CHAPTER

5 Privacy

Count not him among your friends who will retail your privacies to the world.

–PUBLILIUS SYRUS (100 BCE)

5.1 Introduction

COMPUTERS AND THE INTERNET HAVE ACCELERATED THE RATE AT WHICH ORGANIZATIONS can collect, exchange, combine, and distribute information about individuals. All these capabilities make it a challenge to preserve your privacy.

Are you familiar with Google's Phonebook service? If you visit the Google Web site and type my phone number in as a query, it returns a page giving my name and address. Click on a link, and the screen shows a map to my house. Phonebook can do this because it's easy for a computer to combine information from multiple sources, as long as they share a key. In this case the common key is my home address. Given my phone number, Phonebook accesses telephone directory records to learn my address. It can then consult a geographic information system to determine my home's location from its address [1].

Someone in campus security at Georgetown University accidentally sent out to the entire campus community an email crime report containing the names of three students. To protect these students, system administrators shut down the email system at Georgetown University for several hours and deleted the offending email from the mailboxes

of the recipients [2]. This incident illustrates the power of modern communication networks to broadcast personal information at high speed. It's also a reminder that system administrators have the ability to read our email messages.

In 1993 Maryland created a database containing medical records of its residents. The purpose of the database was to help the state find ways to contain health care costs. A member of Maryland's public health commission, who happened to be a banker, had access to the database. He used this information to call in the loans of his customers who had cancer [3].

In 2005 a senior at UMass Dartmouth was collecting materials for a research paper on communism he was writing for one of his history classes. The campus library did not have a copy of Mao Tse-Tung's "Little Red Book," so he filled out an interlibrary loan request, giving his name, address, phone number, and Social Security number. A couple of months later, two agents of the Department of Homeland Security visited him. They told him the book is on a "watch list." The student's interlibrary loan request, combined with the fact that he had spent significant time abroad, apparently triggered the visit. His professor said, "I shudder to think of all the students I've had monitoring al-Qaeda Web sites, what the government must think of that" [4].

On the morning of July 18, 1989, actress Rebecca Schaeffer opened the door to her apartment and was shot to death by obsessed fan Robert Bardo. Bardo got Schaeffer's home address from a private investigator who purchased her driver's license information from the California Department of Motor Vehicles [5]. In response to this murder, the U.S. Congress passed the Driver's Privacy Protection Act in 1994. The law prohibits states from revealing certain personal information provided by drivers in order to obtain licenses. *It also requires states to provide this information to the federal government.*

In this chapter we focus on privacy issues related to the introduction of information technology. We begin by taking a philosophical look at privacy. What is privacy exactly? Do we have a natural right to privacy distinct from other rights, such as the right to property and the right to liberty? What about our need to know enough about others that we can trust them? How do we handle conflicts between the right to privacy and the right to free expression?

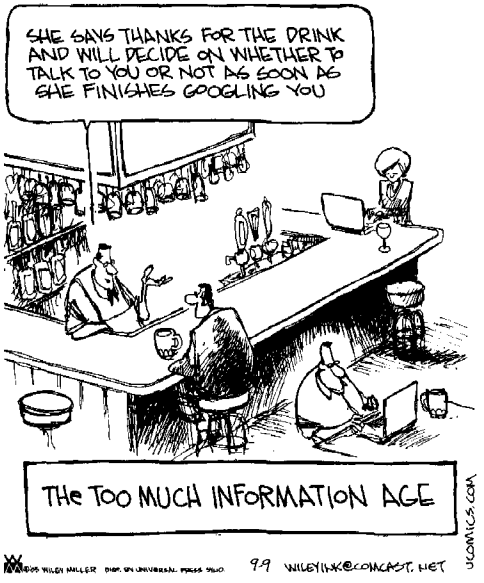
We then survey some of the ways that we leave an "electronic trail" of information behind us as we go about our daily lives. Both private organizations and governments construct databases documenting our activities. A variety of laws have been passed to regulate the collection and distribution of information gathered by private and public entities. We will study what these laws do—and don't do—to protect individual privacy.

With new technologies have come new ways for governments to intercept the communications of their citizens. We examine the history of covert electronic surveillance by the U.S. government, and how the Fourth Amendment to the Constitution has put boundaries around the surveillance activities of law enforcement organizations. Since 1968, Congress has passed a variety of laws allowing various forms of surveillance by law enforcement and intelligence agencies. Most notable is the USA PATRIOT Act, passed after the September 11, 2001, hijacking of four passenger airliners. Because the Patriot Act gives the government many new powers to collect information, it has generated contro-

versy. We'll examine the major provisions of the Patriot Act and the concerns raised by its detractors.

Next, we take a look at data mining, an important tool for building profiles of individuals and communities. Companies use data mining to improve service and target product marketing to the right consumers. Governments use it to fight crime and enhance national security. The Department of Defense and the National Security Agency have created new data mining programs in response to the terrorist attacks of September 11. Like the Patriot Act, these programs have raised the ire of privacy advocates.

Identity theft is an increasingly common crime. We describe a variety of ways in which thieves steal credit card numbers and other personal and financial information. The Social Security number has become a commonly used identifier; we study its weaknesses. Some have proposed the creation of a new national identification card for the Unites States. We consider the arguments in favor and against this idea, and we discuss the implications of the REAL ID Act of 2005.



© Wiley Miller.

How can people preserve their privacy in the Information Age? One powerful tool is encryption. New encryption technology allows individuals to send messages that are very difficult, if not impossible, for others to decipher. Another tool is digital cash, a technology enabling people to make anonymous transactions in the Information Age. We survey both of these technologies, as well as the attempts by the U.S. government to prevent strong encryption software from being exported to foreign countries.

5.2 Perspectives on Privacy

5.2.1 Defining Privacy

Philosophers struggle to define privacy. Discussions about privacy revolve around the notion of *access*, where access means either physical proximity to a person or knowledge about that person. There is a tug of war between the desires, rights, and responsibilities of a person who wants to restrict access to himself, and the desires, rights, and responsibilities of outsiders to gain access.

Edmund Byrne takes the point of view of the individual seeking to restrict access when he defines privacy as a "zone of inaccessibility" that surrounds a person [6]. You have privacy to the extent that you can control who is allowed into your zone of inaccessibility. For example, you exercise your privacy when you lock the door behind you when using the toilet. You also exercise your privacy when you choose not to tell the clerk at the video store your Social Security number. However, privacy is not the same thing as being alone. Two people can have a private relationship. It might be a physical relationship, in which each person lets the other person become physically close while excluding others. It might be an intellectual relationship, in which they exchange letters containing private thoughts.

When we look at privacy from the point of view of outsiders seeking access, the discussion revolves around where to draw the line between what is private and what is public (known to all). As Edward Bloustein has pointed out, stepping over this line and violating someone's privacy is an affront to that person's dignity [7]. You violate someone's privacy when you treat him or her as a means to an end. Put another way, some things ought not to be known. Suppose a friend invites you to see a cool movie trailer available on the Web. You follow him into the computer lab. He sits down at an available computer and begins to type in his login name and password. While it is his responsibility to keep his password confidential, it is also generally accepted that you ought to avert your eyes when someone is typing in their password. Another person's password is something that you should not know.

On the other hand, society can be harmed if individuals have too much privacy. Suppose a group of wealthy white, Anglo-Saxon, Protestant men forms a private club. The members of the club share information with each other that is not available to the general public. If the club facilitates business deals among its members, it may give them an unfair advantage over others in the community who are just as capable of fulfilling the contracts. In this way privacy can encourage social and economic inequities, and the public at large may benefit if the group had less privacy (or its membership were more diverse).

Here is another example of a public/private conflict, but this one focuses on the privacy of an individual. Most of us distinguish between a person's "private life" (what they do at home) and their "public life" (what they do at work). In general, we may agree that people have the right to keep outsiders from knowing what they do away from work. However, suppose a journalist learns that a wealthy candidate for high public office has lost millions of dollars gambling in Las Vegas. Does the public interest outweigh the politician's desire for privacy in this case?

In summary, privacy is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information.

5.2.2 Harms and Benefits of Privacy

HARMS OF PRIVACY

Giving people privacy can result in harm to society. Some people take advantage of privacy to plan and carry out illegal or immoral activities. Ferdinand Schoeman observes that most wrongdoing takes place under the cover of privacy [8].

Edmund Leach suggests that increasing privacy has caused unhappiness by putting too great a burden on the nuclear family to care for all of its members. He notes that in the past, people received moral support not just from their immediate family, but also from other relatives and neighbors. Today, by contrast, families are expected to solve their own problems, which puts a great strain on some individuals [9].

On a related note, family violence leads to much pain and suffering in our society. Often, outsiders do not even acknowledge that a family is dysfunctional until one of its members is seriously injured. One reason dysfunctional families can maintain the pretense of normality as long as they do is because our culture respects the privacy of each family [10].

Humans are social beings. Most of us seek some engagement with others. The poor, the mentally ill, and others living on the fringes of society may have no problem maintaining a "zone of inaccessibility," because nobody is paying any attention to them. For outcasts, privacy may be a curse, not a blessing.

BENEFITS OF PRIVACY

According to Morton Levine, socialization and individuation are both necessary steps for a person to reach maturity. Privacy is necessary for a person to blossom as an individual [11].

Jeffrey Reiman has defined privacy as the way in which a social group recognizes and communicates to the individual that he is responsible for his development as a unique person, a separate moral agent [12]. Stanley Benn reinforces this point when he says that privacy is a recognition of each person's true freedom [13].

