Has Technology Outstripped Telephone Legal Protections?

By Peter P. Swire

Since 1967 Supreme Court cases have stood for a grand conception of the Fourth Amendment as a bulwark against wiretaps and other emerging forms of surveillance. But, changing technology means that many telephone calls are likely to be subject to routine recording in the near future. Because the Supreme Court has been so supportive of government access to stored records, its protective opinions on telephone interception may soon be dead on their facts.

The message of ***Miller v. U. S.*** in 1976 was that information voluntarily revealed to a third party, such as a bank, does not enjoy a "reasonable expectation of privacy." The message of ***Smith v. Maryland*** in 1979, as explained by Justice Potter Stewart, was that Fourth Amendment safeguards "do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes." The Stored Communications Act, first enacted in 1986 in the wake of ***Smith v. Maryland***, permits the government to get access to the content of ***stored communications*** from a communications provider without a warrant. Its complex rules allow access to the content of e-mail and other stored communications with less than probable cause.

What if the contents of ordinary telephone calls become stored as a matter of routine? This technological change would arguably, and plausibly, make the recording of the telephone call into a stored record subject to the Stored Communications Act. A search warrant would no longer be required.

This slide of telephone calls from content protected by the Fourth Amendment to stored records available under the Stored Communications Act has already begun. The looming question is what will happen if and when ordinary phone calls themselves are routinely stored.

This storage is likely to become far more common with the imminent growth of VOIP (Voice over Internet Protocol) telephone calls. VOIP uses the packet-switching network of the Internet to connect telephone calls rather than the traditional circuit-switching used by established phone systems. ***The Wall Street Journal*** reported in early 2004: "By the end of this year, about 20 percent of the new phones being shipped to U.S. businesses will use VOIP technology, according to Yankee Group, a technology consulting firm based in Boston. By 2007 that figure should exceed 50 percent, and eventually almost all of the new phones shipped will use VOIP."

Use of VOIP is likely to result in a drastic increase in storage of the content of telephone calls, for at least two reasons. First, the use of computers for making telephone calls makes it trivially easy for one party to store the contents of the conversation. This ease of storage makes a telephone call more like an e-mail, where users can foresee that the recipient may keep a copy of the communication or forward it to others. The ease of storage would make it easier for

PRIVACY JOURNAL
Founded in 1974
Robert Ellis Smith
Publisher
401/274-7861 fax 401/274-4747
orders@privacyjournal.net
www.privacyjournal.net

PRIVACY JOURNAL is published monthly, reporting on legislation, legal trends, new technology, and public attitudes affecting the confidentiality of personal information. **$125 a year, $165 overseas.** PRIVACY JOURNAL is available by postal mail, or by electronic mail, or in selected news and bookstores in the U.S. Back issues are available by mail in hard copy or in electronic form, by e-mail, or at our Web site. MasterCard, Visa, American Express, and Discover credit cards are accepted for payment. **CIRCULATION MANAGER:** Mikhail Zolikoff. **CONSULTING EDITOR:** Shauna Van Dongen

PRIVACY JOURNAL publishes: *Compilation of State and Federal Privacy Laws*, a book describing more than 1000 state and federal laws on confidentiality ($31, 2003). *Ben Franklin's Web Site*, a 407-page history of privacy in the U.S. reprinted in 2004 ($17.50). *War Stories IV*, accounts of individuals victimized by invasions of privacy, with the source of each story ($17.50, 2004). *A National ID Card, A License to Live*, a 46-page special report ($18.50, 2002). *The Law of Privacy Explained*, a 57-page legal guide to the current case law ($14.50, 2004). *Directory of Privacy Professionals*, listing 600 individuals and groups with knowledge in the field, including e-mail addresses ($18.50, 2003). *Our Vanishing Privacy*, a 132-page paperback published in 1993 with essays on consumer issues ($16.95). *Social Security Numbers: Uses and Abuses* ($14.95, 2001). *Index* from 1994 to October 2003 ($14.50).

