CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Warshak v. United States
Federal Appeals Court Holds Email Constitutionally Protected

July 24, 2007

In an important case, the federal appeals court for the Sixth Circuit ruled on June 18 that email users generally enjoy a constitutionally-protected right of privacy in their email as it sits in storage with a service provider. The court also declared unconstitutional a provision of the Electronic Communications Privacy Act that allows government investigators to use a subpoena or court order issued on less than probable cause to obtain older email without notice to the person whose email is being disclosed.

The rule established by the court is simple: in order to obtain email from a service provider, either (i) the government must obtain a search warrant issued under the relatively high standard of probable cause set forth in the Constitution's Fourth Amendment, or (ii) if the government wants to use a mere subpoena or a court order issued on less than probable cause, it must provide notice to the person whose communications are being sought, giving him an opportunity to object. Warshak v. United States, http://www.ca6.uscourts.gov/opinions.pdf/07a0225p-06.pdf.

For Internet users, the ruling is a small but significant victory for privacy. From a corporate perspective, the ruling brings some needed simplicity to the rules governing disclosure of stored email. The ruling should be welcome to email providers for another reason: as Internet users remain acutely sensitive to privacy, this case gives them some measure of confidence by specifying that online communications enjoy constitutional protection. While the Justice Department is likely to seek to overturn the decision, the case actually should not have a major impact on law enforcement practices, since under ECPA law enforcement agencies already have to obtain a warrant to get more current email.

The court decided a relatively narrow issue, filling just one gap in a remarkably uneven area of the law. The court accepted as a given some aspects of Fourth Amendment law that probably deserve to be re-examined in other cases, especially the business records doctrine that leaves transactional data about our daily activities unprotected by the Constitution. The premise of the court's constitutional ruling – that email users reasonably expect that an email is a private communication between sender and recipient

– is obviously true, as reflected in the widespread reliance on email for sensitive communications in commerce, government and personal relations. Perhaps the only thing remarkable about the case is that the constitutional issues it posed had never been addressed before by the regular federal courts. (Oddly enough, U.S. Court of Appeals for the Armed Forces had already declared email to be constitutionally protected.)

The case begins the process of addressing the impact on privacy of one of the major technology trends of our time: the movement of stored email and other sensitive personal information off the personal computer or laptop, out of the home or office, and onto the computers of Internet based web services. CDT outlined the implications of this "storage revolution" in our February 2006 report, "Digital Search and Seizure" http://www.cdt.org/publications/digital-search-and-seizure.pdf. At least with respect to the content of email communications, the court said, email is entitled to essentially the same constitutional protection whether it is downloaded onto one's personal computer or stored remotely on the servers of MSN, Yahoo or Google.

The Facts and Procedural Posture of the Warshak Case

In 2005, the government was investigating Mr. Warshak and the company he owned. The investigation pertained to allegations of mail and wire fraud, money laundering and related offenses. The government obtained an order from a magistrate directing an ISP, NuVox Communications, to turn over information pertaining to Warshak's email account. The information to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information pertaining to the customer, including set up, synchronization, etc."; (2) "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak; and (3) "[a]ll Log files and backup tapes."

The magistrate's disclosure order stated that it was issued under 18 U.S.C. § 2703, which is in a part of ECPA sometimes referred to as the Stored Communications Act ("SCA"). The order stated that it was based on "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation," the standard set forth in § 2703(d). The order was issued under seal and prohibited NuVox from disclosing the existence of the application or the order to Warshak. The magistrate further ordered that "the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days." Later, the government obtained a nearly identical order pertaining to Yahoo, another ISP.

When the government finally (over 9 months late) notified Warshak of both orders, he filed suit, alleging that the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and seeking declaratory and injunctive relief. Warshak's counsel sought the government's assurance that it would not seek additional orders under section

2703(d) directed at his e-mails, at least for some discrete period of time during the pendency of his civil suit. The government declined to provide any such assurance. In response, Warshak moved for a temporary restraining order and/or a preliminary injunction prohibiting such future searches. The district court ruled in Warshak's favor and granted an injunction. The government appealed.

The Context: Fourth Amendment Privacy Law at the Beginning of the 21st Century

To understand the Court of Appeals decision, a short review of constitutional law as it affects privacy may be useful. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing he place to be searched, and the persons or things to be seized." Normally, with quite a few exception, for a search or seizure to be reasonable, the government must obtain a warrant issued by a judge based on a finding of probable cause to believe that a crime has been, is being or is about to be committed and that the search will uncover evidence of the crime.

