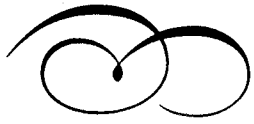
New technologies allow total strangers to know a lot more about you than you think. The ongoing invasion of your privacy will get much worse unless better safeguards are quickly established.

By Peter F. Eder

Privacy ON PARADE



YOUR SECRETS FOR SALE!

Would you want your closest friends or even your relatives to know everything about you? Who you called during the past week, what you bought at the drug store, what movies you rented at the video store, what you borrowed from the bank, how much money you owe, how well you've kept up on your payments? Would you want to surrender information about yourself in exchange for acquiring "free information"?

Today, many companies, many governmental bodies, and many organizations that most people would not recognize are gathering information and have assembled sophisticated databases that "know" all these things about you. They then sell that information to other firms and organizations that manipulate or add to the data for yet other purposes.

Are their motives sinister? Perhaps not. Most broadly, they gather this information because it makes it cheaper to market goods and services, keep track of transactions, minimize business risks, and operate more cost efficiently. As the mass market breaks apart into more and more segments, organizations must work harder to learn about consumers in greater detail.

Tied to this need is the explosion of available information and the dramatic changes in where the information is stored, how individuals can gain access to it, and what the individual has to pay in terms of monetary cost or the surrender of personal information for access and use.

More Information, Less Privacy

There are about 5 billion records now in the United States that describe each resident's whereabouts and other personal details. Information about each of us is moved from one computer to another an average of five times a day.

Information bureaus—private firms such as TRW, Equifax, and Trans Union—are the largest storehouses of information about Americans. Their 450 million records on 160 million individuals include birth dates, family makeup, current and previous addresses, telephone numbers, Social Security numbers, employment and salary histories, credit transactions and balances, mortgage rates, bankruptcies, tax liens, and legal entanglements.

That stupendous pile of data is dwarfed by the nearly 2,000 databanks maintained by the 178 largest federal agencies and departments and containing tens of millions of files each. The files of a single agency like the Social Security Administration or the Internal Revenue Service can boggle the mind. And for much of this personal information, the safeguards are fragile, and in-depth information on any individual may be readily accessible.

GARISON WEILAND

Penetration of these databases for mischief—or worse—is surprisingly easy, as investigative reporter Jeffrey Rothfeder demonstrates in his book *Privacy for Sale*. Given a few pieces of individual information—a Social Security number, a checking-account number, some simple mortgage information—a hacker can tap into startling amounts of sensitive information. Organizations can collect even more: Employers use records to screen employees and to control hiring practices in procedures that obviously violate the privacy rights of individuals, according to Rothfeder.

Privacy legislation has not had the priority in the United States that it has had in many other countries. In Europe, the notion of a data-protection panel is not strange or novel. Great Britain has had one since 1984, and Germany and France since 1978. Australia, Austria, Ireland, the Netherlands, Norway, and Sweden all have permanent data-protection agencies, and Canada has had an information-protection agency since 1978.

In the United States, the Privacy Act of 1974 was passed by Congress to "provide certain safeguards for an individual against invasion of privacy." The law says the government may not maintain secret databanks and mandates that all information the government collects about people be kept confidential. Under the legislation, you have the right to know about records pertaining to you, and you must be told who else sees them and how the information is used. Further, an agency is prohibited from sharing your records with anyone else and from using them for a secondary purpose without your written consent.

While the Privacy Act's aim was noble, the implementation has been inept. After an investigation in 1990, the General Accounting Office reported that the government is a sloppier caretaker of personal data now than it was before the Privacy Act went on the books!

The cause is technology. Prior to the passage of the Privacy Act, most records were stored manually and on paper. But in order to abide by the Privacy Act, federal agencies were forced to quickly computerize their backward systems. They needed computers to index the data they collected and to provide a means to sort through it quickly. With computers came new loopholes and weaknesses.

Insecure Social Security Information

While the government tries to protect the civil rights and privacy of individuals, its ineptitude is demonstrated in a spate of recent information break-ins and misuse of Social Security data. For example, networks of "information thieves" are infiltrating Social Security's computer files, stealing confidential personal records, and selling the information to whoever will buy it.

Investigators note that, while only a tiny fraction of Social Security's 200 million records have been compromised, hundreds of thousands of files have been stolen. The records are valuable, containing information about lifetime earnings, employment, current benefits, direct-deposit data, and bank-account numbers.

Buyers of this material include insurers, lawyers, employers, private detectives, and bill collectors. Investigators say the biggest trading is with lawyers seeking information

"Organizations need to be sensitive to the impacts of the growth of information [and] to the mischief and harm that can be created by misuse."

about litigants, health-care operations wanting data about people trying to collect claims, and employers doing background checks on prospective employees. Typically, thieves bribe Social Security workers for files that can then be sold for as much as 10 times the price of the bribe.

In one case, two executives pleaded guilty to conspiracy charges in 1992 for their role in buying and selling Social Security records. So far, at least 20 individuals in 12 states, including three former Social Security employees, have been indicted for allegedly participating in thefts.

