New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 249—NO. 88
WEDNESDAY, MAY 8, 2013

TAX LITIGATION ISSUES

Expert Analysis

The IRS, Email Privacy And the Legislative Answer

By
Jeremy H. Temkin

Communication through email is a reality of the modern world. Another reality is that even the most careful among us have pangs of regret shortly after hitting the send button, realizing that an email did not accurately convey our intended thoughts. And every day, lawyers representing clients in criminal investigations blanch when they review their clients' emails: a client's pangs of regret become the lawyer's challenge to explain the client's intended meaning to a cynical prosecutor or, even worse, a lay jury.

While emails are often produced pursuant to subpoenas addressed to the sender or recipient (or the sender's or recipient's employer), the Stored Communications Act, part of the Electronic Communications Privacy Act of 1986, enables the government to obtain emails and electronic data stored by third parties like Google, Yahoo! and Facebook.[1] Of course, the world—and especially the way in which we communicate electronically—has changed dramatically over the past 27 years, and Congress is presently drafting legislation aimed at bringing the rules regulating the government's access to electronic communications into the 21st century.

This legislative effort is likely to get a boost from publicity surrounding the release last month of internal IRS documents describing the agency's policies regarding how it obtains emails, text messages and other private electronic communications.[2] While the IRS's historical practices appear to have been consistent with those applied by other law enforcement agencies, the public furor surrounding the documents and a growing consensus of federal courts holding that emails are entitled to Fourth Amendment protection demonstrate the need for reform.

Stored Communications Act

In *United States v. Miller*,[3] the U.S. Supreme Court held that an individual does not have a reasonable expectation of privacy in bank records because he voluntarily transmitted the underlying information to the banking institution. *Miller* was decided in 1976 over a vigorous dissent by Justice William Brennan who argued that because "it is impossible to participate in the economic life of contemporary society without maintaining a bank account," the disclosure cannot be "entirely volitional."[4] Nevertheless, the Supreme Court continued to develop the doctrine that the Fourth Amendment does not protect information given to third-party service providers. For example, in *Smith v. Maryland*, decided three years later, the court applied similar reasoning to find that phone records are not subject to Fourth Amendment protection.[5]

In light of this case law, Congress passed the act to expand the protection of electronic communications beyond what was available under the then-existing Fourth Amendment jurisprudence. In doing so, Congress hoped to shield electronic communications—which are revealed to a third party that hosts or stores them—by creating a statutory "zone of privacy." To obtain the contents of unopened communications that have been stored for less than 180 days from Internet Service Providers (ISPs), such as Yahoo!, the act requires the government to obtain a search warrant based on a showing of probable cause.

By contrast, the government does not need a warrant to get (a) emails that have been opened; (b) emails that are more than 180 days old; and (c) documents stored by a "remote computing service provider," such as Dropbox or other document hosting services. Rather, the government can obtain such information, including pictures stored on Facebook, files shared between coworkers using Google Documents or information from many of the other services millions of Americans use every day, through the relatively minimal step of issuing administrative summonses and grand jury or trial subpoenas.

While the act's provisions were intended to be expansive in 1986, given technological advances, they are now outdated and provide limited protection to Internet users. Indeed, the distinction between unopened emails that have been stored for less than 180 days and emails that either have been

JEREMY H. TEMKIN *is a principal in Morvillo Abramowitz Grand Iason & Anello.* ESTER MURDUKHAYEVA, *an associate of the firm, assisted in the preparation of this article.*

opened or are more than 180 days old is arbitrary and at odds with the modern use of technology.

'United States v. Warshak'

Over the past three years, several courts have found that emails and other forms of electronic communications are entitled to greater protections than provided by the act.[6] The leading case in this area is the decision of the U.S. Court of Appeals for the Sixth Circuit in *United States v. Warshak*.[7] The defendants in *Warshak* were charged with numerous counts of fraud, primarily relating to the sale of herbal supplements over the telephone and online. Following a six-week trial, the defendants were convicted of a majority of the charges and Warshak, the lead defendant, was sentenced to 25 years in prison.

During its investigation, the government asked NuVox, an email service provider, to "prospectively preserve the contents of any emails to or from Warshak's email account." NuVox agreed and "per the government's instructions, Warshak was not informed that his messages were being archived." The government then obtained a subpoena and an ex parte administrative order under the act, and NuVox produced over 27,000 responsive emails. The district court denied Warshak's motion to suppress the emails, finding that they were not protected under the Fourth Amendment.

