Bloomberg Law Reports® Privacy & Information

Sixth Circuit Requires Warrants for Production of All Stored Electronic Communications

Contributed by Ronald D. Lee and Stephen Marsh, Arnold & Porter LLP

In *United States v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit recently issued a significant decision applying the Fourth Amendment of the U.S. Constitution to e-mails stored by an Internet Service Provider ("ISP"). Although the Stored Communications Act ("SCA") requires the issuance of a warrant for the government to obtain unopened e-mails stored for 180 days or less, the statute permits the government to obtain retrieved e-mails or e-mails older than 180 days by issuing a grand jury subpoena or a court order predicated on a standard lower than probable cause. The *Warshak* court concluded that such provisions permitting the government to examine an individual's stored, electronic communications without a warrant violate the Fourth Amendment.[1] While some commentators have hailed the decision as rationalizing the constitutional treatment of personal communications, the case leaves open a number of important questions about the scope of protections afforded to communications stored with third party providers, including ISPs. In light of this decision, companies that provide electronic communication services will need to carefully reconsider their current policies for responding to government requests for stored data.

Summary of the Investigation

Steven Warshak was convicted of a number of federal charges for his role in conducting a large fraudulent marketing and distribution scheme involving the sale and distribution of herbal supplements. As part of its investigation, the government contacted NuVox Communications, an ISP that provided service for one of Warshak's e-mail accounts. In October 2004, the government asked the ISP to prospectively preserve Warshak's e-mails pursuant to the SCA, specifically 18 U.S.C. § 2703(f). NuVox proceeded to preserve Warshak's incoming and outgoing e-mails without notifying Warshak that it was doing so. In January 2005, the government issued a subpoena, as permitted under Section 2703(b) of the SCA, and compelled the ISP to turn over the e-mails it had previously preserved. A few months later, in May 2005, the government obtained an *ex parte* court order pursuant to § 2703(d) requiring NuVox to turn over any additional e-mails in Warshak's account. Neither the government nor the ISP informed Warshak of the subpoena or court order for approximately a year.

Application of the Fourth Amendment to the SCA

On appeal, Warshak argued that the government's seizure of approximately 27,000 private e-mails without a warrant or prior notice to Warshak constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures.

In examining this claim, the Sixth Circuit's analysis hinged on whether a subscriber such as Warshak had a reasonable expectation of privacy with respect to the e-mails stored by his ISP. The Sixth Circuit concluded that Warshak had a reasonable expectation of privacy in his e-mail communications.[2]

The court's rationale was based in part on analogies between e-mail and other forms of communication, such as letters and telephone calls, in which the U.S. Supreme Court has already found an expectation of privacy to be reasonable. Because of the "fundamental similarities between [e-mail] and traditional forms of communication," the court concluded that e-mails are subject to the same Fourth Amendment protections as phone calls and letters.[3] The court also rejected the notion that an ISP's contractual right to access a subscriber's e-mail under the agreement between the subscriber and the ISP somehow nullified the otherwise reasonable expectation of privacy. The court again made analogies to letters and phone calls, in which a reasonable expectation of privacy exists even though such communications may be subject to inspection or monitoring by the delivery agent. "If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. . . ."[4] Thus, to the extent that the SCA permits the government to obtain retrieved e-mails without a warrant, the court concluded that the SCA is unconstitutional.[5]

Implications of Warshak for Companies Transmitting and Storing E-mail

1. *Geographic Reach of* Warshak

At present, the *Warshak* decision serves as binding precedent only in the four states that make up the Sixth Circuit: Tennessee, Kentucky, Ohio, and Michigan. But because the decision affects electronic communications, the reach of the decision likely will be felt beyond the Sixth Circuit.

For instance, what if the ISP is headquartered or has servers located in the Sixth Circuit, but the law enforcement agents and subscriber subject to the investigation reside in the Ninth Circuit?

Or conversely, what if the ISP maintains the servers where the communications are stored in the Ninth Circuit but all other interested parties reside in the Sixth Circuit? In some cases, law enforcement agents, the ISP, and the subscriber may reside in three different circuits. In any of these scenarios, the affected parties should give strong consideration as to whether they can rely on *Warshak* and the newly imposed warrant requirement where the government demands the production of electronic communications without a warrant.

