

Read the article "Death of Privacy" and answer Numbers 1 through 8.

DEATH OF PRIVACY

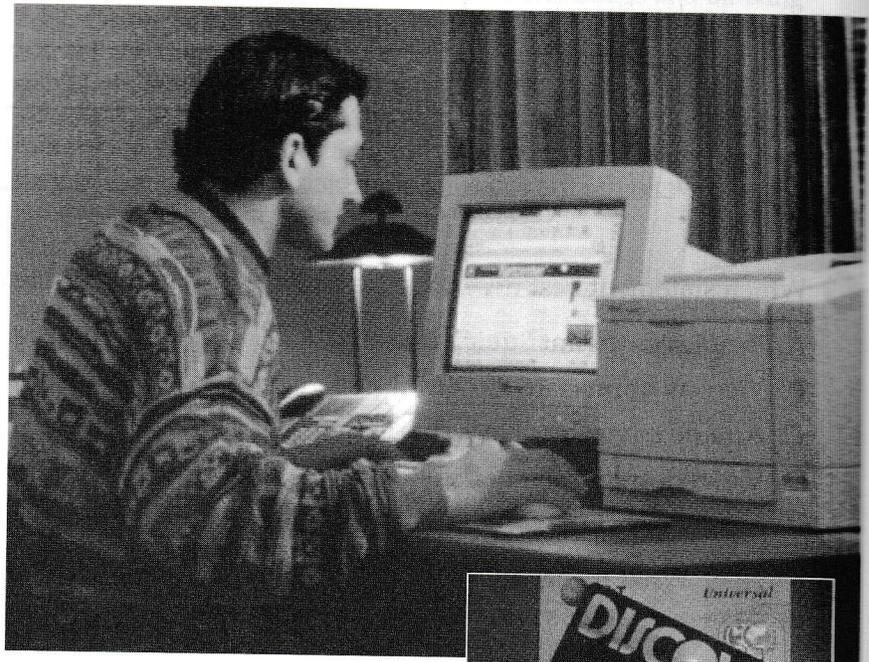
By Christine Varney

Cyberspace security: Information technology can be a threat as well as a blessing. What rules do we need to prevent misuse of all the personal data that we trail behind us when we navigate the Web?

At the beginning of the last century, my grandparents sailed to America, leaving behind their Irish farming village. The people in their community knew my family's history, their opinions and personalities, friendships and feuds.

At the beginning of this century, we are in some ways returning to that village. On-line and at work, we are organizing ourselves as a series of tight knit communities where secrets are very hard to keep. We are, once again, becoming a transparent society—one where everyone knows everything about everyone else in real time. But today, the communities are digital and often global, and the information isn't in words but bytes. There also are some significant differences between today's electronic transparency and the personal familiarities of the rural agrarian village.

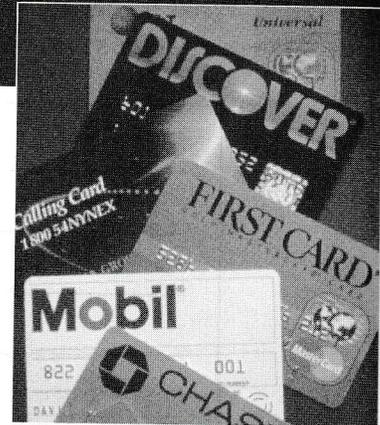
These differences, in fact, give rise to one of the most complex questions we face as we enter this new era: how do we reconcile our concerns about personal privacy with the massive new flow of readily available personal information? The decisions we are making today could determine whether we bequeath our children a society in which their lives are enhanced by modern information



A man browses at an online store.

technology, or one in which they feel themselves the victims of it.

In my ancestral village back in Ireland, people had the advantage of context. My grandparents knew most of the people they received information about; they were in a position to evaluate its accuracy. And more often than not, sharing information fostered a closer sense of community. In their village, knowing that someone was ill, for example, allowed others to lend a hand. The utter absence of privacy was sometimes annoying; every small town had



its gossips and its ruined reputations. But social sanctions—all the more powerful because everybody know everybody else—generally kept people from misusing personal information.

By contrast, in today's data-rich environment where information is free-floating and widely available, there is no context. Information is open to interpretation without first-hand knowledge of the individuals involved. There are few sanctions—legal, social or otherwise—against abusing or exploiting it.

This is the crux of the problem. When we shop often at a particular Web site, we don't mind if that site gives us discounts because we are good customers—it's called rewarding loyalty. But we are outraged to learn that information about us can be used to determine our "price flexibility"—marketing jargon for the maximum amount we might pay for an item based on our previous buying behavior.

