New York Law Journal
White-Collar Crime
WWW.NYLJ.COM
An ALM Publication
VOLUME 256—NO. 60
MONDAY, SEPTEMBER 26, 2016

How Proposed **Changes to the ECPA** Affect **Privacy Interests** in Investigations

BY JOSHUA NEWVILLE AND LINDSEY A. OLSON


ISTOCK

Privacy advocates cheered the Second Circuit's July 2016 *Microsoft v. United States* decision holding that electronic communications stored abroad cannot be seized from an Internet service provider (ISP) with a search warrant under the Stored Communications Act (SCA). Coupled with recent efforts to amend the Electronic Communications Privacy Act of 1986 (the ECPA), the pendulum has swung in favor of privacy protection from government access for remotely-stored electronic data. Today it is growing harder for the government to obtain personal email content.

For financial fraud investigations, the proposed amendments to the ECPA could have significant consequences. The amendments may lead to earlier and greater cooperation between civil agencies like the SEC and the Department of Justice. It may become more difficult for the SEC to meet the standard for scienter in cases where individuals used personal email accounts as part of the alleged misconduct. Finally, in light of the Second Circuit's recent decision in *Microsoft*, an ISP's decision to maintain its customers' cloud storage data in a foreign location could be a key factor in the privacy analysis.

JOSHUA M. NEWVILLE *is a partner and* LINDSEY A. OLSON *is an associate in the litigation department at Proskauer Rose in New York.*

Current Status of the SCA

The SCA allows the government to compel ISPs to disclose an individual's electronic communications under certain circumstances. The SCA, Title II of the ECPA, generally addresses electronic communications once they are received and held in storage. ECPA Title I, the Wiretap Act, covers interception of communications in transit, while ECPA Title III addresses pen registers and trap and trace devices. Under the SCA, there are three general categories at issue, each with different levels of protection, listed from highest to lowest:

- Email content held in storage for 180 days or *less* can be obtained only with a search warrant under §2703(a), which does not require notice to the subscriber (18 U.S.C. §2703(b)(1)(A)).
- Under the SCA, email content held for *more* than 180 days is obtainable by warrant *or* administrative subpoena with notice to the subscriber (or delayed notice under certain circumstances) under §2703(b) – at least prior to the *Warshak* decision (see below).
- Basic subscriber and session information listed in 18 U.S.C. §2703(c)(2), including IP addresses, can be compelled

using an administrative subpoena without notice to the subscriber.

However, in 2010, the U.S. Court of Appeals for the Sixth Circuit held in *United States v. Warshak*, 632 F.3d 266 (6th Cir. 2010) that SCA §2703(b) was unconstitutional to the extent it allowed the government to compel email content using an administrative subpoena. *Warshak* found that, under the Fourth Amendment, users have a reasonable expectation of privacy in emails stored by their ISP, and as such, seizure of those emails would require a warrant based on probable cause. As the concurrence in *Microsoft* noted, the DOJ has incorporated the *Warshak* decision into its official policy and, as a matter of course, seeks warrants to obtain the contents of emails even where the SCA allows for a less-protective standard. We understand that the SEC has also generally refrained from using §2703(b) administrative subpoenas since *Warshak*.

Technical Limitations of the SCA/ECPA

The SCA was written in the 1980s, when the Internet was in its infancy and when electronic storage was expensive and rarely used. As a result, certain of its provisions draw distinctions that modern technology has rendered arbitrary, including the following examples:

- The SCA provides emails older than 180 days less protection, on the theory that most systems in 1986 only kept copies of messages for a few months, and older data was akin to a "business record maintained by a third party."
- The SCA distinguishes emails held in "electronic storage" under §2703(a) from those held by a "remote computing service," under §2703(b). As a result, many courts have interpreted this to mean that opened emails are no longer in "electronic storage" and thus receive less protection under §2703(b) of the SCA (but see *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), holding that emails were in "electronic storage" regardless of whether they had been accessed).
- Because §2703(b) of the SCA only refers to "contents" of an electronic communication, for an email older than 180 days, there is less protection for its content than for its transaction or "header" information (i.e., To, From, Date), which requires a 2703(d) court order (or warrant) for production.

Many people expect that the vast amounts of personal and financial data they maintain in cloud-based storage will be kept private. **Most do not draw distinctions** based on where "the cloud" happens to reside, how old their email messages are, or whether an email has been opened.

These distinctions make little sense in today's world of remote email services, cloud-based storage and widespread mobile technology. Many people expect that the vast amounts of personal and financial data they maintain in cloud-based storage will be kept private. Most do not draw distinctions based on where "the cloud" happens to reside, how old their email messages are, or whether an email has been opened.