On appeal, Warshak argued, among other things, that the government violated his Fourth Amendment rights by obtaining his emails without a search warrant. The Sixth Circuit agreed, finding that "the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[8] The court distinguished *Miller*, arguing that unlike a bank that uses its clients' financial transactional information "in the ordinary course of business," an ISP is an intermediary and not the "intended recipient of the emails."[9]

The court then compared emails to traditionally protected forms of private communication, such as letters: "People are now able to send sensitive and intimate information, instantaneously to friends, family and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email…. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities."[10]

The court concluded that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[11] Thus, the court held that email users have a "reasonable expectation of privacy in [their] emails" and that the government must obtain a warrant based on probable cause in order to require a service provider to turn over the electronic communications.[12]

Congress is presently drafting legislation aimed at bringing the rules regulating the government's access to electronic communications into the 21st century.

IRS's Approach

Recently, the American Civil Liberties Union disclosed documents received in response to a Freedom of Information Act request demonstrating that, consistent with the approach taken by the FBI agents and Postal Inspectors in *Warshak*, the IRS has long taken the position that the Fourth Amendment does not apply to certain electronic communications.[13] For example, a 2008 presentation by IRS Criminal Investigation division explained the provisions of the act, including the need for a warrant to obtain unopened emails stored for 180 days or less and the ability to obtain opened emails and emails that are more than 180 days old through administrative summonses or grand jury subpoenas.

Similarly, in a 2009 Search Warrant Handbook, the IRS's Office of Chief Counsel explained that "[l]ike files shared over a network, emails and other transmissions generally lose their reasonable expectation of privacy and thus their Fourth Amendment protection once they have been sent from an individual's computer." The Chief Counsel's Office further asserted that "the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications," but recognized that the act requires a search warrant "if the government seeks to compel disclosure of the contents of electronic communications and other information without prior notice" to the subscriber.

The 2009 version of the Internal Revenue Manual addresses the investigative techniques available to agents conducting criminal investigations. The manual provides a detailed discussion of the act, including the need for a warrant for communications that "have been in storage for 180 days or less" and the ability to get information more than 180 days old through a subpoena or summons. A March 2011 revision to the manual, published four months after the *Warshak* decision, did not alter this policy, stating that "[i]nvestigators can obtain everything in an account except for unopened email or voice mail stored with a provider for 180 days or less" without having to seek a search warrant.

Following *Warshak*, however, numerous ISPs, including Google, Microsoft, Yahoo! and Facebook, have taken the position that search warrants are required for all emails.[14] Yet the impact of *Warshak* on the IRS's internal policies was unclear. In a mid-January 2011 email exchange regarding *Warshak*, an IRS Special Counsel for Criminal Tax noted that the IRS has "always taken the position that a warrant is necessary when retrieving emails that are less than 180 days old." In an October 2011 memorandum, the IRS Chief Counsel advised that "as a practical matter it would not be sensible" to attempt to obtain emails older than 180 days without a warrant as it would be unlikely that, in light of the position taken by ISPs, the IRS could obtain the emails "without protracted litigation, if at all." Yet the memorandum focused on the practical policy considerations rather than the Sixth Circuit's legal analysis in *Warshak*.

A Stormy Reaction

While the IRS's view of electronic communications appears to be consistent with the approach taken by the agents in *Warshak*, given criticisms lodged against the agency in the not too distant past, the negative publicity generated by the ACLU's disclosure is especially problematic.[15] For decades leading up to the late 1990s, the IRS was challenged for being overly aggressive and unduly intrusive on taxpayers' rights. In response to these complaints and a review conducted by the Webster Commission, Congress passed the IRS Restructuring and Reform Act of 1998,[16] which sought to rein in perceived abuses. In the years following these reforms, the IRS has tried to soften its image and approach to the difficult job of collecting taxes.

Recently, the American Civil Liberties Union disclosed documents received in response to a Freedom of Information Act request demonstrating that the IRS has long taken the position that the Fourth Amendment does not apply to certain electronic communications.