Privacy Champions

In 1991, the U.S. Privacy Council was established and developed several broad objectives, many of which would require federal legislation. Its goals include:

- Requiring companies to get an individual's consent before transferring personal information electronically.
- Encouraging the development of new technology to protect privacy.
- Analyzing how government record-keeping systems affect privacy.
- Opposing the idea, popular among some law-enforcement agencies, of a national identification card.

Privacy issues are numerous, diverse, and often elusive. One point of dispute is that business firms often have unrestricted use of information that individuals provided voluntarily for a specific purpose. Privacy advocates argue that such use violates an understanding established between two parties when the information was first provided. As many as 69% of Americans favor barring businesses from distributing or selling information about customers without their permission, according to a poll by the Barna Research Group.

Another issue is the growth of technology that makes it easier to collect personal information. The Council is also trying to foster the establishment of a government data-protection board or privacy commission similar to those already in place in other countries.

A Tale of Two Companies

The U.S. government could learn much from a few companies that are responsibly dealing with privacy issues.

- **AT&T.** Through the years, AT&T personnel have set a high standard for ethical business conduct. Although AT&T is in a new, keenly competitive era, and change has become a way of life for its employees, one thing in its long heritage has not changed: its commitment to integrity, which every employee has a personal responsibility to sustain.

Here are some of the basic rules in AT&T's Personal Responsibility Guide:

1. Don't tamper with or intrude upon any transmission, whether by voice, nonvoice, or data.
2. Don't listen to or repeat other people's conversation or communication or permit them to be monitored or recorded, except as required in the proper management of business.
3. Don't allow an unauthorized person to have access to communications transmitted over AT&T facilities. This includes divulging information about who was speaking or what was spoken about, except as authorized by the customer or required in the proper management of the business.
4. Don't install or permit installation of any device that will enable someone to listen to, observe, or realize that a communication has occurred, except as authorized by an official service or installation order issued in accordance with company practices.
5. Don't use information from any communication, or even the fact that a communication has occurred, for your personal benefit or for the benefit of others.
6. Don't disclose information about consumer billing arrangements or the location of equipment, circuits, or trunks and cables to any unauthorized person.
7. Employees are responsible for ensuring that computer systems and the information they contain are adequately safeguarded against damage, alteration, theft, fraudulent manipulation, and unauthorized access or disclosure.

- **Equifax.** One of the Big Three credit-reporting companies (along with TRW and Trans Union), Equifax was founded in 1899 and employs 15,000 workers in 1,100 locations in the United States, Canada, and Europe. Its annual revenues exceed $1 billion. In recent years, Equifax has reexamined its operational practices in dealing with privacy and put into practice extensive and aggressive actions to be sensitive and responsible to public concerns.

In response to a series of actions, charges, and investigations by federal branches and state attorneys general, and also in response to increasing consumer dissatisfaction and complaints, Equifax launched a benchmark consumer survey on privacy in 1990 and then quickly implemented a series of sweeping reforms. The company engaged privacy expert Alan F. Westin of Columbia University to establish a series of privacy audits and to act as a consumer ombudsman.

Equifax developed a series of fair-information practices to be implemented throughout the corporation. The company has:

1. Established 24-hour, toll-free access to credit reports (the first such system in the United States).
2. Discontinued the sale of direct-marketing lists derived from its consumer credit files.
3. Created a corporate-level office of consumer affairs.

Medical Records and Privacy

Computerizing medical records may improve and streamline the U.S. health-care-delivery system, but it threatens to make private information less private.

As the computerization of medical records proceeds, federal laws will be needed to resolve issues of patient privacy, according to a new report by the U.S. Office of Technology Assessment (OTA). Current laws "do not provide consistent, comprehensive protection for privacy of medical information," either computerized or in paper form.

Without new legislation, the unfortunate result will be a chipping away of the already-limited privacy protection now in place for medical information, say the authors of *Protecting Privacy in Computerized Medical Information*.

"Existing models for data protection will no longer be workable," warn the authors. For one thing, the increased networking of computers means that medical information will no longer be managed by a single institution.

The OTA researchers recommend that legal limits for access to computerized medical information be established. Issues such as informed patient consent for information disclosure, standardization of information storage, and access by secondary users will have to be resolved to protect a patient's right to privacy.

The challenge is in balancing the individual's right to privacy with the need for access of "appropriate information" for approved uses, such as medical research. The report acknowledges that "health information and medical records include sensitive personal information that reveals some of the most intimate aspects of an individual's life." Disclosure of certain medical information can lead to a denial of access to credit, admission to educational institutions, and the ability to secure employment and obtain insurance. As a result, "inaccuracies in the information, or its improper disclosure, can threaten personal and financial well-being."

Pilot programs in other countries—such as the Framework for European Services in Telemedicine—prove that the day when these issues are dealt with regularly is soon approaching. With the possible realization of such innovations as home telemonitoring (to reduce the need for bed space and ambulance costs), teleconsultation (enabling specialists to confer more easily), and the interlinking of doctors and hospitals, a flood of medical information over the "cyberwaves" would be sure to follow.