Charles Sykes argues that privacy is valuable because it lets us be ourselves, suggesting the following example [14]. Imagine you are in a park playing with your child. How would your behavior be different if you knew someone was carefully watching you, perhaps even videotaping you, so that he or she could tell others about your parenting skills? You might well become self-conscious about your behavior. Few people would be able to carry on without any change to their emotional state or physical actions.

In a related observation, Gini Graham Scott points out that privacy lets us remove our public persona [15]. Imagine a businessman who is having a hard time with one of his company's important clients. At work he must be polite to the client and scrupulously avoid saying anything negative about the client in front of any coworkers, lest he demoralize them, or even worse, lose his job. In the privacy of his home he can "blow off

steam" by confiding in his wife, who lends him a sympathetic ear and helps motivate him to get through the tough time at work. If people did not have privacy, they would have to wear their public face at all times, which could be damaging to their psychological health.

Other philosophers have pointed out the ways in which privacy can foster intellectual activities. Constance Fischer has pointed out that privacy allows us to shut out the rest of the world so that we can focus our thoughts without interruption [16]. Robert Neville describes how privacy is needed to live a creative life [17]. Joseph Keegan argues that privacy is needed for spiritual growth, the opportunity to become intimate with the Absolute Being [18].

Charles Fried goes a step further, stating that privacy is the only way in which people can develop relationships involving respect, love, friendship, and trust. According to Fried, "privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable" [19]. Fried refers to privacy as "moral capital." People use this capital to build intimate relationships. Taking away people's privacy means taking away their moral capital. Without moral capital, they have no means to develop close personal relationships.

James Rachels voices a similar sentiment, when he writes that "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people" [20]. Charles Sykes echoes Rachels when he says that each person has a "ladder" of privacy [14]. At the top of the ladder is the person we share the most information with. For many people this person is their spouse. As we work our way down the ladder, we encounter people we would share progressively less information with. Here is an example of what someone's ladder of privacy might look like:

spouse
priest/minister/rabbi
brothers and sisters
parents
children
friends
in-laws
coworkers
neighbors
marketers
employers
government
news media
ex-spouses
potential rivals/enemies

On the other hand, Jeffrey Reiman is critical of suggestions that tie intimacy too closely to sharing information [12]. A woman might tell her psychoanalyst things she would not even reveal to her husband, but that does not imply she experiences deeper intimacy with her psychoanalyst than with her husband. Intimacy is not just about sharing information, it's also about caring. The mutual caring that characterizes a healthy marriage results in a greater level of intimacy than can be gained simply by sharing personal information.

SUMMARY

To summarize our discussion, allowing people to have some privacy has a variety of beneficial effects. Giving people privacy is one way that society recognizes them as adults and indicates they are responsible for their own moral behavior. Privacy allows people to develop as individuals and to truly be themselves. Privacy gives people the opportunity to shut out the world, be more creative, and develop spiritually. Privacy gives each of us the opportunity to create different kinds of relationships with different people. Privacy also has numerous harmful effects. Privacy provides people with a way of covering up actions that are immoral or illegal. If a society sends a message that certain kinds of information must be kept private, some people caught in abusive or dysfunctional relationships may feel trapped and unable to ask others for help. Weighing these benefits and harms, we conclude that allowing people at least some privacy is better than denying people any privacy at all. That leads us to our next question: Is privacy a natural right, like the right to life?

5.2.3 Is There a Natural Right to Privacy?

Most of us agree that every person has certain natural rights, such as the right to life, the right to liberty, and the right to own property. Many people also talk about our right to privacy. Is this a natural right as well?

LEVINE: PRIVACY RIGHTS EVOLVE FROM PROPERTY RIGHTS

Morton Levine has shown how our belief in a right to privacy grew out of our property rights [11]. Historically, Europeans have viewed the home as a sanctuary. The English common law tradition has been that "a man's home is his castle." No one—not even the King—can enter without permission, unless there is probable cause of criminal activity.

In 1765 the British Parliament passed the Quartering Act, which required American colonies to provide British soldiers with accommodations in taverns, inns, and unoccupied buildings. After the Boston Tea Party of 1773, the British Parliament attempted to restore order in the colonies by passing the Coercive Acts. One of these acts amended the Quartering Act to allow the billeting of soldiers in private homes, breaking the centuries-old common law tradition and infuriating many colonists. It's not surprising, then, that Americans restored the principle of home as sanctuary in the Bill of Rights.

THIRD AMENDMENT TO THE UNITED STATES CONSTITUTION

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

In certain villages in the Basque region of Spain, each house is named after the person who originally constructed it. Villagers refer to people by their house names, even if the family living in the house has no relation to the family originally dwelling there.

These examples show a strong link between a person and his property. From this viewpoint, privacy is seen in terms of control over personal territory, and privacy rights evolve out of property rights.

WARREN AND BRANDEIS: CLEARLY PEOPLE HAVE A RIGHT TO PRIVACY

We can see this evolution laid out in a highly influential paper, published in 1890, by Samuel Warren and Louis Brandeis. Samuel Warren was a Harvard-educated lawyer who became a businessman when he inherited a paper manufacturing business. His wife was the daughter of a U.S. Senator and a leading socialite in Boston. Her parties attracted the upper-crust of Boston society. They also attracted the attention of the *Saturday Evening Gazette*, a tabloid that delighted in shocking its readers with lurid details about the lives of the Boston Brahmins.[1] Fuming at the paper's coverage of his daughter's wedding, Warren enlisted the aid of Harvard classmate Louis Brandeis, a highly successful Boston attorney (and future U.S. Supreme Court justice). Together, Warren and Brandeis published an article in the *Harvard Law Review* called "The Right to Privacy" [21]. In their highly influential paper, Warren and Brandeis argue that political, social, and economic changes demand recognition for new kinds of legal rights. In particular, they write that it is clear that people in modern society have a right to privacy and that this right ought to be respected. To make their case, they focus on—you guessed it—abuses of newspapers.

According to Warren and Brandeis:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy the prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers . . . The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so

1. To learn more about the Boston Brahmins, consult Wikipedia (www.wikipedia.org).

> that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. [21]

Meanwhile, Warren and Brandeis argue, there are no adequate legal remedies available to the victims. Laws against libel and slander are not sufficient because they do not address the situation where malicious, but true, stories about someone are circulated. Laws addressing property rights also fall short because they assume people have control over the ways in which information about themselves is revealed. However, cameras and other devices are capable of capturing information about a person without that person's consent.

Warren and Brandeis pointed out that the right to privacy had already been recognized by French law. They urged the American legal system to recognize the right to privacy, which they called "the right to be let alone" [21]. Their reasoning was highly influential. Though it took decades, the right to privacy is now recognized in courts across America [22].

THOMSON: EVERY "PRIVACY RIGHT" VIOLATION IS A VIOLATION OF ANOTHER RIGHT

Judith Jarvis Thomson has a completely different view about a right to privacy. She writes: "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is" [23]. Thomson points out problems with defining privacy as "the right to be let alone," as Warren and Brandeis have done. In some respects, this definition of privacy is too narrow. Suppose the police use an X-ray device and supersensitive microphones to monitor the movements and conversations of Smith in his home. The police have not touched Smith or even come close to him. He has no knowledge they are monitoring him. The police have let Smith alone, yet people who believe in a right to privacy would surely argue that they have violated Smith's privacy. In other respects, the definition of privacy as "the right to be let alone" is too broad. If I hit Jones on the head with a brick, I have not let him alone, but it is not his right of privacy I have violated—it is his right to be secure in his own person.

Thomson argues that whenever the right to privacy is violated, another right is violated as well. For example, suppose a man owns a pornographic picture. He doesn't want anyone else to know he owns it, so he keeps it in a wall safe. He only takes it out of his safe when he has taken pains to prevent others from looking into his home. Suppose we use an X-ray machine to look into his home safe and view the picture. We have violated his privacy, but we have also violated one of his property rights—the right to decide who (if anybody) will see the picture.

Here is another example. Suppose a Saudi Arabian woman wishes to keep her face covered for religious reasons. When she goes out in public, she puts a veil over her face. If I should walk up and pull away her veil to see her face, I have violated her privacy. But I have also violated one of her rights over her person—to decide who should touch her.

According to Thomson, there are a cluster of rights associated with privacy, just as there are a cluster of rights associated with property and a cluster of rights associated with our physical self. However, every violation of a privacy right is also a violation of a right in some other cluster. Since this is the case, there is no need to define privacy precisely or to decide exactly where to draw the line between violations of privacy and acceptable conduct.

BENN AND REIMAN: AUTONOMOUS MORAL AGENTS NEED SOME PRIVACY

Instead of referring to privacy as a natural right, Stanley Benn proposes that privacy principles be based on the more fundamental principle that each person is worthy of respect [13]. We give each other privacy because we recognize privacy is needed if people are to be autonomous moral agents able to develop healthy personal relationships and act as free citizens in a democratic society.

Jeffrey Reiman expands on Benn's view. He writes:

> The right to privacy protects the individual's interest in becoming, being, and remaining a person. It is thus a right which *all* human individuals possess—even those in solitary confinement. It does not assert a right never to be seen even on a crowded street. It is sufficient that I can control whether and by whom my body is experienced in some significant places and that I have the real possibility of repairing to those places. It is a right which protects my capacity to enter into intimate relations, not because it protects my reserve of generally withheld information, but because it enables me to make the commitment that underlies caring as *my* commitment uniquely conveyed by *my* thoughts and witnessed by *my* actions. [12]

Note Reiman's fairly restricted view of privacy. He carefully points out areas where privacy is necessary. He does not argue that privacy is a natural right, nor does he suggest that a person has complete control over what is held private.