Sitting uneasily outside this framework are subpoenas. The government can use grand jury or administrative subpoenas to compel disclosure on a very low standard of relevance to a legitimate investigation. Indeed, the government does not need to suspect that any crime has been committed.[1] The subpoena for production of documents is sometimes called a "constructive search," but it is viewed differently because, unlike the warrant, it can be challenged before compliance is required. Subpoenas are issued on far less than probable cause. While the search warrant authorizes immediate seizure, a subpoena often calls for compliance at some point in the future (often 10 days). This gives the recipient of the subpoena the opportunity to go to court and challenge the subpoena, as the Sixth Circuit had explained in an earlier case:

> whereas the Fourth Amendment mandates a showing of probable cause for the issuance of search warrants, subpoenas are analyzed only under the Fourth Amendment's general reasonableness standard. ... One primary reason for this distinction is that, unlike "the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant[,]" the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced.[2]

The standard for enforcement of a subpoena is very low, but the ability to challenge is not meaningless. In addition, the process of challenge often involves negotiation between the government and the record holder in which the record holder educates the government

---

[1] In *United States v. Morton Salt Co.,* 338 U.S. 632, 652-53 (1950), the Supreme Court stated that an agency's request for documents should be approved by the judiciary so long as it "is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant."

[2] Doe v. United States, 253 F.3d 256, 263-64 (6th Cir. 2001), quoted in Warshak, slip op. at 9.

about the nature of the records it has and the government sometimes scales back its request to something more focused. This is what happened, for example, in the Google search terms case.

The subpoena is limited also by the Fifth Amendment's privilege against self-incrimination, which often means that an individual cannot be compelled to disclose records about himself.

The Warsahk court accepted this framework: the government can obtain sensitive personal records either with a warrant based on probable cause for immediate seizure or with a subpoena with notice and an opportunity to object.

As a result of Supreme Court decisions interpreting the Fourth and Fifth Amendments, this framework often provides no meaningful protection to the many records about our personal lives that are held by the businesses we interact with daily. In U.S. v. Miller and a series of other cases in the 1970s, the Supreme Court held that an individual retains no Fourth Amendment right in records disclosed to a third party like a bank. Consider, for example, the implications of this "business records" doctrine when the government seeks sensitive financial records: To seize a suspect's bank records from his desk at home, the government needs a search warrant issued on probable cause, or it needs to serve the suspect with a subpoena, giving him notice of the investigation and an opportunity to seek to narrow or quash the subpoena. Under U.S. v. Miller, however, the government can go to the bank with a mere subpoena and no notice to the record subject. The bank has a Fourth Amendment right to challenge the subpoena, but it has little grounds and less incentive to do so. Comparing the cost of attorney's fees with the cost of copying even large amounts of data onto a CD, banks, banks, ISPs and other businesses almost never challenge subpoenas for customer records. (Google's challenge to a subpoena for search records was an exception.) As to the Fifth Amendment, neither the bank nor the customer to whom the records pertain can raise the privilege in response to a subpoena served on the bank: the bank is not being compelled to do anything that would incriminate it and the customer, who may well be incriminated, is not being forced to disclose anything.

Miller and its progeny look increasingly suspect, given the richness of data held by businesses and the ease of accessing and analyzing it as a result of the digital revolution. There is a growing body of academic literature calling for a re-examination of the business records doctrine.[3]

---

[3] Profs. Patricia Bellia and Deirdre Mulligan have done the major work on this issue. See Patricia Bellia, "Surveillance Law Through Cyberlaw's Lens," 72 Geo. Wash. L. Rev. 1357 at 1403-09 (2004), and Deirdre Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," 72 Geo. Wash. L. Rev. 1557 at 1576-82, 1593-96 (2004). See also Susan Freiwald, "First Principles of Communications Privacy," Stan. Tech. L. Rev. (2007).

The Logic and Simplicity of the Warshak Decision

As noted, the Warshak court accepted this framework. However, the case presented in an unavoidable way the question of where stored email fits within the framework: is email just another business record in which the individual has no constitutionally protected privacy interest?

The Supreme Court has held that the Fourth Amendment protects people, not places. Whether something is protected turns on whether an individual has a "reasonable expectation of privacy" in whatever it is, real or virtual, that is going to be searched or seized. The Court has held that telephone calls are constitutionally protected because individuals have a reasonable expectation in the privacy of their calls even though they pass through networks owned by third parties and even though the phone companies can and sometimes do listen in for service quality monitoring and to protect themselves against theft of services. On the other hand, the Court has held, a bank customer has no reasonable expectation of privacy in his bank records since he knows that his bank has to look at and use the information on his checks and deposit slips.

The Supreme Court has never addressed the constitutional status of email. It is widely assumed that email in transit is just as fully protected as a telephone call. But unlike voice communications, email rests in storage on the network before it is read by the intended recipient – and increasingly, it is stored on the network even after it is read by the intended recipient.