Notwithstanding significant progress by the agency, following the ACLU's release of these documents, Congressman Charles Boustany Jr. wrote to Acting Commissioner Steve Miller, seeking more information about the IRS's searches of emails, text messages and social media. In a press release, Boustany stated: "It is concerning that the IRS may be gathering information through Americans' emails and social media and I demand to know what purpose it is serving."[17]

Several days later, Acting Commissioner Miller testified before the Senate Finance Committee on April 16, stating that the IRS would abandon its previous policy on emails. Miller did not, however, state whether the Service would continue to seek data from other electronic communication and remote computing service providers, such as Facebook, Twitter, Dropbox and Google Documents, without a search warrant. Following this testimony, a group of senators wrote a sternly worded letter to the acting commissioner, urging the "IRS to provide further details and a timetable for its plans to update policies to adhere to Americans' constitutional rights."[18]

Legislative Developments

On April 25, the Electronic Communications Privacy Act Amendments Act of 2013 passed the Senate Judiciary Committee.[19] The bill, introduced by Senators Patrick Leahy and Mike Lee, requires the government to obtain warrants based on probable cause before accessing electronic communications and files stored on "cloud-based" services like Dropbox and Google Documents. While there are exceptions for exigent circumstances and to protect national security, this legislation eliminates the distinction between opened and unopened emails as well as the distinction between emails based on whether they are more or less than 180 days old.

Importantly, the proposed amendments also discard the distinction between communications stored by electronic communication service providers (like Gmail or Yahoo!) and those stored by remote computing service providers (like Dropbox or Google Documents). The bill also requires the government to promptly notify individuals whose electronic communications were obtained from a third-party service provider and include a copy of the search warrant.

Under the bill, however, the government will still be able to obtain emails and other electronic communications without a search warrant by serving subpoenas on individuals and their employers and can seek a court order temporarily delaying notification to individuals whose emails have been obtained.

Conclusion

As the Sixth Circuit recognized in *Warshak*, "email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication."[20] The documents released by the ACLU highlight the limited protections accorded emails and other electronic data under the act, as well as the difficulty in keeping up with changing technology and the need for further legislation. Moreover, while lawyers representing taxpayers in criminal cases are already painfully aware that emails, text messages and other forms of electronic communication can be damning evidence, the documents released by the ACLU suggest that defense counsel need to understand how the IRS and other law enforcement agencies obtain that evidence and be mindful of possible challenges to the government's ability to present it at trial.

1. Pub.L. 99-508, 100 Stat. 1848 (1986), codified at 18 U.S.C. §§2701 et. seq.
2. Nathan Freed Wessler, ACLU Staff Attorney, New Documents Suggest IRS Reads Emails Without a Warrant (April 10, 2013).
3. *United States v. Miller*, 425 U.S. 435 (1976).
4. *Miller*, 425 U.S. at 451 (1976) (Brennan, J., dissenting).
5. 442 U.S. 735 (1979).
6. *United States v. Ali*, 870 F.Supp.2d 10, 39, n. 39 (D.D.C. 2012); *In re Application of United States for Order Authorizing Release of Historical Cell-Site Info.*, 809 F.Supp.2d 113, 124-25 (E.D.N.Y. 2011); cf. *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
7. 631 F.3d 266 (6th Cir. 2010).
8. Id. at 286.
9. Id at 288.
10. Id. at 284.
11. Id. at 285-86.
12. Id. at 288. The court, however, declined to reverse the convictions on this ground, holding that the emails were not subject to the exclusionary remedy since the government had relied in good faith on the act. Id. at 288-89.
13. The documents are available at the ACLU's website: http://www.aclu.org/national-security/irs-response-warrantless-electronic-communications-foia-request.
14. Brendan Sasso, Facebook, email providers say they require warrants for private data seizures, The Hill (Jan. 25, 2013), http://thehill.com/blogs/hillicon-valley/technology/279441-facebook-email-providers-require-warrant-for-private-data.
15. The ACLU also submitted FOIA requests to the FBI, the Department of Justice and a number of U.S. Attorney's Offices regarding their policies on collecting email, text messages and other electronic communications post-*Warshak*. As of May 2013, the ACLU has not received a response from these offices.
16. Pub.L. 105–206, 112 Stat. 685 (1998).
17. Press Release, Boustany Demands IRS Explanation for Reading Taxpayer Emails (April 11, 2013), http://waysandmeans.house.gov/news/documentsingle.aspx?DocumentID=328598.
18. Senator Mark Udall et. al., Letter to Steven Miller, Acting Commissioner of Internal Revenue (April 16, 2013), available at http://www.lee.senate.gov/public/index.cfm/files/serve?File_id=681bf5a0-564a-418b-97d1-42a1816e1905.
19. S. 607, 113th Cong. (1st Sess. 2013). See also Bridget M. Rohde and Sara J. Cresson, "Government Access to Email and Data Stored Online," NYLJ (Jan. 29, 2013).
20. 631 F. 3d at 286.