

IN PRACTICE

## INTERNET LAW

### Internet Service Providers' Access to E-mail Content: Not an Invasion of Privacy

BY JONATHAN BICK

An Internet Service Provider (ISP) can legally search the e-mail that it processes. ISPs may lawfully search the content of users' e-mails for many purposes, including assisting law enforcement, ensuring compliance with the ISP's terms of use agreement and protecting the ISP from legal difficulties, to name a few. Such activities do not currently constitute an invasion of the e-mail user's privacy.

An ISP may process — and, hence, read — e-mails containing medical, legal and other information that the sender may desire to keep confidential. The Internet's protocol of passing e-mails through many computers, each of which copies (but does not necessarily delete) those e-mails, may result in access to confidential information by third parties simply because the Internet, when used as a communication system, is not designed to protect content privacy.

The court in *United States v. Richardson*, 607 F.3d 357 (2010), found that

*Bick is of counsel at Brach Eichler in Roseland. He is also an adjunct professor at Pace and Rutgers law schools, and the author of 101 Things You Need to Know About Internet Law (Random House 2000).*

the question of whether someone has a reasonable expectation of privacy in the content of her e-mail can be complex and difficult. However, this is not based on whether people actually expect their e-mail content to remain private, but on the fact that e-mail's role in society hasn't yet become clear.

Due to an increasing understanding of the Internet and terms of use agreements, which specifically state that ISPs are allowed to read the e-mail they process, Internet users have no reasonable expectation of privacy for their e-mail. Without an *expectation* of privacy, courts will not find such a *right* to such privacy.

E-mail users who understand that Internet protocol allows access by unauthorized third parties, thereby abandon their expectation of e-mail privacy *per se*. These e-mail users know that Internet protocol requires use of the "store-and-forward" model. They understand that typically, e-mails are sent to several intermediaries, including two ISPs (one for the sender and one for the recipient). Thus, knowledgeable e-mail users have no expectation of e-mail privacy; hence, their privacy cannot be violated by ISP access in the due course of processing their e-mail.

Both court rulings and contract law are the legal bases for divesting all other

Internet users of their expectation of e-mail privacy. Court decisions such as *United States v. Vaghari*, 653 F.Supp.2d 537 (2009), and *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (2008), have detailed Internet e-mail protocol and have uniformly held that the e-mail headers specifically, and e-mail generally, is not subject to Fourth Amendment protection when in the possession of a third party, such as an ISP.

Additionally, in order to reduce an ISP's secondary liability, most ISP terms-of-use agreements explicitly require e-mail users to abandon their expectation of e-mail privacy. Such agreements directly state that the ISP may access a user's e-mail for a host of reasons.

It should be noted that not all e-mail may be accessed by an ISP. For example, normally, if an e-mail exists solely in the sender's or recipient's computer, an ISP cannot physically (or lawfully) access it, and governmental access is limited by the Fourth Amendment. However, if a copy of an e-mail is stored on an ISP's computer, then it is accessible both legally and physically by the ISP and possibly the government.

An e-mail sent using a Post Office Protocol (POP) program is generally saved on the sender's and recipient's computer. Once the POP program has been executed, it is unusual for an ISP to have access to the e-mail that it processed. However, e-mail systems such as Gmail use an Interactive Message Access Protocol (IMAP) program which saves the e-mail on the ISP's computer. Such e-mail is accessible both legally and physically by the ISP, even after the completion of the IMAP process.

IMAP ISPs are currently free to access that e-mail on their own and turn

it over to law enforcement. Privacy laws and the Fourth Amendment limitation are not applicable because the ISP is an authorized third party.

It is generally accepted that the extent to which law enforcement can obtain e-mail content is strictly circumscribed. Due to the ISP agreement and the lack of an expectation of privacy, ISP access and use of e-mail content is virtually unlimited. Additionally, ISPs can restrict speech via e-mail processing with near impunity.

In addition to contract and expectation-related immunities, ISPs in the United States enjoy freedom from liability for the actions of third parties who use their networks, because they are treated as telecommunication providers by the Communications Decency Act of 1996. Also, as found by the court in *United States v. Forrester*, 495 F.3d 1041 (2007), ISPs are private actors that are not subject to

constitutional restrictions.

An ISP may even lawfully block an e-mail transmission based on reading its content. Just as other private Internet facilitators, including PayPal, Amazon, MasterCard and Visa, dropped their services to Wikileaks, an ISP may choose to whom it wishes to provide service. Computer programs, sometimes called Net Nannies, make it possible to search the content of each e-mail sent over a network and prevent its transmission without a noticeable change in service level.

It should be noted that ISPs need the ability to read the e-mail content they process in order to manage and secure their networks. In particular, ISPs need the ability to determine how much data there is to be transferred, where it's coming from, where it's going and whether any viruses, worms, bots or other malware are contained in the e-mail they process.

An ISP without the capability to search the content of the e-mail it processes could not inhibit spam or divert it to users' spam folders, nor could it detect and limit child pornography or comply with certain law enforcement requests. Without e-mail search capability, ISPs could not find and report potential national security threats or criminal conduct, such as "violent jihad" or "money laundering."

Technology also provides an alternative to existing naked e-mails. While an ISP can efficiently read e-mails, the same is not true for reading attachments or encrypted e-mails. Searching e-mail attachments and encrypted e-mails is time consuming and costly. Additionally, e-mail users can have a reasonable expectation that an attachment or encrypted e-mail will be private. Thus, privacy difficulties may be overcome via relatively simple, existing technological solutions. ■