

New Limits on Access to Debtor's E-mail in Bankruptcy Crime Investigations

Written by: Meagan M. Gillette

Cox Smith Matthews Inc.; San Antonio
mgillette@coxsmith.com

Since at least 1986, the government and its attorneys have been facing the issue of seizing electronically stored information with federal legislation designed to assist them in doing so. Title II of the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§2701-2712, regulates the government's ability to obtain electronically stored information from third-party Internet service providers.

Under the Bankruptcy Code, the U.S. Trustee has a duty to seek the enforcement of the bankruptcy laws and rules and to address fraud and abuse in the bankruptcy system, although its power to enforce this mandate with the issuance of search warrants and similar types of process to investigate a debtor is unclear.¹ However, the U.S. Trustee has the power – and is obligated – to refer to the U.S. Attorney any potential criminal activity in the bankruptcy system. Indeed, the government's ability to address white-collar crime in the bankruptcy system is arguably contingent upon the U.S. Trustee's referral of bankruptcy crimes to the government's attorneys. One investigative tool available in such investigations is the ECPA.

A recent U.S. Sixth Circuit Court of Appeals opinion, *Warshak v. United States*, No. 06-4092, 490 F.3d 455 (6th Cir. June 18, 2007), limited the scope of the ECPA by concluding that the lower level of scrutiny required to obtain certain electronically stored communications from third party storage providers under the ECPA violated constitutional Fourth Amendment protections. While the practical impact of the opinion is currently unknown, it suggests a new limit on the government's "tool kit" in criminal investigations.

To a certain extent, the ECPA codifies the Fourth Amendment protections against unreasonable government searches and seizures with respect to electronically stored communications. Under the statute, the level of scrutiny and protection provided to a particular communication is determined by the type of third party storage provider and the length of time the communication has been in storage. For communications that have been stored less than 180 days, the government can only obtain such communications pursuant to a search warrant. If, however, the communications have been in storage for more than 180 days, the statute sets forth a sliding scale for the government to obtain the communications. The government may use (1) a search warrant complying with the traditional probable cause standard as well as using the normal procedures dictated by the Federal Rules of Criminal Procedure, (2) an administrative subpoena, or (3) a statutory court order. If the government uses either a subpoena or a court order, it must also provide notice to the subscriber, allowing the subscriber an opportunity to challenge the government's process. In addition, under this particular provision, the government may actually delay notice to the subscriber for up to 180 days upon application to a court for an appropriate

¹ For a discussion on the Fourth Amendment protections implicated by a U.S. Trustee's ability to issue warrants for the search of a debtor's residence, see Michael D. Sousa, *A Panel Trustee's Ability to Uncover Potential Debtor Abuse: Bankruptcy Law Meets the Fourth Amendment*, 24-7 AM. BANK. INST. J. 30 (September 2005).

order. The availability of delayed notice to the subscriber was the root of the controversy in *Warshak*.

In *Warshak*, the government had been pursuing an investigation of Steven Warshak and his company, Berkeley Premium Nutraceuticals Inc., on allegations of mail and wire fraud among other federal offenses. The government obtained an order of a local federal magistrate directing Warshak's Internet service provider (ISP) to turn over, *inter alia*, electronic communications stored by the ISP. Under the ECPA, such an order may be – and was in the case of Warshak – issued upon a showing of specific and articulable facts showing that there are reasonable grounds to believe that the communications are relevant and material to an ongoing criminal investigation, a standard that falls short of the traditional probable cause required to obtain a search warrant. The government also obtained an order delaying the statutory notice to be provided to Warshak. Upon learning of the ISP's compliance with the order, Warshak filed suit alleging that the compelled disclosure of his email without a warrant violated the Fourth Amendment and the ECPA. Warshak later sought a preliminary injunction prohibiting future disclosure after the government failed to assure Warshak that it would not seek additional disclosure of his email. The district court broadly granted Warshak's request for preliminary injunction and prohibited the government from seizing the contents of any email held by an ISP in the name of any resident of the Southern District of Ohio without providing the subscriber with an opportunity to challenge such seizure.

In examining the district court's injunction, the Sixth Circuit seemed to sidestep the preliminary issues of standing and ripeness to focus on the subscriber's expectation of privacy in emails held by an ISP. After summarizing a key Fourth Amendment precedent, the court agreed with the district court that an "individual maintains a reasonable expectation of privacy in emails that are stored with, or sent or received through, a commercial ISP." The court also found that the government failed to demonstrate that this expectation of privacy was undermined by the ISP's ability to access to the content of the email, without showing that an ISP's employees open and read – or subscribers reasonably expect them to open and read – individual subscriber emails as a matter of course (which could amount to a waiver). Ultimately, the Sixth Circuit affirmed the district court's grant of the preliminary injunction with one modification – where the government can show that a subscriber has waived his expectation of privacy in email *vis-à-vis* the ISP, compelled disclosure of emails with notice only to the ISP would be appropriate.

The government has requested rehearing *en banc*, and that is pending as of the writing of this article. Nevertheless, *Warshak* is an interesting and perhaps an important discussion on the application of traditional Fourth Amendment and search and seizure law in the context of electronic mail, including in bankruptcy crime investigations.