CONCLUSION: PRIVACY IS A PRUDENTIAL RIGHT

In conclusion, people disagree whether there is a natural right to privacy. Even if there is no natural right to privacy, most commentators cite the benefits of privacy as a reason why people ought to have some privacy rights. Alexander Rosenberg calls privacy a *prudential right*. That means rational agents would agree to recognize some privacy rights, because granting these rights is to the benefit of society [24].

APPLICATION: TELEMARKETING

Telemarketing provides a good example of how privacy is treated as a prudential right. After being sworn in as Chairman of the Federal Trade Commission (FTC) in 2001, Timothy Muris looked for an action that the FTC could take to protect the privacy of Americans. It did not take long for the FTC to focus on telemarketing. A large segment of the American population views dinner-time phone calls from telemarketers as an annoying invasion of privacy. In fact, Harris Interactive concluded that telemarketing is the reason why the number of Americans who feel it is "extremely important" to not be

disturbed at home rose from 49 percent in 1994 to 62 percent in 2003 [25]. Responding to this desire for greater privacy, the FTC created the National Do Not Call Registry (www.donotcall.gov), a free service that allows people who do not wish to receive telemarketing calls to register their phone numbers. The public reacted enthusiastically to the availability of the Do Not Call Registry by registering more than 50 million phone numbers before it even took effect in October 2003 [26, 27].

The Do Not Call Registry will not eliminate 100 percent of unwanted solicitations. The regulations exempt political organizations, charities, and organizations conducting telephone surveys. Even if your phone number has been registered, you may still receive phone calls from companies with which you have done business in the past eighteen months. Still, the Registry is expected to keep most telemarketers from calling people who do not wish to be solicited. The creation of the Registry demonstrates that privacy is seen as a prudential right: the benefit of shielding people from telemarketers is judged to be greater than the harm caused by putting limits on telephone advertising.

5.2.4 Privacy and Trust

While many people complain about threats to privacy, it is clear upon reflection that we have more privacy than our ancestors did [28]. Only a couple of centuries ago our society was agrarian. People lived with their extended families in small homes. The nearest community center was the village, where everyone knew everyone else and people took a keen interest in each other's business. The Church played an important role in everyday life. In this kind of society there was a strong pressure to conform [15]. There was greater emphasis on the community and lesser emphasis on the individual.

Charles Sykes writes: "Over the past two centuries, the rise of the modern has been the rise of the individual" [14]. He points out that prosperity, the single-family home, the automobile, television, and computers have contributed to our privacy. The single-family home gives us physical separation from other people. The automobile allows us to travel alone instead of on a bus or train in the presence of others. The television brings entertainment to us inside the comfort of our homes, taking us out of the neighborhood movie theater. With a computer and an Internet connection, we can access information at home rather than visit the public library [14]. These are just a few examples of ways in which modern conveniences allow us to spend time by ourselves or in the company of a few family members or friends.

In the past, young people typically lived at home with their parents until they were married. Today, many young unmarried adults live autonomously. This lifestyle provides them with previously unthought-of freedom and privacy [28].

The consequence of all this privacy is that we live among strangers. Many people know little more about their neighbors than their names (if that). Yet when we live in a society with others, we must be able to trust them to some extent. How do we know that the taxi driver will get us where we want to go without hurting us or overcharging us? How do parents know that their children's teachers are not child molesters? How does the bank know that if it loans someone money, it will be repaid?

In order to trust others, we must rely on their reputations. This was easier in the past, when people didn't move around so much and everyone knew everyone else's history. Today, society must get information out of people to establish reputations. One way of getting information from a person is through an **ordeal,** such as a lie detector test or a drug test. The other way to learn more about individuals is to issue (and request) **credentials,** such as a driver's license, key, employee badge, credit card, or college degree. As Steven Nock puts it, "A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy" [28].

5.3 Disclosing Information

As we go about our lives, we leave behind an electronic trail of our activities, thanks to computerized databases. Databases record the purchases we make with credit cards, the groceries we buy at a discount with our loyalty cards, the videos we rent by showing our driver's licenses, the calls we make with our telephones, and much more. The companies collecting this information use it to bill us. They also can use this information to serve us better. For example, Amazon.com uses information about book purchases to build profiles of its customers. With a customer profile, Amazon.com can recommend other books the customer may be interested in buying.

It's important to distinguish between public information and public records [29]. A **public record** contains information about an incident or action reported to a government agency for the purpose of informing the public. Examples of public records are birth certificates, marriage licenses, motor vehicle records, criminal records, and deeds to property.

Public information is information you have provided to an organization that has the right to share it with other organizations. A good example of public information is a listing in a telephone directory. Most of us allow our name, address, and phone number to appear in telephone directories. By doing this, it is easier for our friends and acquaintances to call us or stop by our home. We judge this benefit to be worth the cost to us in the form of less privacy.

Personal information is information that is not public information or part of a public record. You may consider your religion to be personal information. It remains personal information as long as you never disclose it to an organization that has the right to share it. However, if you do disclose your religious affiliation to such an organization, it becomes public information.

Personal information becomes public information or a public record through a voluntary, involuntary, or statutory disclosure (Figure 5.1).

Often people voluntarily make personal information public. Product registration forms and contest entries often ask consumers to reveal a great deal of personal information. I once received a product preference survey from Proctor & Gamble; it said, in part,

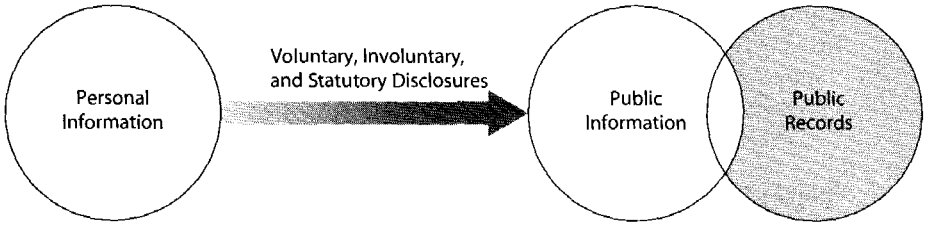


Figure 5.1 Personal information becomes public information or part of a public record as the result of a voluntary, involuntary disclosure, or statutory disclosure. The Privacy Act of 1974 puts some restrictions on access to information in public records. (We will discuss the Privacy Act in Section 5.6.4.)

> Your opinions matter to us. That's why we've selected you to participate in one of the most important consumer research surveys we'll do this year. Whether or not you have completed one of our surveys in the past, you can help us continue to create the products that meet your needs. Simply answer the following questions, provide your name and address and mail it back to us. That way, we will be able to contact you if there are any special offers that might be of interest to you.

The questionnaire asked about my family's use of nasal inhalants, coffee, peanut butter, orange juice, laundry detergent, fabric softener, household cleaner, deodorant, toothpaste, detergents, skin care and hair care products, cosmetics, mouthwash, diapers, laxatives, and disposable briefs. It provided a list of 60 leisure activities, ranging from various sports to travel to gambling, and asked me to choose the three activities most important to my family. It also asked my date of birth, the sex and age of everyone living in my home, my occupation, the credit cards we used, and our annual family income. If I had returned the questionnaire (which I didn't), all of this information would have become public.

Sometimes you must disclose information in order to get something you want. If you want to fly on an airplane, you must allow others to search your luggage. You may even be subjected to a body search. You cannot refuse these searches if you want to travel by air. If you want to get a loan from a bank, you must provide the bank with your full name and Social Security number (so it can do a credit check), as well as detailed information about current income, your assets, and your liabilities. If you want to get married, you must fill out a marriage license and submit yourself to whatever tests are required by the local jurisdiction.

At other times, personal information becomes a public record without your consent. Police agencies and courts maintain records of arrests and convictions. Divorce records are public, and they can contain a significant amount of personal information.

Finally, information is sometimes gathered without our knowledge. There are more than a half million closed-circuit television cameras installed in public places in England. A resident of London may be captured on tape many times every day. A principal reason

for installing these cameras is to reduce crime. However, detractors of this system point to abuses. Some allege that prosecutors have destroyed video footage that may have cleared a suspect. Others say that camera operators have acted like high-tech peeping Toms, using the cameras to watch people having sex [30].

5.4 Public Information

In this section we survey just a few of the many ways that personal information can become public information.

5.4.1 Rewards or Loyalty Programs

Rewards or loyalty programs for shoppers have been around for more than 100 years. Your grandparents may remember using S&H Green Stamps, the most popular rewards program in the United States from the 1950s through the 1970s. Shoppers would collect Green Stamps with purchases, paste them into booklets, and redeem the booklets by shopping in the Sperry and Hutchinson catalog for household items.

Today, many shoppers take advantage of rewards programs sponsored by grocery stores. Card-carrying members of the store's "club" save money on many of their purchases, either through coupons or instant discounts at the cash register. The most significant difference between the Green Stamps program and a contemporary shopper's club is that today's rewards programs are run by computers that record every purchase. Companies can use information about the buying habits of particular customers to provide them with individualized service.

For example, Safeway has unveiled computerized shopping carts at two of its stores in northern California. The shopping cart, called Magellan, has a small computer on the front handle and a card reader on the side. Customers identify themselves by swiping their Safeway Club card through the card reader. The computer taps into the database with the customer's buying history and uses this information to guide the customer to frequently purchased products. As the cart passes through the aisles, pop-up ads display items the computer predicts the customer may be interested in purchasing. It also lets customers purchase some products at sale prices unavailable to others [31].

Critics of grocery club cards say that the problem is not that card users pay less for their groceries, but that those who don't use cards pay more. They give examples of club-member prices being equivalent to the regular product price at stores without customer loyalty programs [32].

