Paul Hastings

June 2007

StayCurrent

A Client Alert from Paul Hastings

"Reasonable Expectation of Privacy" in Stored E-Mail? Sixth Circuit Says "Maybe"

By Behnam Dayanim and Kelly DeMarchis

In an important ruling issued last week,[1] the United States Court of Appeals for the Sixth Circuit placed limits on the Government's power to seize e-mails under the Stored Communications Act (the "SCA" or the "Act"), finding that the e-mail account-holder in that case likely could demonstrate that he had a "reasonable expectation of privacy" in his communications.

WARSHAK V. UNITED STATES

Steven Warshak's Cincinnati-based company, Berkeley Premium Nutraceuticals, Inc., attracted the attention of the Federal Trade Commission with its widely disseminated advertisements for dietary supplements that promised everything from enhanced night vision to increased libido. The claims, unfortunately, were better than the results, and Berkeley Premium's money back guarantees were alleged to be as deceptive as the products they were backing. In the course of its investigation into Warshak and Berkeley Premium, the Government obtained two court orders to seize e-mails in Warshak's accounts from those accounts' internet service providers ("ISPs").Both orders were issued under seal, and Warshak was not notified of either order until over a year later.

THE STORED COMMUNICATIONS ACT

The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act, in an effort to reconcile the privacy protections of the Fourth Amendment with the borderless network of the internet. The Act was necessitated by differences in two "architectures"—while a home has physical walls that clearly demarcate the difference between private and public space (and the rights to privacy in communications within each type of space), the architecture of the internet requires that communications intended to be private travel through "public" spaces (shared computer servers) on the way to their final destination.

The SCA creates privacy protection for internet users' communications in this borderless environment. At issue in *Warshak* was the portion of the SCA, 18 U.S.C. § 2703, that permits the Government to seize the "contents of a wire or electronic communication, that is in electronic storage in an electronic communications system." The Government is required to obtain a search warrant for e-mails in storage for under 180 days. For e-mails in storage longer than that, the Government has three options: a search warrant, an administrative subpoena or a court order.

A search warrant requires the familiar showing of "probable cause." However, when the Government opts to use a court order, it need only proffer "specific and articulable facts showing that there are reasonable grounds to believe that the contents … or records … are relevant and material to an ongoing criminal investigation." Although e-mail account holders are supposed to receive notice of court orders, notice can be delayed for cause.

HOW *WARSHAK* LIMITS THE COURT ORDER POWER UNDER THE SCA

Warshak challenged the court orders in his case, arguing that he had a reasonable expectation of privacy in his e-mails and that to seize them, the Government had to meet the heightened probable cause standard imposed by the Fourth Amendment. The Government disputed

[1] *Warshak v. United States*, Case No. 06-4092 (6th Cir. June 18, 2007).

this contention, maintaining that no such expectation of privacy exists in e-mails stored with an ISP.

Warshak also argued – and the Government conceded – that the delay of over a year in providing notice of the seizures, without approval of the court, violated the statute. The Sixth Circuit did not need to address the impact of that failure in its decision.

Analogizing sending e-mails to mailing a letter, the Sixth Circuit found a reasonable expectation of privacy in e-mail content. Although e-mails **can** be accessed by third party ISPs, the court determined that e-mail account holders do not generally **expect** their e-mails to be accessed in this way, just as a letter writer knows postal workers handle mail, but does not expect them to open and read its contents. This expectation, that the substance of e-mails are assumed by the author to be private, persuaded the Sixth Circuit that the higher probable cause standard should apply to the seizure of e-mail, when effected without notice and opportunity to contest on the part of the account-holder.

Importantly, the court discounted two principal arguments advanced by the Government in reaching this conclusion. First, the court noted that language in the ISPs' user agreements allowing them to access e-mails under certain specified circumstances did not vitiate the reasonable expectation of privacy on the part of the account-holder. Because the circumstances under which the ISPs asserted rights of access were limited, the court concluded that the **generalized** expectation of privacy in those emails remained**.** Second, the court found ISPs' practice of scanning e-mail accounts for viruses and the like to be analogous to the postal service's scanning packages for drugs or dangerous contents. In each case, the sender of the e-mail or package nonetheless expects privacy in the substance of his or her communication.

WHAT HASN'T CHANGED

The *Warshak* court did not find a reasonable expectation of privacy in **all** e-mail communications. If an account-holder has notice that the content of his or her messages may regularly be reviewed or monitored, the court affirmed prior caselaw that there would no longer be a reasonable expectation of privacy in those messages.

In addition, the lower "reasonable grounds" standard continues to apply where the Government issues a subpoena to the account-holder or otherwise provides contemporaneous notice to the account-holder of a court order and the opportunity to contest the seizure. The higher "probable cause" protection was required here, said the court, precisely because no notice was provided.

IMPLICATIONS

The court's decision is interesting in that it reflects what perhaps may be a growing appreciation for the ubiquity of e-mail and the fact that millions of ordinary users treat e-mail communications much as they do their telephone conversations – as private and not subject to external prying. Companies and counsel have witnessed this phenomenon firsthand – often to their chagrin – in the context of civil litigation discovery.

In any event, the court's decision in this case reinforces the importance for employers, ISPs and others to examine closely the language of their electronic communications policies and user agreements. Employers should be sure to evaluate the nature of the notice provided to employees that their communications may be monitored, in order to limit potential privacy claims. In addition, they should take care to consider government orders for employee e-mails carefully before complying. It should not be accepted as a given that the employer may turn over those communications without notice to the employee.

Similarly, ISPs should scrutinize their own user agreements. Unlike an employer, an ISP may have sound reasons for wanting to limit its rights of access, in order to afford its customers the protections promised by the *Warshak* decision. An overly broad agreement – one that is broader than is needed to protect the ISP's interests – may inadvertently deprive customers of that level of protection. Moreover, before complying with a court order or similar process, the ISP should consider carefully whether notice to its customer is required.

As this is the first Circuit Court decision on this issue, the law will remain unsettled for quite some time. Whether other appellate courts follow the Sixth Circuit's approach remains to be seen.

❖ ❖ ❖

Paul Hastings' Privacy and Information Security Practice advises clients on all aspects of privacy and information security law and regulation, conducts privacy assessments, formulates and helps establish privacy and security compliance programs, and represents clients facing privacy enforcement investigations or litigation. We also represent clients in working with Congress and the Federal regulatory agencies in the formulation and implementation of public policy in this dynamic and important area. Behnam Dayanim is a partner and Kelly DeMarchis is an associate in Paul Hastings' Washington, DC, office.

For more information on the subject of this Alert or on any other privacy or information-security related topic, please contact:

New York

Erika Collins
(212) 318-6789
erikacollins@paulhastings.com

Washington, DC

Behnam Dayanim
(202) 551-1737
bdayanim@paulhastings.com

Kelly DeMarchis
(202) 551-1828
kellydemarchis@paulhastings.com

Los Angeles

Michael Lindsey
(213) 683-6262
michaellindsey@paulhastings.com

Stay*Current* is published solely for the interests of friends and clients of Paul, Hastings, Janofsky & Walker LLP and should in no way be relied upon or construed as legal advice. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some states. Paul Hastings is a limited liability partnership. Copyright © 2007 Paul, Hastings, Janofsky & Walker LLP.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.