Our Web site includes a sophisticated capability to download the texts of our reference books.

 ISSN 0145-7659. FEIN 52-1007918. Periodicals postage paid at Providence RI. **POSTMASTER:** Send address changes to PO Box 28577, Providence RI 02908 (offices at 89 Valley St., East Providence RI 02914). **MAILING ADDRESS:** PO Box 28577, Providence RI 02908 USA. **E MAIL:** orders@privacyjournal.net.

future courts to say that a user has voluntarily consented to storage by a third party. That storage, in turn, makes it less likely that the courts will hold there is a reasonable expectation of privacy in the communication.

A second technical change with VOIP is the likelihood that there will be systematic "caching," or storage, of telephone communications at the network level. One existing product, for instance, is called "CacheEnforcer," which stores phone conversations for a group of users, like a company or a university.

Once again, the existence of pervasive caching of telephone communications could undermine the earlier court holdings that there is a "reasonable expectation of privacy" in telephone communications.

The increasing storage of telephone calls is part of the much broader expansion since 1967 of stored records in the hands of third parties. A line of cases makes it quite possible that all of these records may be taken by the government without Fourth Amendment protections.

For instance, voice mail was rare in 1967, and e-mail practically unknown. Financial transactions have shifted away from cash to credit card, debit card, and other recorded transactions. Individuals now store their calendars, personal diaries, and family photographs online. Even the movements of individuals are being increasingly recorded.

With the rise of cellular telephones, and the regulatory requirement that such phones be readily located, the technology is in place to keep track of the movements of cell-phone users.

It is time for the courts to apply the Fourth Amendment to the many intrusive searches that employ new technologies or seek private information held by third parties. One new role for the courts would be what many had thought was the old role — a searching substantive inquiry into whether a search violates a person's "reasonable expectation of privacy."

Peter P. Swire is professor of Law, Moritz College of Law of the Ohio State University, and was Chief Counselor for Privacy in the Clinton Administration and chair of a White House working group on how to update electronic-surveillance law for the Internet age. This essay is adapted from his forthcoming article in the *Michigan Law Review*.

20 MINUTES A MONTH

PRIVACY JOURNAL *intern Mikhail Zolikoff of the University of Michigan Gerald R. Ford School of Public Policy provided this suggestion:*

Volunteering your time to a local organization is one thing. Volunteering your personal information to buy batteries is another. For years, some retailers have zeroed in on consumers at checkout, continually asking for Zip code or phone number. This may seem innocuous, but once that data is in someone else's hands you have little recourse regarding its use. It can conceivably be pooled with credit-card information to identify you and target unwanted advertising to you. Even when that's not the case, it's important to practice "just saying no" to requests for personal data of any kind in the marketplace. A further tip: Volunteer only as much information as is absolutely necessary to complete the transaction. MasterCard and Visa rules tell merchants ***not*** to ask for identifying information or even phone numbers if credit-card signatures match or the sale is authorized by telephone. (Of course, a phone number and address will be necessary if you want purchases delivered, but still the information should not go on your credit-card slip. To protect yourself, you may want to give a work number or landlord's number.) Above all, be prepared to shop elsewhere, where your privacy is respected.

Washington (Continued from page one)

tical dissidence in the McCarthy era," Craig said. His friend, Ashcroft, opposes the proposal.

The commission to investigate the 9-11 terrorist attacks is expected to recommend still further expansions of the government's authority to use the Foreign Intelligence Surveillance Act (FISA). The PATRIOT Act expanded such use so that evidence from wiretaps authorized by a FISA court for gathering foreign intelligence may now be used in criminal trials and so that a FISA court order has wide geographical applicability. The commission's report, due July 26, will likely recommend against "sunsetting" certain provisions of the PATRIOT Act, at the end of 2005, as required in the act. The expansion of FISA's authority is one provision that