Some consumers respond to the potential loss of privacy by giving phony personal information when they apply for these cards. Others take it a step further by regularly exchanging their cards with those held by other people [33].

5.4.2 Body Scanners

Looking good is important to many, if not most, of us. Computer technology is making it possible for us to save time shopping and find clothes that fit us better (Figure 5.2).

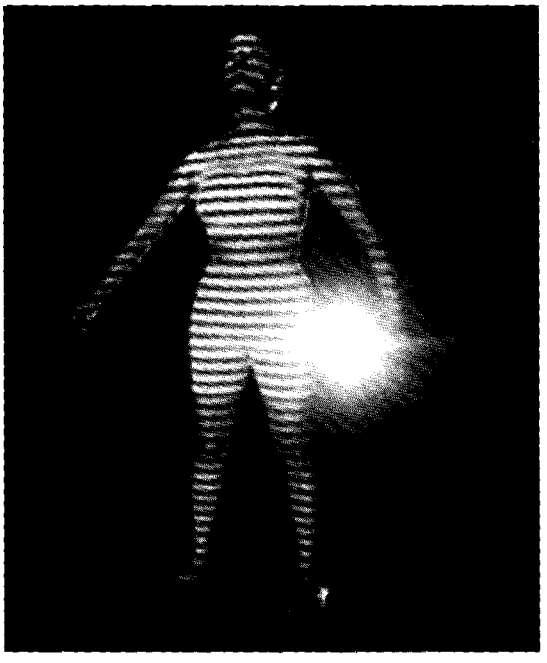


FIGURE 5.2 A computer takes a customer's measurements. (AP/Wideworld Photos)

In some stores in the United Kingdom, you can enter a booth, strip to your undergarments, and be scanned by a computer, which produces a three-dimensional model of your body. The computer uses this information to recommend which pairs of jeans ought to fit you the best. You can then sit in front of a computer screen and preview what various pairs of jeans will look like on you. When you have narrowed down your search to a few particular brands and sizes, you can actually try on the jeans.

Body scans are also being used to produce custom-made clothing. At Brooks Brothers stores in the United States, customers who have been scanned can purchase suits tailored to their particular physiques [34].

5.4.3 Digital Video Recorders

TiVo, Inc. manufactures a digital video recorder (DVR), which is similar to a VCR except that it records TV programs on a hard disk instead of videotape. TiVo also provides a service that allows its subscribers to more easily record programs they are interested in watching later. For example, with a single command a subscriber can instruct the TiVo to record every episode of a TV series. What many consumers may not know is that TiVo sells detailed information about the viewing habits of its customers. Because the system monitors the activities of the user second by second, its data are more valuable than that provided by other services. For example, TiVo's records show that 54 percent of its customers skip commercials [35].

5.4.4 Automobile "Black Boxes"

You probably know about airplane flight data recorders, also called "black boxes," which provide information useful in postcrash investigations. Did you know that modern automobiles also come equipped with a "black box"? A microprocessor attached to the car's airbag records information about the speed of the car, the amount of pressure being put on the brake pedal, and whether the seat belts are connected. After a collision, investigators can retrieve the microprocessor from the automobile and view data collected in the five seconds before the accident [36].

5.4.5 Enhanced 911 Service

The U.S. Federal Communications Commission has passed an enhanced 911 mandate that requires cell phone providers to be able to track the locations of active cell phone users to within 100 meters. The safety benefit of enhanced 911 service is obvious. Emergency response teams can reach people in distress even if they are unable to speak or do not know exactly where they are.

The ability to identify the location of active cell phone users has other benefits. For example, it makes it easier for cell phone companies to identify where signal strength is weak and coverage needs to be improved. In the past, this information had to be gained by sending people into the field to check signal strength, à la the Verizon commercial ("Can you hear me now? Good!").

The downside to enhanced 911 service is a loss of privacy. Because it is possible to track the location of active cell phone users, what happens if information is sold or shared? Suppose you call your employer and tell him you are too sick to come into work. Your boss is suspicious, since this is the third Friday this winter you've called in sick. Your employer pays your cell phone provider and discovers that you made your call from a ski resort [37].

5.4.6 RFIDs

Imagine getting up in the morning, walking into the bathroom, and seeing a message on the medicine cabinet's computer screen warning you that your bottle of aspirin is close to its expiration date. Later that day, you are shopping for a new pair of pants. As you try them on, a screen in the dressing room displays other pieces of clothing that would complement your selection.

These scenarios are possible today thanks to a new technology called RFID, short for radio frequency identification. An RFID is a tiny wireless transmitter. Manufacturers are replacing bar codes with RFIDs, because they give more information about the product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached (or embedded), and a scanner can read an RFID from six feet away. When barcodes are replaced by RFIDs, check-outs are quicker and companies track their inventory more accurately (Figure 5.3).

However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. Imagine a workplace full of RFID scanners. A

FIGURE 5.3 Employees take inventory more quickly and make fewer errors when items are marked with RFID tags. (Courtesy Tibbett & Britten)

scanner in your cubicle enables a monitoring system to associate you with the tags in your clothes. Another scanner picks up your presence at the water cooler. The next thing you know, your boss has called you in for a heart-to-heart talk about how many breaks you're taking. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase [38, 39].

The U.S. government plans to replace traditional passports with electronic passports equipped with RFID tags. The RFID tag would duplicate the passport's identifying information and include a digital photograph. By combining the RFID tag's information with new facial recognition technology, the government hopes to improve security at border crossings. Critics of this plan say that RFID tags can be read by anyone within 25 feet who has a powerful enough chip reader. They fear that these tags could make travelers more vulnerable to identity theft [40]. Others wonder if terrorists with powerful RFID tag readers might begin "scanning" foreign cafes, searching for locations with a high concentration of Americans [41]. Some experts, however, claim that these fears are exaggerated and that RFID tags are difficult to read at a distance [42].

5.4.7 Implanted Chips

In Taiwan every domesticated dog must contain a microchip implant identifying its owner and residence [43]. The microchip, about the size of a grain of rice, is implanted into the dog's ear using a syringe.

Verichip Corporation makes an RFID tag approved for use in humans. More than 2,000 people worldwide have had a Verichip implant. The most common reason for getting an implanted RFID chip is to alert doctors to a medical condition. Even if the

patient is unconscious, a doctor can retrieve valuable medical information from the chip [44]. In some trendy European nightclubs, patrons can leave their wallets at home and use their RFID chips as in-house "debit cards" for purchasing food and drinks [45].

Some people believe that parents should implant microchips in their children. They say that the life of a child is more important than any concerns about privacy [46].

5.4.8 Cookies

A **cookie** is a file placed on your computer's hard drive by a Web server. The file contains information about your visits to a Web site. Cookies can contain login names and passwords, product preferences, and the contents of virtual "shopping carts." Web sites use cookies to provide you with personalized services, such as custom Web pages. Instead of asking you to type in the same information multiple times, a Web site can retrieve that information from a cookie. Most Web sites do not ask for permission before creating a cookie on your hard drive. You can configure your Web browser to alert you when a cookie is being placed on your computer, or you can set your Web browser to refuse to accept any cookies. However, some Web sites cannot be accessed by browsers that block cookies.

5.4.9 Biometrics

Cookies are one way for companies to provide personalized service over the Internet, but they have a weakness. A cookie makes a link between a Web site and a particular computer. If you are the only person using your computer, that's not a problem, but if you share your computer account with others, all the cookies get lumped together. One way to solve this problem is through biometrics. Imagine a mouse with a fingerprint scanner on the side where you place your thumb. Now all your mouse clicks can be tied back to you personally, giving Web sites the ability to do a better job keeping track of your preferences [47].

5.4.10 Spyware

Spyware is a program that communicates over your Internet connection without your knowledge or consent. Spyware programs can monitor Web surfing, log keystrokes, take snapshots of your computer screen, summon pop-up advertisements, and send reports back to a host computer.

Free software downloaded from the Internet often contains spyware. A 2003 survey of 120 U.S. consumers with broadband Internet connections found that 91 percent of them had spyware on their computers [48].

Some ISPs are responding to the outbreak of spyware by releasing tools to help their customers protect their privacy. For example, America Online includes spyware-detecting tools with its software distribution.

5.5 U.S. Legislation

Reflecting public concerns about privacy, Congress has passed numerous laws regulating the collection and distribution of information gathered by private enterprises. We review eight of these laws: the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Family Education Rights and Privacy Act, the Employee Polygraph Protection Act, the Video Privacy Protection Act, the Financial Services Modernization Act, the Children's Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

5.5.1 Fair Credit Reporting Act

Credit bureaus and other consumer reporting agencies maintain information on your bill-paying record, whether you've been sued or arrested, and if you've filed for bankruptcy. They sell reports to other organizations that are trying to determine the creditworthiness of consumers who are applying for credit, applying for a job, or trying to rent an apartment. The Fair Credit Reporting Act, passed in 1970 and revised in 1996, was designed to promote the accuracy and privacy of information used by credit bureaus and other consumer reporting agencies to produce consumer reports. It also ensures that negative information does not haunt a consumer for a lifetime.

The three major credit bureaus are Equifax, Experian, and Trans Union. According to the Fair Credit Reporting Act, these credit bureaus may keep negative information about a consumer for a maximum of seven years. There are several exceptions to this rule. The two most important are that information about criminal convictions may be kept indefinitely, and bankruptcy information may be held for 10 years.

5.5.2 Fair and Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions Act of 2004 requires the three major credit bureaus to provide consumers a free copy of their credit report every 12 months. Consumers can use this opportunity to detect and correct errors in their credit reports. The bureaus do not issue the reports automatically; consumers must take the initiative and request them.

