Computers and the Threat to Privacy

It's hardly news any longer: we live in the so-called Information Age. Information, virtually all of it stored in computer databases, is the lifeblood of the public and private bureaucracies that dominate postindustrial society. The quest for ever-greater levels of efficiency has led to a scramble to obtain more and more information about individual citizens and consumers.

Yet, while many people express concerns about the loss of their privacy, most of us are willing accomplices. Do you use a bank card at ATM machines? Do you shop by mail order or visit commercial websites? Do you browse websites on the Internet? If so, you are being tracked, and most of us realize it. Yet, we are unwilling to change our habits. Why? Because, perhaps when it comes right down to it, we value convenience over privacy.

Here are just a few examples of how by doing very simple, everyday things you inadvertently leave electronic footprints, and how those might be used by others:

- At work, you send an e-mail saying unflattering things about your boss. Your company (as do many corporations) routinely reviews e-mails, so your boss reads yours. You are dismissed. You file a suit, but lose. The prospective employer at the next job you apply for uses an Internet investigation service to check records and your lawsuit is discovered. What do you think your chances are of being employed by that firm?
- You have allergies and call an 800 number to check pollen count in your area. Your number is recorded by caller ID, and you are put on a list of allergy sufferers. The list is sold to a drug company. Next thing you know, you are sent a coupon for that company's allergy medication.
- You are eating out, and order a burger with fries. At the restaurant, your order is entered into a computer. You pay by credit card. The restaurant then checks your credit rating and sends you a discount offer for your next visit. Unfortunately, the restaurant goes bankrupt, and its list of burger and fries lovers goes on the information market.

Those are just a few examples, some innocuous sounding, some not. But what about direct abuses?

Here are a few examples:

- Some years ago, a convicted child rapist who worked at a Boston hospital went through 1000 computerized records seeking potential victims. He was caught when the father of a nine-year-old girl traced his call back to the hospital using caller ID.
- A banker who was also working for Maryland's state health commission accessed a list of known cancer patients and identified the names of his bank's customers who were ill. The bank revoked the loans of those people.
- A large company that sells baked goods planned to work together with a healthcare company to analyze employee health records and work performance reports to identify workers who might benefit from antidepressants sold by the healthcare company.

Unusual? No. An increasing share of companies check health information before hiring someone. But what about the government gathering information about you? The FBI has a database on the millions of people who have ever been arrested, even if they were not convicted. Government abuses are

currently regulated by the Privacy Act of 1974, but many feel that this law needs to be updated to keep pace with technological innovation. Harvard law professor Lawrence Tribe supports an amendment to the Constitution ensuring that the Bill of Rights will not be endangered by developing communication and computer technologies.

Critics who wonder whether such safeguards are really necessary need only look to the Orwellian steps now being taken by the Thai government. By 2006, information on 65 million Thais was stored in a single, integrated computer network and each citizen over age of fifteen is required to carry a photo ID with an identification number. This card allows the government to obtain the citizen's fingerprints, height, home address, parents' and children's names, marital status, education, occupation, income, nationality, religion, and, potentially, criminal records.

In spite of resistance to these pools of private information, the means of accessing some basic data about individuals seems to be growing easier. Through search engines on the Internet's World Wide Web such as Google and Yahoo!, anyone with Internet access can enter an individual's name to look for his or her phone number, residential address, email address, and in some cases, a map showing where in a city that person lives. Once that far, anyone can find out what that person does for a living, the names and ages of a spouse and children, the kind of car that person drives, the value of the person's house, and the taxes paid on it.

Kevin Kelly, executive editor of *Wired* magazine, points out that privacy also did not exist in the traditional village or small town. The difference back then was that people knew about each other, creating a kind of symmetry of knowledge. That's what has changed. Today's technology allows more organizations to gather more information about us without our knowledge—and without our knowing how, why, or by whom this information may be used.

Discussion Questions:

1. What sorts of personal information should be kept private? Is it even possible today to keep information private?

2. Is the loss of privacy a result of technology that cannot be regulated? Or do you think that new laws and regulations can protect the interests of citizens and customers?