In 1986, before email became popular and before email search and seizure cases had begun to percolate through the courts, Congress set a statutory framework for email in the Electronic Communications Privacy Act (ECPA). For government access to email in electronic storage for 180 days old or less, ECPA requires a search warrant issued on probable cause. However, ECPA treats older email somewhat like a business record, allowing the government to obtain access to at least some (maybe a lot) of a person's email with a mere subpoena to the service provider, affording the email subscriber neither the benefit of the probable cause determination nor an opportunity to challenge the subpoena.

Specifically, 2703(b) of ECPA provides:

> (b) Contents of wire or electronic communications in a remote computing service. (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--
>
> > (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
>
> > (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> >
> > (ii) obtains a court order for such disclosure under subsection (d) of this section;
>
> except that delayed notice may be given pursuant to section 2705 of this title.[4]

This is the provision the government relied on in Warshak. It is premised on the assumption that older email (or email not "in electronic storage" as defined in ECPA) does not enjoy the full protection of the Constitution's Fourth Amendment. However, that assumption has come to seem increasingly out of touch with the way email is used for a wide range of sensitive communications. Government access to stored email without either probable cause or a meaningful opportunity to object fits within the existing framework only if email is unprotected by the Fourth Amendment. Thus, the Warshak court was compelled to answer the question of whether customers have a reasonable expectation of privacy in their stored email.

The question of email's constitutional status had never before been directly confronted by an Article III federal court.[5] This may have been due in part to the fact that, until recently, ECPA's rule requiring a warrant for access to email stored by a service provider for less than 181 days had the practical effect of providing most email of many users with a statutory protection equivalent to that available under the Fourth Amendment. In 1986, when ECPA was adopted, and until recently, many users, such as AOL subscribers, accessed their email by downloading onto their own computers. The process generally resulted in the deletion of the email from the service providers' computers, and fee-based service providers encouraged their subscribers to delete old email from the service provider's system. To the extent that downloaded email, whether opened or unopened, was stored only on the user's computer, it was fully protected by the Fourth Amendment.[6]

---

[4] The court's slip opinion misprinted subsection (b), making it look as if the delayed notice proviso applied only to (b)(1)(B)(ii) when in fact delayed notice is available for both "(d) orders" and subpoenas.

[5] The U.S. Court of Appeals for the Armed Forces had confronted the issue and had ruled that email account holders have a reasonable expectation of privacy in their stored email. *See United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006); *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996).

[6] Internal systems of corporations were, and many still are, different.

Today, however, in contrast to 1986, a significant percentage of email is Web-based (including most consumer systems like AOL, Gmail, Hotmail, and YahooMail) and that web-based storage is free or very inexpensive. Accordingly, even opened email is kept for long periods of time on the computers of service providers like AOL, Google, MSN and Yahoo.

In Warshak, the government cited the business records cases for the proposition that a subpoena or court order issued without probable cause and without notice to the record subject is sufficient for access to stored records. In rejecting the government's analysis, the Sixth Circuit pointed out that in all the business records cases, the person to whom the records pertained had no reasonable expectation of privacy in them, for they had been disclosed to the business for use by its employees. The court stated:

> The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure — in this instance, the ISPs. If he does not, as in *Phibbs* or *Miller*, then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure.

The court went on to hold that email users do have a reasonable expectation of privacy in the content of their email. The court distinguished between content and transactional records. It assumed that the user does not, vis-a-vis the service provider, maintain an expectation of privacy in transactional data. As to content, however, the court stated, "simply because the phone company or the ISP **could** access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course."

The Sixth Circuit noted that email in storage was like the contents of a safety deposit box. The courts have held that, when an individual stores personal property with a third party, the owner of the property retains a privacy interest in the stored items, meaning that a warrant is required to search the storage space.

The Warshak court noted that the terms of service and practice of an email provider could deprive the user of any legitimate expectation of privacy, but the court emphasized that the government has a high burden to show that the reasonable expectation of privacy has been extinguished. The court held that the fact that the ISP retained, through its terms of service, some right to review email was insufficient to waive privacy expectations. "In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited … , the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service

provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy." What it requires, therefore, to extinguish the reasonable expectation of privacy is that "the government must show that the ISP or other intermediary clearly established **and** utilized the right to inspect, monitor or audit the content of e-mails. Slip op, at 14 (emphasis added).[7]

What mattered, said, the court, is that employees of commercial ISPs do not normally open and read -- and their subscribers do not expect them to open and read -- individual subscriber e-mails as a matter of course. The fact that ISPs regularly screen users' e-mails for viruses, spam, and child pornography was not sufficient to waive an expectation of privacy in the content of e-mails sent through the ISP. Likewise presumably, Google's scanning of email for purposes of delivering ads would not obliterate users' expectation that Google will not read their email for other purposes. Compelled disclosure of e-mails through notice to the ISP alone would be appropriate only if the government could show, based on specific facts, that an e-mail account holder has waived his expectation of privacy vis-a-vis the ISP.