The law also has provisions to reduce identity theft. It requires the truncation of account numbers on credit card receipts, and it establishes the National Fraud Alert System. Victims of identity theft may put a fraud alert on their credit files, warning credit card issuers that they must take "reasonable steps" to verify the requestor's identity before granting credit.

5.5.3 Family Education Rights and Privacy Act

The Family Education Rights and Privacy Act (FERPA) provides students 18 years of age and older the right to review their educational records and to request changes to records that contain erroneous information. Students also have the right to prevent information

in these records from being released without their permission, except under certain circumstances. For students under the age of 18, these rights are held by their parents or guardians. FERPA applies to all educational institutions that receive funds from the U.S. Department of Education; in other words, both public and private schools.

5.5.4 Employee Polygraph Protection Act

The Employee Polygraph Protection Act of 1988 (EPPA) prohibits most private employers from using lie detector tests under most situations. An employer may not require or even request a job applicant or employee to take a lie detector test, and an employee who refuses to take a lie detector test cannot suffer any retaliation.

The Act has several important exceptions. Pharmaceutical companies and security firms may administer polygraph tests to job applicants in certain job categories. Employers who have suffered an economic loss, such as theft, may administer polygraph tests to employees whom they reasonably suspect were involved. Most significantly, EPPA does not apply to federal, state, and local governments.

5.5.5 Video Privacy Protection Act

In 1988 President Ronald Reagan nominated Judge Robert Bork to the U.S. Supreme Court. Bork was a noted conservative, and his nomination was controversial. A Washington, D.C., video store provided a list of Bork's video rental records to a reporter for the *Washington City Paper*, which published the list. While the intention of the paper was most likely to embarrass Bork, it also had the effect of prompting Congress to pass the Video Privacy Protection Act of 1988. According to this law, videotape service providers cannot disclose rental records without the written consent of the customer. In addition, rental stores must destroy personally identifiable information about rentals within a year of the date when this information is no longer needed for the purpose for which it was collected.

5.5.6 Financial Services Modernization Act

The Financial Services Modernization Act (also called the Gramm-Leach-Bliley Act of 1999) contains dozens of provisions related to how financial institutions do business. One of the major provisions of the Act allows the creation of "financial supermarkets" offering banking, insurance, and brokerage services.

The law also contains some privacy-related provisions. It requires financial institutions to disclose their privacy policies to their customers. When a customer establishes an account, and at least once per year thereafter, the institution must let the customer know the kinds of information it collects and how it uses that information. These notices must contain an opt-out clause that explains to customers how they can request that their confidential information not be revealed to other companies. The law requires financial institutions to develop policies that will prevent unauthorized access of their customers' confidential information [49].

5.5.7 Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), which went into effect in 2000, is designed to reduce the amount of public information gathered from children using the Internet. According to COPPA, online services must obtain parental consent before collecting any information from children 12 years old and younger.

5.5.8 Health Insurance Portability and Accountability Act

As part of the Health Insurance Portability and Accountability Act of 1996, Congress directed the Department of Health and Human Services (HHS) to come up with guidelines for protecting the privacy of patients. These guidelines went into effect in April 2003. They limit how doctors, hospitals, pharmacies, and insurance companies can use medical information collected from patients.

The regulations attempt to limit the exchange of information among health care providers to that information necessary to care for the patient. They forbid health care providers from releasing information to life insurance companies, banks, or other businesses without specific signed authorization from the person being treated. Health care providers must provide their patients with a notice describing how they use the information they gather. Patients have the right to see their medical records and to request corrections to errors they find in those records [50].

5.6 Public Records

The federal government maintains thousands of databases containing billions of records about the activities of U.S. citizens. In this section we consider the public-record-keeping activities of the Census Bureau, the Internal Revenue Service, and the FBI, paying particular attention to ways in which information collected for one purpose often has been used for another.

5.6.1 Census Records

In order to ensure each state has fair representation in the House of Representatives, the United States Constitution requires the government to perform a census every 10 years.

The first census of 1790 had six questions. It asked for the name of the head of the household and the number of persons in each of the following categories: free white males at least 16 years old; free white males under 16 years old; free white females; all other free persons (by sex and color); and slaves.

As time passed, the number of questions asked during the census increased. The 1820 census determined the number of people engaged in agriculture, commerce, and manufacturing. The 1840 census had questions regarding school attendance, illiteracy, and occupations. In 1850 census takers began asking questions about taxes, schools, crime, wages, and property values. The 1940 census is notable because for the first time statistical sampling was put to extensive use. A random sample of the population, about

5 percent of those surveyed, received a longer form with more questions. The use of sampling enabled the Census Bureau to produce detailed demographic profiles without substantially increasing the amount of data it needed to process.

According to federal law, the Census Bureau is supposed to keep confidential the information it collects. However, in times of national emergency the Census Bureau has revealed its information to other agencies. During World War I, the Census Bureau provided the names and addresses of young men to the military, which was searching for draft resistors. After the attack on Pearl Harbor, the Census Bureau provided the Justice Department with information from the 1940 census about the general location of Japanese-Americans. The Army used this information to round up Japanese-Americans and send them to internment camps.

5.6.2 Internal Revenue Service Records

The United States enacted a national income tax in 1862 to help pay for expenses related to the Civil War. In 1872 the income tax was repealed. Congress resurrected the national income tax in 1894, but a year later the Supreme Court ruled it unconstitutional. The 16th Amendment to the Constitution, ratified by the states in 1913, gives the United States government the power to collect an income tax. A national income tax has been in place ever since. The Internal Revenue Service (IRS) now collects more than $2 trillion a year in taxes.

Your income tax form may reveal a tremendous amount of personal information about your income, your assets, the organizations to which you give charitable contributions, your medical expenses, and much more. Every year the IRS investigates hundreds of employees for misusing their access to these records. In one notable case, a member of the Ku Klux Klan examined records of fellow Klan members, hoping to identify a suspected undercover agent in his group. The IRS has also misplaced hundreds of tapes and diskettes containing income tax data [51].

In 2003 five consumer protection groups complained to the U.S. Treasury Department that consumers using H&R Block's Web-based Free File tax filing service were being subjected to advertising for tax-related products and home mortgage loans [52]. For example, after a user entered mortgage interest in his tax form, a window popped up with this message:

> We noticed that you entered an itemized deduction for home mortgage interest. By refinancing your mortgage, you may be able to lower your monthly payments or pay off other debts. Now is a great time to take advantage of historically low interest rates. It's easy! Do you want to learn how refinancing your mortgage can help you?

The groups claimed that H&R Block was requiring everyone using its Free File service to consent to cross-marketing, even though that was against the law.

5.6.3 FBI National Crime Information Center 2000

The FBI National Crime Information Center 2000 (NCIC) is a collection of databases supporting the activities of federal, state, and local law-enforcement agencies in the

United States, the United States Virgin Islands, Puerto Rico, and Canada [53]. Its predecessor, the National Crime Information Center, was established by the FBI in January 1967 under the direction of J. Edgar Hoover.

When it was first activated, the NCIC consisted of about 95,000 records in five databases: stolen automobiles, stolen license plates, stolen or missing guns, other stolen items, and missing persons. Today, NCIC databases contain more than 39 million records. The databases have been expanded to include such categories as wanted persons, criminal histories, people incarcerated in federal prisons, convicted sex offenders, unidentified persons, people believed to be a threat to the President, foreign fugitives, violent gang members, and suspected terrorists. More than 80,000 law enforcement agencies have access to these data files. The NCIC processes about five million requests for information each day, with an average response time of less than one second.

The FBI points to the following successes of the NCIC:

- Investigating the assassination of Dr. Martin Luther King, Jr., the NCIC provided the FBI with the information it needed to link a fingerprint on the murder weapon to James Earl Ray.
- In 1992 the NCIC led to the apprehension of 81,750 "wanted" persons, 113,293 arrests, the location of 39,268 missing juveniles and 8,549 missing adults, and the retrieval of 110,681 stolen cars.
- About an hour after the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma state trooper Charles Hanger pulled over a Mercury Marquis with no license plates. Seeing a gun in the back seat of the car, Hanger arrested the driver—Timothy McVeigh—on the charge of transporting a loaded firearm in a motor vehicle. He took McVeigh to the county jail, and the arrest was duly entered into the NCIC database. Two days later, when federal agents ran McVeigh's name through the NCIC, they saw Hanger's arrest record. FBI agents reached the jail just before McVeigh was released. McVeigh was subsequently convicted of the bombing.

Critics of the National Crime Information Center point out ways in which the existence of the NCIC has led to privacy violations of innocent people:

- Erroneous records can lead law enforcement agencies to arrest innocent persons.
- Innocent people have been arrested because their name is the same as someone listed in the arrest warrants database.
- The FBI has used the NCIC to keep records about people not suspected of any crime, such as opponents of the Vietnam War.
- Corrupt employees of law-enforcement organizations with access to the NCIC have sold information to private investigators and altered or deleted records.
- People with access to the NCIC have illegally used it to search for criminal records on acquaintances or to screen potential employees, such as babysitters.

5.6.4 OneDOJ Database

The U.S. Department of Justice is constructing a new database that will give state and local police officers access to information provided by five federal law enforcement agencies: the FBI, the Drug Enforcement Agency, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the U.S. Marshals Service, and the Bureau of Prisons. The database, called OneDOJ, stores incident reports, interrogation summaries, and other information not presently available through the National Crime Information Center. At the end of 2006 the OneDOJ database already contained more than 1 million records.