Indeed, the Justice Department has agreed that "there is no principled basis" to treat email differently based on whether it is 180 days old. And in a concurring opinion in the *Microsoft* case, Judge Gerard E. Lynch of the Second Circuit implored Congress to revisit the statute in order to better balance privacy interests with law enforcement needs in the age of "the cloud," when remote service providers can move data in and out of the United States at "lightning speed" to serve their business needs, providing much greater privacy to those customers whose data happens to get stored on servers located abroad.

The Congressional Response

In early May 2016, the Email Privacy Act (H.R. 699) was unanimously passed by the House of Representatives with overwhelming bi-partisan support. A version of H.R. 699, the Electronic Communications Privacy Act Amendments Act of 2015 (S. 356), is currently before the Senate and also expected to pass. Both bills strive to bring the ECPA up to date with the digital age and to create more robust privacy protections for digital information. For example, the proposals would:

- remove the 180-day and "electronic storage" versus "remote computing service" distinctions;
- require the government to obtain a warrant to acquire the contents of stored communications from an ISP, essentially codifying the Sixth Circuit's decision in *Warshak*; and
- require that the government notify the individual, albeit post-disclosure, that his or her information was requested and received by the government (allowing the government to request delayed notification).

SEC's Objections to ECPA Amendments

The SEC, as a civil enforcement agency, does not have the power to obtain

search warrants. As such, the SEC and other civil law enforcement agencies have taken issue with the proposed warrant requirement. Here are some of the reasons:

- According to SEC Enforcement Director Andrew Ceresney, who was writing before H.R. 699 passed, "if [H.R. 699] becomes law without modifications, the SEC and other civil law enforcement agencies would be denied the ability to obtain critical evidence, including potentially inculpatory electronic communications from ISPs, even in instances where a subscriber deleted his emails, related hardware was lost or damaged, or the subscriber fled to another jurisdiction." He also noted that personal emails tend to show evidence of intent, a factor difficult to prove otherwise.
- In a letter to the Senate Judiciary Committee and in an Op-Ed piece in the New York Times, the SEC advocated for changes, pointing out that civil law enforcement agencies would not be able to meet the warrant requirement of the new bill because they do not have criminal law enforcement powers. As a consequence, the Commission would be unable to obtain evidence in cases like insider trading and Ponzi schemes, for example, if the individual being investigated either deletes or otherwise fails to turn over electronic records.
- The SEC has appealed to the legislature to consider alternatives (appeals that did not appear to move the House). Those alternatives include a provision that would allow the SEC to seek authority from a court to obtain emails under a standard akin to probable cause. It also expressed willingness to provide individual subscribers with notice and an opportunity to object *before* the ISP produces the data.

Second Circuit Holds That SCA Does Not Apply Extraterritorially

This summer, the U.S. Court of Appeals for the Second Circuit, in *Microsoft Corp. v. United States*, held that the SCA does not apply extraterritorially and that allowing the government to execute a warrant for data stored by a U.S. ISP on a server located in a foreign country would be an impermissible extraterritorial application of the statute. As a result of the *Microsoft* decision, an additional distinction has arisen—the physical location of the server used to store the data.

Takeaways

- The ECPA amendments will eliminate the SEC's ability to subpoena personal email communications from ISPs without the consent of the subscriber. This may not affect a typical investigation where the SEC subpoenas a company for messages involving employees using business email accounts. The SEC will likely have access to the same relevant communications (assuming the employee does not use personal email accounts for electronic communications, possibly in violation of company email policies).
- Where an investigation does involve personal email, the SEC likely will have to seek electronic data directly from the individual or with the individual's consent. In civil investigations, individuals may find it easier to shield personal emails by asserting the Fifth Amendment "act of production" doctrine, or simply by refusing to comply with a request.
- Civil and criminal law enforcement may cooperate earlier in investigations. In investigations where personal communications may be particularly relevant, like insider trading, microcap fraud, or offering frauds, SEC staff may refer matters to the Justice Department.
- The *Microsoft* decision may incentivize individuals and companies to store data abroad. Because offshore content is outside the reach of a warrant under *Microsoft*, and cannot be subpoenaed under *Warshak*, the government would be forced to seek foreign cooperation to obtain data offshore, using the slower MLAT process.
- Emails maintained in a non-U.S. cloud location (even a location unknown to the subscriber) that has strong data protection laws may be subject to greater privacy protections than emails kept in a secure, domestic location.
- In light of the *Microsoft* decision, the Senate could take the opportunity to debate the implications of the proposed ECPA amendments and consider whether extraterritorial reach of the government's power to obtain digital information stored abroad is appropriate in the age of cloud storage. The SEC may make further efforts to advocate revisions, especially in the wake of *Microsoft*.