2. *Does* Warshak *Apply to All Stored E-mails or Only Those E-mails Retained by an ISP Acting in the Capacity of a Delivery Agent?*

The extent to which *Warshak* applies to ISPs or other electronic communication providers where those providers act in the capacity of a remote electronic storage facility remains uncertain. Given the court's repeated analogies to other communication delivery agents such as the postal service and telephone companies, one could read the court's opinion as applying Fourth Amendment protections to all communications in transit, including those communications stored by ISPs as part of the delivery process. The court phrased its holding, however, in exceedingly broad terms, concluding that "a subscriber enjoys a reasonable expectation of privacy in the contents of e-mails 'that are stored with, or sent or received through, a commercial ISP.'"[6]

The opinion does not indicate that Warshak actually stored his e-mails with the ISP. In fact, according to the court, the defendant routinely downloaded his e-mails from the ISP and, but for the government's request, the ISP would not have retained copies of those communications.[7]

This issue could be important for ISPs and other providers of electronic communication services that function as digital storage facilities for users seeking remote access to their electronic communications. Many of these providers play dual roles as both delivery agents in transmitting e-mails to and from a subscriber, as well as storage providers for subscribers who leave their e-mails in remote storage. Consequently, such providers will need to carefully examine whether the standards that apply to them in their capacities as delivery agents also apply when they act as a storage provider.

3. *Application of* Warshak *to Employers or Any Other Parties That Transmit or Store Third Party E-mails*

Although *Warshak* addresses the application of the Fourth Amendment to e-mails transmitted by an ISP, the breadth of the court's ruling may result in efforts by litigants to extend that ruling to electronic communications transmitted and stored by private companies on behalf of their employees. Companies that provide users, including employees, with the ability to transmit and receive electronic communications may already come within the provisions of the SCA that govern "electronic communication services."[8] The SCA requires the government to obtain a warrant in order to compel a company that qualifies as an electronic communication service to disclose unopened e-mails 180 days old or less.

The rules that apply to opened or retrieved e-mails differ, however, depending on whether the company provides computer storage for the public at large. For public providers, the SCA requires that the government either obtain a warrant or issue "a subpoena with prior notice" to the subscriber.[9] Those requirements do not apply to private companies that store retrieved communications of their users, including companies that provide internal e-mail for employees. In the wake of *Warshak*, however, a genuine question exists as to whether the employees or other users of electronic communications provided by a private company have an expectation of privacy vis-à-vis third parties like the government with respect to the content of their retrieved communications. As with terms of use agreements involving ISPs, an employee could argue that the employer's right to inspect her e-mail does not abrogate the expectation of privacy in those e-mails unless her employer has manifested an intent to monitor those communications. If a court accepted that argument, the government would then be required to obtain a warrant prior to compelling the disclosure of those retrieved communications on private networks.[10]

4. *Reviewing ISP Subscriber Agreements*

The *Warshak* court rejected the notion that a subscriber agreement that permits the ISP to access a user's e-mail account eliminates an otherwise reasonable expectation of privacy. But the court left open the possibility that a more aggressive access policy might suffice in upsetting such an expectation of privacy. "[I]f the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's [e-mails], that might be enough to render an expression of privacy unreasonable."[11] Whether or not they engage in monitoring or inspection of subscriber e-mails, ISPs and other entities subject to the *Warshak* decision should carefully review their access agreements and practices to determine what level of process the government must provide in order to obtain subscribers' communications.

5. *Does* Warshak *Affect the Validity of Preservation Requests Issued by the Government?*

Warshak raises two important questions relating to preservation requests – the letters issued by the government pursuant to section 2703(f) of the SCA that command electronic communication providers to preserve evidence for a period of up to 90 days pending the issuance of compulsory process. The first issue concerns whether the government can issue a prospective request to preserve e-mails as they are created in the future rather than preserving those already in existence. The court never resolved that issue, but the concurring

opinion suggested that a prospective request for e-mails without the user's knowledge, when the ISP otherwise would have destroyed the old e-mails, amounts to "back-door wiretapping."[12] The Department of Justice already counsels against the use of prospective preservation requests.[13] In the wake of *Warshak*, such requests should be given even greater scrutiny.

Warshak's holding also raises constitutional questions as to whether the government has the authority to instruct an electronic communications provider to retain existing e-mails in the absence of a warrant. A leading commentator has expressed the view that any effort to freeze or divert data from its intended path or timing constitutes a "seizure" within the meaning of the Fourth Amendment.[14] If a subscriber maintains a reasonable expectation of privacy in his or her e-mail, and the government seizes the e-mail by requiring preservation without a warrant, what are the constitutional implications of that action?[15] Although that issue was not addressed in *Warshak*, it is one of a number of issues likely to surface in the wake of that decision.