Critics of the OneDOJ database point out that it will give local police officers access to information about people who have not been arrested or charged with any crime. Barry Steinhardt of the American Civil Liberties Union said, "Raw police files or FBI reports can never be verified and can never be corrected. . . The idea that the whole system is going to be full of inaccurate information is just chilling" [54].

5.6.5 Privacy Act of 1974

In the early 1970s, Elliot Richardson, the Secretary of the U.S. Department of Health, Education, and Welfare, convened a group to recommend policies for the development of government databases that would protect the privacy of American citizens. The Secretary's Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens produced a report for Congress, which included the following "bill of rights" for the Information Age [55]:

CODE OF FAIR INFORMATION PRACTICES

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Interestingly, the Richardson report had a greater impact in Europe than in the United States. Nearly every nation in Europe passed laws based on the Code of Fair Information Practices [56].

The Privacy Act of 1974 represents Congress's codification of these principles. While the Privacy Act does allow individuals in some cases to get access to federal files containing information about them, in other respects it has fallen short of the desires of privacy advocates. In particular, they say the Privacy Act has not been effective in reducing the flow of personal information into governmental databases, preventing agencies from sharing information with each other, or preventing unauthorized access to the data. They claim agencies have been unresponsive to outside attempts to bring them into alignment with the provisions of the Privacy Act. The Privacy Act has the following principal limitations [57]:

1. *The Privacy Act applies only to government databases.*

   Far more information is held in private databases, which are excluded. This is an enormous loophole, because government agencies can purchase information from private organizations that have the data they want.

2. *The Privacy Act only covers records indexed by a personal identifier.*

   Records about individuals that are not indexed by name or another identifying number are excluded. For example, a former IRS agent tried to gain access to a file containing derogatory information about himself, but the judge ruled he did not have a right to see the file, since it was indexed under the name of the IRS investigator, not the IRS agent.

3. *No one in the federal government is in charge of enforcing the provisions of the Privacy Act.*

   Federal agencies have taken it upon themselves to determine which databases they can exempt. The IRS has exempted its database containing the names of taxpayers it is investigating. The Department of Justice has announced that the FBI does not have to ensure the reliability of the data in its NCIC databases.

4. *The Privacy Act allows one agency to share records with another agency as long as they are for a "routine use."*

   Each agency is able to decide for itself what "routine use" means. The Department of Justice has encouraged agencies to define "routine use" as broadly as possible.

5.7 Covert Government Surveillance

Section 5.4 gave a few examples of ways private organizations collect information about individuals. In most cases the goal of the organization's information gathering is to stimulate commerce, and for the most part the individual consumer voluntarily provides the information. Section 5.6 focused on the databases of public records created by the federal government. Some of these records are the result of transactions initiated by individuals, such as filing a tax return. In other cases individuals are required by law to provide the information, such as filling out a census form. Whether people are providing the information willingly or unwillingly, they are aware the government is collecting the data.

In this section we focus on ways in which the United States government has collected information in order to detect and apprehend suspected criminals or to improve national security. Because the individuals being observed are suspected of wrongdoing, they are not alerted or asked for permission before the surveillance begins.

Does covert surveillance violate any of the rights of a citizen? The most relevant statement in the U.S. Constitution is the Fourth Amendment:

FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Before the American Revolution, English agents in pursuit of smugglers made use of *writs of assistance*, which gave them authority to enter any house or building and seize any prohibited goods they could find. This activity drew the ire of the colonists. It is not surprising, then, that a prohibition against unreasonable searches and seizures appears in the Bill of Rights.

The position of the U.S. Supreme Court with respect to covert electronic surveillance has changed over time. Let's see how the Supreme Court's position evolved.

5.7.1 Wiretaps and Bugs

Wiretapping refers to the interception of a telephone conversation. (The term is somewhat anachronistic, because many telephone conversations are no longer transmitted over wires.) Wiretapping has been taking place ever since the 1890s, when telephones became commonly used. In 1892 the State of New York made wiretapping a felony, but the police in New York City ignored the law and continued the practice of wiretapping. Until 1920 the New York City police listened to conversations between lawyers and clients, doctors and patients, and priests and penitents. On several occasions the police even tapped the trunk lines into hotels and listened to the telephone conversations of all the hotel guests [58].

OLMSTEAD V. UNITED STATES

Wiretapping was a popular tool for catching bootleggers during Prohibition (1919–1933). The most famous case involved Roy Olmstead, who ran a $2-million-a-year bootlegging business in Seattle, Washington. Without a warrant, federal agents tapped Olmstead's phone and collected enough evidence to convict him. Although wiretapping was illegal under Washington law, the state court allowed evidence obtained through the wiretapping to be admitted. Olmstead appealed all the way to the U.S. Supreme Court.

His lawyer argued that the police had violated Olmstead's right to privacy by listening in on his telephone conversations. He also argued that the evidence should be thrown out because it was obtained without a search warrant [58, 59].

In a 5-4 decision, the Supreme Court ruled in *Olmstead v. United States* that the Fourth Amendment protected tangible assets alone. The federal agents did not "search" a physical place; they did not "seize" a physical item. Hence the Fourth Amendment's provision against warrantless search and seizure did not apply. Justice Louis Brandeis was one of the four judges siding with Olmstead. In his dissenting opinion, Brandeis argued that the protections afforded by the Bill of Rights ought to extend to electronic communications as well. He wrote:

> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping. [60]

CONGRESS MAKES WIRETAPPING ILLEGAL

The public and the press were critical of the Supreme Court decision. Since the Court had ruled that wiretapping was constitutional, those interested in prohibiting wiretapping focused their efforts on the legislative branch. In 1934 the U.S. Congress passed the Federal Communications Act, which (among other things) made it illegal to intercept and reveal wire communications. Three years later, the Supreme Court used the Federal Communications Act to reverse its position on warrantless wiretaps. In *Nardone v. United States*, the Court ruled that evidence obtained by federal agents from warrantless wiretaps was inadmissible in court. In another decision, *Weiss v. United States*, it ruled that the prohibition on wiretapping applied to intrastate as well as interstate telephone calls. Subsequently, the attorney general announced that the FBI would cease wiretapping [58, 59].

FBI CONTINUES SECRET WIRETAPPING

After World War II broke out in Europe, FBI Director J. Edgar Hoover pressed to have the ban on wiretapping withdrawn (Figure 5.4). The position of the Department of Justice was that the Federal Communications Act simply prohibited intercepting *and* revealing telephone conversations. In the Justice Department's view, it was permissible to intercept conversations as long as they were not revealed to an agency outside the federal government. President Roosevelt agreed to let the FBI resume wiretapping in cases involving national security, though he asked that the wiretaps be kept to a minimum and limited as much as possible to aliens [58].

Because it knew evidence obtained through wiretapping was inadmissible in court, the FBI began maintaining two sets of files: the official files that contained legally obtained evidence, and confidential files containing evidence obtained from wiretaps and

FIGURE 5.4 Under the leadership of J. Edgar Hoover, the FBI engaged in illegal wiretapping. (©Bettmann/CORBIS)

other confidential sources. In case of a trial, only the official file would be released to the court [58].

The FBI was supposed to get permission from the Department of Justice before installing a wiretap, but in practice it did not always work that way. During his 48-year reign as Director of the FBI, J. Edgar Hoover routinely engaged in political surveillance, tapping the telephones of senators, congressmen, and Supreme Court justices. The information the FBI collected on these figures had great political value, even if the recordings revealed no criminal activity. There is evidence Hoover used information gathered during this surveillance to discredit Congressmen who were trying to limit the power of the FBI [58].

CHARLES KATZ V. UNITED STATES

A **bug** is a hidden microphone used for surveillance. In a series of decisions, the U.S. Supreme Court gradually came to an understanding that citizens should also be protected from all electronic surveillance conducted without warrants, including bugs. The key decision was rendered in 1967. Charles Katz used a public telephone to place bets. The FBI placed a bug on the outside of the telephone booth to record Katz's telephone conversations. With this evidence, Katz was convicted of illegal gambling. The Justice Department argued that since it placed the microphone on the outside of the telephone booth, it did not intrude into the space occupied by Katz [58]. In *Charles Katz v. United States*, the Supreme Court ruled in favor of Katz. Justice Stewart Potter wrote that "the Fourth Amendment protects people, not places" [61]. Katz entered the phone booth with the reasonable expectation that his conversation would not be heard, and

what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" [61].

5.7.2 Operation Shamrock

During World War II the U.S. government censored all messages entering and leaving the country, meaning U.S. intelligence agencies had access to all telegram traffic. At the end of the war the censorship bureaucracy was shut down, and the Signal Security Agency (predecessor to the National Security Agency) wanted to find a new way to get access to telegram traffic. It contacted Western Union Telegraph Company, ITT Communications, and RCA Communications, and asked them to allow it to make photographic copies of all foreign government telegram traffic that entered, left, or transited the United States. In other words, the Signal Security Agency asked these companies to break federal law in the interests of national security. All three companies agreed to the request. The Signal Security Agency gave this intelligence-gathering operation the name "Shamrock."

When the National Security Agency (NSA) was formed in 1952, it inherited Operation Shamrock. The sophistication of the surveillance operation took a giant leap forward in the 1960s, when the telegram companies converted to computers. Now the contents of telegrams could be transmitted electronically to the NSA, and the NSA could use computers to search for key words and phrases.

In 1961 Robert Kennedy became the new attorney general of the United States, and he immediately focused his attention on organized crime. Discovering that information about mobsters was scattered piecemeal among the FBI, IRS, Securities and Exchange Commission (SEC), and other agencies, he convened a meeting in which investigators from all of these agencies could exchange information. The Justice Department gave the names of hundreds of alleged crime figures to the NSA, asking that these figures be put on its "watch list." Intelligence gathered by the NSA contributed to several prosecutions.