Conclusions – The Impact of the Case, and Some Issues for Later Cases

The rule announced by Warshak brings some welcome clarity to the complexity created by ECPA and exacerbated by technology's ongoing evolution. ECPA established one rule for email less than 181 days old and a different rule for email more than 180 days old. The Justice Department argues that opened email less than 181 days old falls under the standard for email more than 180 days old. More broadly, there is uncertainty about what is "electronic storage," especially as technology has evolved. The Warshak decision cuts through all of this confusion, setting a simple rule for government access to email: A warrant based on probable cause, or a subpoena served with notice to the email subscriber.

The order at issue in the case, presumably drafted by DOJ, was carefully, albeit ambiguously, worded when it referred to "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak. Under ECPA, "electronic storage" is a defined term referring only to email in "temporary, intermediate storage … incidental to … transmission," plus backup storage. ECPA requires a warrant for access to email "in electronic storage" not more than 180 days. Email "in electronic storage" more than 180 days is available with a mere subpoena or an order under18 U.S.C. 2703(d). However, the Justice Department argues that email, once opened by the intended recipient, is no longer in "electronic storage" as defined under ECPA and loses the protection of the warrant standard, regardless of how fresh it is. That argument has

[7] At one point, the court said that the government would have to show that the ISP had "total access" to the email in question. Slip op at 14. t another point, the court said that the government would have to show that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business." Slip op. at 15.

been considered only by the Ninth Circuit Court of Appeals, and that court rejected it, but the decision is not binding outside the Ninth Circuit. The wording of the Warshak disclosure order suggests that DOJ outside the Ninth Circuit gets orders for email "not in electronic storage" on less than probable cause and uses those orders to obtain from service providers (who have little incentive to raise the Ninth Circuit decision) any opened email, regardless of how old it is, as well as opened and unopened email more than 180 days old.[8] It is also possible that DOJ interprets "not in electronic storage" to include even unopened email less than 181 days old, claiming that it is no longer in electronic storage "incidental to transmission" once it is "stored in directories or files owned or controlled" by the user. It is certainly likely that some service providers don't understand ECPA's finer points and turn over considerable amounts of email in response to a subpoena or court order issued on less than probable cause. The Sixth Circuit did not discuss these issues, but its ruling cuts through all of them by setting a single rule for all email and obviating any need to distinguish between the common meaning of "electronic storage" and ECPA's unique definition.

The Warshak rule subsumes the practical effect of the Theofel decision in the Ninth Circuit. Theofel interpreted "electronic storage" to include opened email, requiring a warrant in the Ninth Circuit for all email 180 days old or less. Warshak requires a warrant or a subpoena with notice for all email, period.

The Warshak decision, by bringing email under the Fourth Amendment, affords a suppression remedy to those whose email is illegally seized, which may result in more judicial decisions addressing government access to email. Some of those decisions may side with the government. Overall, the constitutionalization of email seizures should, over time, bring clarity to an area that has so far been analyzed only in statutory terms.

Warshak did not give a lot of consideration to two separate issues, possibly leaving them to later cases: (1) Is a warrant served on a service provider without notice to the subscriber sufficient under the Fourth Amendment? (2) Is a subpoena with notice to the record subject sufficient? The court assumed an affirmative answer to both (1) and (2). However, both (1) and (2) fall short of the paradigmatic reasonable search, which is one in which the government both obtains a warrant based on probable cause *and* serves it on the party in interest at the time of the search. There are arguments that, absent another exception to either the probable cause requirement or the notice requirement, a search is unreasonable if it lacks either one of these two elements. The subpoena seems to be especially weak, even with notice, since the standard for enforcement of a subpoena is so far below probable cause.

The Warshak court did not confront the Fifth Amendment implications of its decision. Compare Fisher v. US, 425 US 391 (1976), and US v. Hubbell, 530 US 27 (2000). Best left to other cases are questions such as whether the person could be immunized from the

[8] Inexplicably, the order said "greater than 181 days old:" it would seem that it should have said "greater than 180 days old" or "181 days old or older."

implications of compliance with the subpoena and still, consistent with the Fifth Amendment, be prosecuted using the email.

The Warshak court went only as far as it needed to go to decide the case before it: it granted Warshak the relief he had requested, enjoining the government from using a subpoena without notice to access email, unless the specific circumstances showed that the user did not retain an expectation of privacy in the email. The case brings a long-overdue measure of constitutional clarity to an area critical to privacy in the digital age.

For further information: Jim Dempsey, 202-365-8026 jdempsey@cdt.org