpoena supposedly affording a party an opportunity to participate or object may not result in much actual privacy protection in practice. For example, under the Right to Financial Privacy Act of 1978 (the ''RFPA''), federal government agencies must provide individuals with notice and an opportunity to object before a bank can disclose personal financial information to that agency. Yet subpoenas under the RFPA are rarely contested. It is possible and/or likely that such a provision in an amended ECPA would also be rarely used and thus of little protection to individual privacy.

Does SEC enforcement data offer any help in determining how to balance these conflicting interests, perhaps by showing how important the SCA actually is to the SEC? In short, not really. Despite the SEC's stated warning of being forever relegated to relying only on subpoenas to individuals to produce relevant information, the SEC has lived in this landscape since the 2010 *Warshak* decision. Yet despite not having issued subpoenas for subscribers' emails directly to ISPs, the SEC has managed to bring more enforceable actions in the years after 2010 than before 2010. From 2011 to 2014, the SEC brought each year a total of 735, 734, 676 and 755 enforcement actions respectively, while from 2005 to 2009, the SEC brought 630, 574, 655, 671, and 664 enforcement actions respectively. Still, while this impressive rate of enforcement militates against the SEC needing to subpoena emails from ISPs, it is not conclusive. It is of course possible that the SEC was unable to bring actions against perpetrators it otherwise could have brought had it obtained access to personal emails.

Conclusion

So where does all of this leave you in your hypothetical role as a hedge fund analyst under subpoena? Caught between a rock and a hard place. You know the SEC—a powerful administrative agency that has the power to refer cases to criminal authorities—knows about your Gmail address. Do you produce your personal emails, or do you take the time and endure the expense of fighting the subpoena, greatly increasing the likelihood of suspicion by the SEC staff that you have something to hide. Either decision carries pros and cons, and until Congress updates ECPA, the legal landscape will not provide clarity as to whether one decision is better than the other.

  SRLR ISSN 0037-0665