Conclusion

The *Warshak* decision provides that the government may not obtain any individual's e-mails from an ISP without first obtaining a warrant, which represents a higher standard than the one that previously applied to certain stored communications under the SCA. The decision could represent a significant change in the legal obligations of ISPs and other companies that provide users with the ability to send, receive, and store electronic communications. Companies that provide these services should carefully consider their policies and procedures for responding to government requests for user information in light of this decision.

Ronald D. Lee is a partner of Arnold & Porter LLP in Washington, D.C., practicing in national security, cybersecurity, and technology law and policy. He was formerly General Counsel of the U.S. National Security Agency and Associate Deputy Attorney General with the U.S. Department of Justice, handling national security, cyber and counterterrorism matters. Mr. Lee can be reached at (202) 942-5380 or Ronald.Lee@aporter.com.

Stephen Marsh is an associate in the Washington office of Arnold & Porter LLP, practicing in white collar criminal defense, cybersecurity, and intellectual property litigation. He was formerly an Assistant U.S. Attorney. Mr. Marsh can be reached at (202) 942-5232 or Stephen.Marsh@aporter.com.

The authors express their gratitude to partner Marcus A. Asner and associate Bassel Korkor, in the New York and Washington offices respectively, for their assistance in the preparation of this article.

---

1 *United States v. Warshak*, __ F.3d __, Nos. 08-3997/4085/4087/4212/4429, 09-2176 2010 BL 295414 (6th Cir. Dec. 14, 2010).

2 The court, however, ultimately upheld the convictions of Warshak and the other defendants, finding the evidence admissible because officers reasonably relied on the SCA in good faith while seeking the e-mail data, and the SCA was not plainly or obviously unconstitutional. The court noted that this good-faith reliance defense would not be valid in future cases in light of the court's ruling in this case.

3 *Warshak* at 19. In support of its holding, the court relied on Supreme Court decisions recognizing a reasonable expectation of privacy with respect to phone calls and letters. *See Katz v. United States*, 389 U.S. 347 (1967) (reasonable expectation of privacy for phone communications); *United States v. Jacobsen*, 466 U.S. 109 (1984) (reasonable expectation of privacy for letters transmitted by postal service).

4 *Warshak* at 20.

5 The deadline to file a motion for reh'g in this case is currently January 27, 2011. *See Warshak v. United States*, Docket No. 09-3176 (6th Cir. 2011).

6 *Warshak* at 23 (quoting *Warshak v. United States*, 490 F.3d 455, 73 (6th Cir. 2007) ("*Warshak I*")).

7 *Warshak* at 16 n.14, 27.

8 *See* "Searching and Seizing Computers and Obtaining Electronic Evidence Manual," U.S. Department of Justice, Ch. 3 § B.1.,

http://www.justice.gov/criminal/cybercrime/ssmanual/03ssma.html ("Any company or government entity that provides others with the means to communicate electronically can be a 'provider of electronic communication service' relating to the communications it provides, regardless of the entity's primary business or function.").

[9] *See* 18 U.S.C. § 2703(b). Notice may be delayed if the government certifies in writing that there is reason to believe that the prior notice could adversely affect an ongoing investigation or prosecution (e.g., destruction of evidence or witness intimidation). *See* 18 U.S.C. § 2705(a).

[10] *Cf. United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007) (concluding that an employee had an objectively reasonable expectation of privacy with respect to his workplace computer and that any search of that device had to comply with the Fourth Amendment).

[11] *Warshak* at 22 (citing *Warshak I* at 472-73 and *United States v. Simmons*, 206 F.3d 392, 398 (4th Cir. 2000)).

[12] *Warshak* at 97.

[13] "Searching and Seizing Computers and Obtaining Electronic Evidence Manual," U.S. Department of Justice, Ch. 3 § G.1., http://www.justice.gov/criminal/cybercrime/ssmanual/03ssma.html (noting that preservation requests for future documents should comply with the requirements that apply to electronic surveillance in the federal wiretap statute).

[14] *See* Orin S. Kerr, "FOURTH AMENDMENT SEIZURES OF COMPUTER DATA," 119 Yale L.J. 700, 721-24 (Jan. 2010).

[15] Courts have permitted law enforcement agents to seize evidence pending the issuance of a warrant in order to prevent its disappearance or destruction, but in such cases, courts require the government to diligently obtain a warrant. Although no bright line rule exists, courts have typically demanded that agents obtain a warrant much sooner than the 90 days the SCA allows the government to have electronic records retained prior to issuing compulsory process. *Cf. United States v. Dass*, 849 F.2d 414 (9th Cir. 1988) (delay of between 7 and 23 days between seizure and warrant unreasonable); *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) (delay of 21 days between seizure of hard drive and warrant unreasonable under Fourth Amendment).