Also during the Kennedy administration, the FBI asked the NSA to put on its watch list the names of U.S. citizens and companies doing business with Cuba. The NSA sent information gathered from intercepted telegrams and international telephone calls back to the FBI.

During the Vietnam War the Johnson and Nixon administrations hypothesized that foreign governments were controlling or influencing the activities of American groups opposed to the war. They asked the NSA to put the names of war protesters on its watch list. Some of the people placed on the watch list included the Reverend Dr. Martin Luther King, Jr., the Reverend Ralph Abernathy, Black Panther leader Eldrige Cleaver, Dr. Benjamin Spock, Joan Baez, and Jane Fonda.

In 1969 President Nixon established the White House Task Force on Heroin Suppression. The NSA soon became an active participant in the war on drugs, monitoring the phone calls of people put on its drug watch list. Intelligence gathered by the NSA led to convictions for drug-related crimes.

Facing hostile Congressional and press scrutiny, the NSA called an end to Operation Shamrock in May 1975 [62].

5.7.3 Carnivore Surveillance System

The FBI developed the Carnivore system in the late 1990s to monitor Internet traffic, including email messages. The system itself consisted of a Windows PC and packet-sniffing software capable of identifying and recording packets originating from or directed to a particular IP address. Armed with a search warrant, the FBI would set up its Carnivore system at the suspect's Internet service provider [63].

In 2000 the Justice Department demanded that Earthlink, an Internet service provider, allow the FBI to use Carnivore without a warrant. Earthlink filed a legal challenge questioning the FBI's authority to do this under the Electronic Communications Privacy Act, but a U.S. District Court ruled against Earthlink [64, 65].

Between 1998 and 2000 the FBI used the Carnivore system about 25 times. In late 2001 the FBI stopped using Carnivore, replacing it with commercial software capable of performing the same function [66].

5.7.4 Covert Activities after 9/11

The September 11, 2001, attacks on the World Trade Center and the Pentagon spawned new, secret intelligence-gathering operations within the United States. The same question emerged after each activity became public knowledge: Is it constitutional?

NSA WIRETAPPING

Early in 2002 the Central Intelligence Agency captured several top al-Qaeda members, along with their personal computers and cell phones. The CIA recovered telephone numbers from these devices and provided them to the NSA. The NSA was eager to eavesdrop on these telephone numbers, hoping to gather information that could be used to disrupt future terrorist attacks. President Bush signed a presidential order allowing the NSA to eavesdrop on international telephone calls and international emails initiated by people living inside the United States, without first obtaining a search warrant [67].

The list of persons being monitored gradually expanded, as the NSA followed connections from the original list of telephone numbers. At any one time, the NSA eavesdropped on up to 500 people inside the United States, including American citizens, permanent residents, and foreigners. The NSA also monitored another 5,000 to 7,000 people living outside the United States at any one time [67].

Sources told *The New York Times* that the surveillance program had foiled at least two al-Qaeda plots: Ohio truck driver Iyman Faris's plan to "bring down the Brooklyn Bridge with blowtorches" and another scheme to bomb British pubs and train stations. Civil libertarians and some members of Congress objected to the program, arguing that warrantless wiretapping of American citizens violated the Fourth Amendment to the U.S. Constitution [67].

TALON DATABASE

In 2003 the U.S. Department of Defense created the Threat and Local Observation Notices (TALON) database. The purpose of the database was to collect reports of suspicious

activities or terrorist threats near military bases. These reports were submitted by military personnel or civilians and then assessed by Department of Defense experts as either "credible" or "not credible."

In December 2005 NBC News reported that the database contained reports on antiwar protests occurring far from military bases [68]. In July 2006 the Servicemembers Legal Defense Network reported that the TALON database contained emails from students at Southern Connecticut State University, the State University of New York at Albany, the University of California at Berkeley, and William Paterson University of New Jersey who were planning protests against on-campus military recruiting [71].

The Department of Defense removed many of these reports from TALON after conducting an in-house review that concluded the database should only contain information related to terrorist activity. The American Civil Liberties Union asked Congress to take steps "to ensure that Americans may once again exercise their First Amendment rights without fear that they will be tracked in a government database of suspicious activities" [69]. In April 2007 the new Under Secretary of Defense for Intelligence recommended that the TALON program be terminated [70].

5.8 U.S. Legislation Authorizing Wiretapping

As we have seen, the Federal Communications Act of 1934 made wiretapping illegal, and by 1967 the U.S. Supreme Court had closed the door to wiretapping and bugging performed without a warrant (court order). After the Katz decision, police were left without any electronic surveillance tools in their fight against crime.

Meanwhile, the United States was in the middle of the Vietnam War. In 1968 the country was rocked by violent antiwar demonstrations and the assassinations of Martin Luther King, Jr., and Robert F. Kennedy. Law-enforcement agencies pressured Congress to allow wiretapping under some circumstances.

5.8.1 Title III

Congress responded by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III allows a police agency that has obtained a court order to tap a phone for up to 30 days [58].

The government continued to argue that in cases of national security, agencies should be able to tap phones without a warrant. In 1972 the Supreme Court rejected this argument when it ruled that the Fourth Amendment forbids warrantless wiretapping, even in cases of national security [58].

5.8.2 Electronic Communications Privacy Act

Congress updated the wiretapping law in 1986 with the passage of the Electronic Communications Privacy Act (ECPA). The ECPA allows police to attach two kinds of surveillance devices to a suspect's phone line. If the suspect makes a phone call, a **pen register** displays the number being dialed. If the suspect gets a phone call, a **trap-and-trace device**

displays the caller's phone number. While a court order is needed to approve the installation of pen registers and trap-and-trace devices, prosecutors do not need to demonstrate probable cause, and the approval is virtually automatic.

The ECPA also allows police to conduct **roving wiretaps**—wiretaps that move from phone to phone—if they can demonstrate the suspect is attempting to avoid surveillance by using many different phones [58].

5.8.3 Communications Assistance for Law Enforcement Act

The implementation of digital phone networks interfered with the wiretapping ability of the FBI and other organizations. In response to these technological changes, Congress passed the Communications Assistance for Law Enforcement Act of 1994 (CALEA), also known as the Digital Telephony Act. This law required networking equipment used by phone companies be designed or modified so that law-enforcement agencies can trace calls, listen in on telephone calls, and intercept email messages. CALEA thereby ensured that court-ordered wiretapping would still be possible even as new digital technologies were introduced.

CALEA left unanswered many important details about the kind of information the FBI would be able to extract from digital phone calls. The precise requirements were to be worked out between the FBI and industry representatives. The FBI asked for many capabilities, including the ability to intercept digits typed by the caller after the phone call was placed. This feature would let it catch credit card numbers and bank account numbers, for example. In 1999 the FCC finally issued the guidelines, which included this capability and five more requested by the FBI [72]. Privacy-rights organizations argued these capabilities went beyond the authorization of CALEA [73]. Telecommunications companies claimed that implementing these capabilities would cost them billions [74]. Nevertheless, in August 2005 the FCC gave voice over Internet Protocol (VoIP) and certain other broadband providers 18 months to modify their systems as necessary so that law enforcement agencies could wiretap calls made using their services [75].

5.8.4 USA PATRIOT Act

BACKGROUND

On the morning of September 11, 2001, terrorists hijacked four passenger airliners in the United States and turned them into flying bombs. Two of the planes flew into New York's World Trade Center, a third hit the Pentagon, and the fourth crashed in a field in Pennsylvania. Soon after these attacks, which resulted in about 3,000 deaths and the destruction of the twin towers of the World Trade Center, the United States Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, henceforth referred to as the Patriot Act [76].

PROVISIONS OF THE PATRIOT ACT

The Patriot Act amended many existing laws. Its provisions fall into four principal categories:

1. Providing federal law enforcement and intelligence officials with greater authority to monitor communications;
2. Giving the Secretary of the Treasury greater powers to regulate banks, preventing them from being used to launder foreign money;
3. Making it more difficult for terrorists to enter the United States; and
4. Defining new crimes and penalties for terrorist activity.

We focus on those provisions of the Patriot Act that most directly affect the privacy of persons living inside the United States.

The Patriot Act expands the kinds of information that law enforcement officials can gather with pen registers and trap-and-trace devices. It allows police to use pen registers on the Internet to track email addresses and URLs. The law does not require they demonstrate probable cause. To obtain a warrant, police simply certify that the information to be gained is relevant to an ongoing criminal investigation.

Law enforcement agencies seeking to install a wiretap or a pen register/trap-and-trace device have always been required to get a court order from a judge with jurisdiction over the location where the device was to be installed. The Patriot Act extends the jurisdiction of court-ordered wiretaps to the entire country. A judge in New York can authorize the installation of a device in California, for example. The act also allows the nationwide application of court-ordered search warrants for terrorist-related investigations.

The Patriot Act broadened the number of circumstances under which roving surveillance can take place. Previously, roving surveillance could only be done for the purpose of law enforcement, and the agency had to demonstrate to the court that the person under investigation actually used the device to be monitored. The Patriot Act allows roving surveillance to be performed for the purpose of intelligence, and the government does not have to prove that the person under investigation actually uses the device to be tapped. Additionally, it does not require that the law enforcement agency report back to the authorizing judge regarding the number of devices monitored and the results of the monitoring.

Under the Patriot Act, law enforcement officials wishing to intercept communications to and from a person who has illegally gained access to a computer system do not need a court order if they have the permission of the owner of the computer system.