The key to keeping medical information private, say the OTA researchers, is to get a head start on the problem. Dealing with the issues of privacy at the onset of computerization will enable "system designers [to] build the appropriate mechanisms into software that will implement privacy policy."

Sources: *Protecting Privacy in Computerized Medical Information*, Office of Technology Assessment, Washington, D.C. 20510. Telephone 202/228-6204. Available from the U.S. Government Printing Office (GPO stock no. 052-003-01345-2), P.O. Box 371954, Pittsburgh, Pennsylvania 15250. 1993. 168 pages. $10.

Mediascience International, Av. Pré des Agneaux, 83, B-1160 Brussels, Belgium. Telephone (32) 2242 24 11.

4. Sponsored a series of consumer forums, drawing on 25,000 panelists and designed to obtain information about consumer preferences, trends, and needs.

5. Continued its annual survey of consumer opinions on privacy issues.

6. Put in place an intricate new software system that ensures the proper placement and protection of credit information.

7. Publicized consumer rights under the Fair Credit Reporting Act and the information industry program that allows people to delete themselves from direct-mail lists.

Recommendations for the Future of Privacy

The actions of AT&T and Equifax are a step in the right direction at the corporate level and offer a model for all organizations, public and private. Organizations need to be sensitive to the impacts of the growth of information, to the complexity and cost of acquiring it, to its diminishing free availability, to the rights of every individual to privacy, to the mischief and harm that can be created by misuse, and to the need to practice responsibility at every link in the communications chain.

Here are some further recommendations:

1. We need to determine and place responsibilities. Like AT&T and Equifax, other corporations must develop and maintain fair and firm systems of control and information protection.

2. There has to be a clear definition of the role of government in the process. Government must apply the same strictures to itself as it does to nongovernmental organizations and effectively monitor its vast agencies and bureaucracies.

3. Privacy protections and information-access policies need to be expanded in order to deal with emerging technologies.

4. Consumers must understand the extent of the problem and be encouraged to become actively involved in ensuring their own individual protection and rights.

5. Information collected for any specific purpose or reason should be used only for that reason. Usage for a different purpose could not occur without the individual's specific, active consent. In fact, the personal information should be jointly owned by the consumer and the institution that collects the data.

6. Individuals should have easy and direct access to any information on themselves for the purpose of

"If the Declaration of Independence were rewritten today [consumers] would add privacy to the list of life, liberty, and the pursuit of happiness as a fundamental American right."

knowing, copying, correcting, completing the information, or limiting its usage. Perhaps it should be automatically reported back to each individual on an annual basis.

7. Legal limits should be placed on the collection and use of sensitive information. Any exemptions for national security or civil protection reasons must be clearly defined and publicly stated.

8. All keepers of information databases should have periodic "privacy audits" to determine the effectiveness of their control policies.

9. There should be specific enforcement measures in place, and there should be penalties—civil and criminal—for violations. These enforcements should be created and tailored to protect the individual.

Consumers and Privacy

The time now seems ripe for action. In 1970, only one-third of Americans reported being concerned about invasion of privacy. The figure grew to 47% by 1977 and 79% in 1990.

In 1990, when Equifax launched its first annual poll on consumer attitudes toward privacy, nearly 80% of U.S. consumers responding indicated that if the Declaration of Independence were rewritten today they would add privacy to the list of life, liberty, and the pursuit of happiness as a fundamental American right.

Among the findings of the Equifax study:

- A majority of the Americans polled (55%) felt that protection of information about consumers will worsen by the year 2000.
- More than two-thirds (68%) said present uses of computers are an actual threat to personal privacy.
- More than three-fourths of the public (76%) felt that consumers have lost all control over how personal information about them is circulated and used by companies.
- If privacy is to be preserved, the use of computers must be sharply restricted in the future, according to 67% of respondents.
- While the majority believed that it is all right for companies to check public-record information on consumers applying for credit (71%), auto insurance (77%), or jobs (75%), 80% said it is *not* all right if the consumer has not initiated a transaction.
- To protect people's privacy in the future, 83% of the respondents considered it important for consumer advocacy groups to expose abuses, bring up lawsuits, and sponsor legislation.

While America's founders lacked the wisdom in the eighteenth century to mandate that privacy be an inalienable right, no less an eminent legal scholar than Supreme Court Justice Louis Brandeis, in delivering a dissenting opinion in the 1928 Olmstead phone-tap case, declared privacy "the most comprehensive of rights and the right most valued by civilized man."

Our awareness has been raised; our resistance, increased. We must act with vigor and vigilance to ensure our privacy, for it is a right that affects every individual with an identity and a personal history. □

About the Author
Peter F. Eder is vice president of client services at Wahlstrom & Company, a telephone directory advertising agency. His last article for THE FUTURIST was "The Future of Advertising: Consumption in the Information Age" (July-August 1993). His address is Wahlstrom & Co., 1290 East Main Street, Stamford, Connecticut 06902. Telephone 203/348-7347; fax 203/348-7350.