Where do we draw the line? In the U.S. Congress and in the states, lawmakers are looking for ways to protect consumers and help guide the collection and use of personal information online. There is general agreement that sensitive information—regarding our health, our finances, our children—is entitled to the highest degree of protection. New laws now govern all three of those areas. But even here, in an area that seems relatively straightforward, the devil is in the details. Recently, for example, I went looking on-line for asthma medicine for an ailing relative. I was confronted with a variety of banner ads selling asthma-related products and services. The ads were helpful. With a simple click, I found informational sites I didn't know existed. But, I wondered, what electronic tracks had I left behind me? The ads enhanced my ability to sort relevant and irrelevant

information. I am comfortable with that. I will be much less comfortable if my search is associated with my name or used for purposes like marketing products that I don't want.

Who owns information? That is the heart of the matter. In the United States, federal law has little to say about information in the private sector, but there is a wealth of law on the books restricting the government's ability to gather and keep information about us. Perhaps because Americans long ago fought for their independence from a foreign government, Americans have never been shy about passing laws—in addition to the Fourth and Fifth Amendments to the Constitution—to protect us from unwarranted government intrusion into our personal lives.

Europeans have taken a different approach. For many years in most of Europe, a citizen was "entered on the government rolls" at birth to record his religion, register him in the health-care system and for voting later on. Europe evolved a set of rules allowing virtually unrestricted government use of such information. However, a much stricter set of rules than in America developed regarding corporate abuse of personal data. The differences between these two views of privacy have led to protracted negotiations over the last few years about the flow of personal information between Europe and the United States. The Europeans want to see if the privacy practices of U.S. companies adequately meet their expectations: they are offering "safe harbor" to companies that do. U.S. companies are now reviewing what sorts of privacy practices will satisfy Europe's stricter data-protection laws. What is at stake here is the disruption of

the flow of information between Europe and the United States. Much remains unclear.

In the U.S. Congress and the state legislatures, two opposing forces are lining up for a fight. On the one hand, there are those who say the private sectors efforts to create a framework for protecting privacy have failed and congress must step in. Others argue that industry efforts are sufficient and oppose legislation of any kind. Both are missing the point.

The point, in the Information Age, is to give consumers the power to protect their privacy. Whether obtaining medical or financial information on the Net or buying the latest CD on-line, consumers are entitled to know that their personal interests are not being stored in someone else's data bank. In some instances, the answer may lie in privacy-enhancing technologies that allow us to surf the Web anonymously. In the end, there may be loopholes in existing laws that need to be closed or a lack of law that needs to be filled. Always, there is need for an educated public.

Too often the privacy debate has been polarized between those who wish to fully prohibit the use of personal information and those who wish to fully exploit it. Most of us have a foot in both camps: we welcome the marvelous benefits of information technology, but we have an equally powerful desire for personal privacy. Perhaps the most that can be hoped for is a modus vivendi not unlike that reached in my grandparent's village. They may have chafed sometimes at their lack of privacy, but it gave them a sense of belonging to a larger community—as long as it was not abused. Common sense, in the end prevailed. That is what we should aim for today as well.

Answer questions 1-8. Base your answers on the article "Death of Privacy."

- 1 What is the author's purpose in writing this article?
- A. to compare the global community to an Irish village
 - B. to share ways to protect personal information on-line
 - C. to ease fears about sharing personal information on-line
 - D. to complain about the abuse of personal information by companies
- 2 How does the author feel about companies gathering personal information for marketing purposes?
- F. She is angered by it.
 - G. She is flattered by it.
 - H. She is surprised by it.
 - I. She is encouraged by it.
- 3 What is the author's opinion of European privacy practices?
- A. She disapproves of their practice of recording people's religions.
 - B. She approves of the social services provided by those governments.
 - C. She thinks they do a better job of keeping personal information from government.
 - D. She thinks they do a better job of protecting private information from corporations.
- 4 What does the following excerpt tell you about the author's point of view?
- Too often the privacy debate has been polarized between those who wish to fully prohibit the use of personal information and those who wish to fully exploit it. Most of us have a foot in both camps: we welcome the marvelous benefits of information technology, but we have an equally powerful desire for personal privacy.**
- F. She feels the Internet is a great threat, and should be used with care.
 - G. She believes there will never be a solution that makes everyone happy.
 - H. She thinks the new technology is good, but wants to protect her privacy.
 - I. She imagines that many new laws will be needed to protect personal privacy.
- 5 Which of the following can you infer from the passage about European citizens?
- A. They are distrustful of privacy-enhancing technology.
 - B. They fear exchanging personal information with anyone.
 - C. They are wary of exchanging information with the United States.
 - D. They are fearful of giving their personal information to the government.

