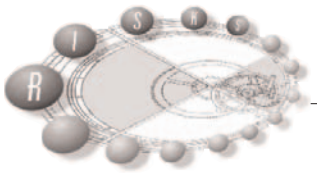

Deirdre K. Mulligan, Ari Schwartz, and Indrani Mondal

Risks of Online Storage

Exponential leaps in online storage capacity, along with a sharp drop in storage costs, have made it possible for Internet users to store large amounts of data online. Unless the law catches up, loss of privacy may be a hidden and unintended price of this new capacity because under current law, a consumer's personal communications and records in electronic storage with an ISP or other service provider receive less privacy protection than those same communications in transit, stored on the consumer's own computer, or hard copies stored in the home.

Protecting user privacy in this new environment requires revisions to the federal Electronic Communications Privacy Act (ECPA), improvement and clarity in industry policies for stored data, and user education. Outside the U.S., other nations are grappling with similar issues, but given the vast scope and complexity of the problem and differences in applicable law, our focus here is on practices and law in the U.S. Three main areas of concern relate to user privacy: diminishing relevance of traditional constitutional search and seizure rules; lack of transparency and clarity regarding ISP practices in storing or deleting subscriber email; and legal uncertainty surrounding what ISPs can do with users' personal information and communications.

The traditional sources of legal privacy protections for electronic data are the Fourth Amendment and ECPA. The Supreme Court has held that the Fourth Amendment protects a person's home and the content of telephone calls from unreasonable search and seizure. While the Court has never explicitly ruled on email, it has been assumed the same protection would apply to the contents of an email message in transit.

In a series of cases in the 1970s, the Supreme Court held that the Fourth Amendment does not apply to personal information voluntarily disclosed to a business. These "business record" decisions predated the digital revolution. There are serious questions whether the doctrine remains constitutionally sound, given the revealing nature of the vast quantity of data, email, photographs, and online diaries that individuals store electronically with businesses. It is time to reconsider the limits of the business records doctrine as applied to electronically stored data.

ECPA, which relied on a broad interpretation of the "business records" cases, is also outdated. Under ECPA, stored email is afforded less privacy protection than email in transit, and the level of protection afforded to stored email depends on the length of time it has been stored. This means the level of privacy protection given to email can change many times within an email message's life—changes that the vast majority of consumers do not recognize or understand. Compounding this issue is a lack of transparency from ISPs regarding the deletion of stored data. How long does an email message, or other data, remain on an ISP's servers after a user deletes it? (Often, "deleted" email will remain on backup storage unbeknownst to users.) Will ISPs automatically delete older email messages from their servers without notifying users? Each ISP should clearly communicate its policies to customers. Congress should eliminate the distinctions ECPA makes based on an email message's age, status as opened or unopened, or the type of provider who retains it, and should amend ECPA to require a search warrant for the government to access stored email content.

Another problem with ECPA was highlighted in a 2004 appeals court decision noting that an ISP could read stored subscriber email for its own business purposes without user consent. ECPA should be amended to clarify that ISPs may read subscribers' email only to provide the service, to protect the ISP's rights or property, or in other limited circumstances.

ECPA also provides insufficient guidance in civil litigation. ECPA does not provide a means for accessing the contents of email communications in the context of civil litigation, and sets no limits on the disclosure of other data about users to private parties including civil litigants. Legislation here is essential. A subpoena, at least, should be required for disclosure of subscriber identifying information and subscribers should receive notice prior to the release of any personal information.

The online storage revolution has outpaced privacy protections. Legal reform, improved industry practices, and consumer education are necessary to meet consumers' privacy expectations as their personal communications and records are remotely, digitally stored. C

Deirdre K. Mulligan is a clinical professor of law at UC Berkeley, **Ari Schwartz** is the deputy director of the Center for Democracy and Technology (CDT), **Indrani Mondal** was a summer intern at CDT. This column is adapted from their article, "Storing our lives online: Expanded email storage raises complex policy issues," *I/S: A Journal of Law and Policy for the Information Society* (Jan. 2005).

PAUL WATSON