The Patriot Act allows courts to authorize law enforcement officers to search a person's premises without first serving a search warrant when there is "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse affect." Officers may seize property that "constitutes evidence of a criminal offense in violation of the laws of the United States," even if that offense is unrelated to terrorism.

The Patriot Act makes it easier for the FBI to collect business, medical, educational, library, and church/mosque/synagogue records. To obtain a search warrant authorizing the collection of these records, the FBI merely needs to state that the records are related to an ongoing investigation. There is no need for the FBI to show probable cause. It is

illegal for anyone supplying records to the FBI to reveal the existence of the warrant or tell anyone that they provided information to the government. The act does specifically prohibit the FBI from investigating citizens solely on the basis of activities protected by the First Amendment.

RESPONSES TO THE PATRIOT ACT

More than a hundred cities and several states have passed anti–Patriot Act resolutions [77]. Critics of the Patriot Act warn that its provisions give too many powers to the federal government. Despite language in the Patriot Act to the contrary, civil libertarians are concerned that law enforcement agencies may use their new powers to reduce the rights of law-abiding Americans, particularly those expressed in the First and Fourth Amendments to the United States Constitution.

We have seen that in the past, the FBI and the NSA used illegal wiretaps to investigate people who had expressed unpopular political views. Congressional investigations led to the termination of Operation Shamrock. Over time, however, Congress has gradually increased the surveillance options available to the police. By making court orders for various kinds of electronic surveillance easy to obtain, the Patriot Act is another step in this direction. If people know how easy it is for law enforcement personnel to monitor their activities, they may be less inclined to exercise their First Amendment rights. For example, knowledge that the Patriot Act allows the FBI to collect records from libraries and bookstores may make people less inclined to read certain books. In November 2003 the American Civil Liberties Union reported that public apprehension about the Patriot Act has led to a significant drop in attendance and donations at mosques [78].

Critics of the Patriot Act are also concerned that some of its provisions undermine rights guaranteed citizens under the Fourth Amendment to the Constitution:

- By revealing the URLs of Web sites visited by a suspect, a pen register is a much more powerful surveillance tool on the Internet than it is on a telephone network. The Patriot Act allows police to install Internet pen registers without demonstrating probable cause that the suspect is engaged in a criminal activity.
- Court orders authorizing roving surveillance do not "particularly describe the place to be searched."
- It allows law enforcement agencies, under certain circumstances, to search homes and seize evidence without first serving a search warrant.
- It allows the FBI to obtain—without showing probable cause—a warrant authorizing the seizure of business, medical, educational, and library records of suspects.

The Council of the American Library Association passed a resolution on the Patriot Act in January 2003. The resolution affirms every person's rights to inquiry and free expression. It "urges librarians everywhere to defend and support user privacy and free and open access to knowledge and information," and it "urges libraries to adopt and implement patron privacy and record retention policies" that minimize the collection of records about the activities of individual patrons [79].

FOLLOW-ON LEGISLATION

In February 2003 a draft copy of the Domestic Security Enhancement Act of 2003 was leaked to the press. The bill, dubbed "Patriot Act II," would have given the U.S. government sweeping new powers. Here are some of the provisions of the act:

- The government would have the ability to expatriate an American citizen "convicted of giving material support to a group that's designated a terrorist organization" [80].
- It would require the names of people being held on suspicion of terrorism to be kept secret.
- Law enforcement officials would be able to use administrative subpoenas to gain access to records held by ISPs, doctors, family members, or friends. An administrative subpoena does not require the approval of a judge unless the person being served the subpoena raises an objection.
- The act would make it simpler for police to gain access to credit reports.
- Police would have the right to collect DNA samples from suspected terrorists. The federal government would create a national DNA database. Federal, state, and local law enforcement agencies would be able to access the national database.
- Police would have the right to wiretap suspects and intercept their email for 15 days without obtaining a warrant.

Unlike the original Patriot Act, which passed Congress with little debate, many voices were raised against the follow-on bill. Congress adjourned at the end of 2003 without passing the Domestic Security Enhancement Act.

SUCCESSES AND FAILURES

According to Tom Ridge, former Secretary of the Department of Homeland Security, the Patriot Act has helped the government in its fight against terrorism by allowing greater information-sharing among law enforcement and intelligence agencies, and by giving law enforcement agencies new investigative tools—"many of which have been used for years to catch mafia dons and drug kingpins" [81]. Terrorism investigations have led to charges being brought against 361 individuals in the United States. Of these, 191 have been convicted or pled guilty, including shoe-bomber Richard Reid, and John Walker Lindh, who fought with the Taliban in Afghanistan. More than 500 individuals linked to the September 11th attacks have been removed from the United States. Terrorist cells in Buffalo, Seattle, Tampa, and Portland (the "Portland Seven")[2] have been broken up [81].

Unfortunately, a few innocent bystanders have been affected by the war against terrorism. A notable example is Brandon Mayfield.

During the morning rush hour on March 11, 2004, ten bombs exploded on four commuter trains in Madrid, Spain, killing 191 people and wounding more than 2,000

2. The "Portland Seven" included six American Muslim men accused of attempting to travel to Afghanistan to fight with the Taliban.

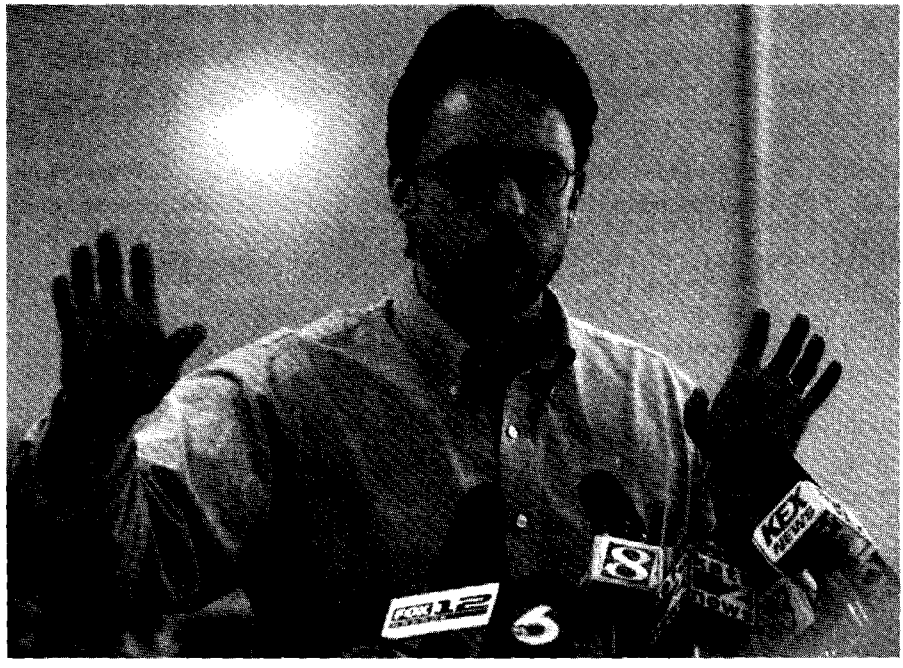


FIGURE 5.5 Brandon Mayfield, an Oregon lawyer, was falsely accused of participating in the terrorist bombing of four commuter trains in Madrid, Spain. (© Greg Wahl-Stephens/Getty Images)

others. The Spanish government retrieved a partial fingerprint from a bag of detonators, and the FBI linked the fingerprint to Brandon Mayfield, an attorney in Portland, Oregon (Figure 5.5) [82].

Without revealing their search warrant, FBI agents secretly entered Mayfield's home multiple times, making copies of documents and computer hard drives, collecting ten DNA samples, removing six cigarette butts for DNA analysis, and taking 355 digital photographs. The FBI also put Mayfield under electronic surveillance [83]. On May 6, 2004, the FBI arrested Mayfield as a material witness and detained him for two weeks. After the Spanish government announced that it had matched the fingerprints to Ouhnane Daoud, an Algerian national living in Spain, a judge ordered that Mayfield be released. The FBI publicly apologized for the fingerprint misidentification [82].

Mayfield said his detention was "an abuse of the judicial process" that "shouldn't happen to anybody" [82]. He said, "I personally was subject to lockdown, strip searches, sleep deprivation, unsanitary living conditions, shackles and chains, threats, physical pain, and humiliation" [84]. The only evidence against Mayfield was a partial fingerprint match that even the Spanish police found dubious. Mayfield had not left the United States in more than a decade, and he had no connections with any terrorist organizations. Some civil rights groups suggest Mayfield was targeted by the FBI because of his

religious beliefs. The affidavit that the FBI used to get an arrest warrant pointed out that Mayfield "had converted to Islam, is married to an Egyptian-born woman, and had once briefly represented a member of the Portland Seven in a child-custody case" [85]. Mayfield sued the U.S. government for continuing to investigate him after the Spanish police had eliminated him as a suspect, and in November 2006 the government issued a formal apology and agreed to pay him $2 million [84].

PATRIOT ACT RENEWAL

In 2006 President Bush signed into law a renewal of the Patriot Act that made most of its provisions permanent. Congress put a four-year sunset clause on two controversial provisions: one allowing roving wiretaps associated with a person rather than a particular phone number, and the other allowing the FBI to seize records from financial institutions, libraries, doctors, and businesses with approval from the secret Foreign Intelligence Surveillance Court [86].

5.9 Data Mining

Data mining is the process of searching through one or more databases looking for patterns or relationships. Data mining is a way to generate new information by combining facts found in multiple transactions. It can also be a way to predict future events.

A record in a database records a single transaction, such as a particular purchase at a store. You can think of a database record as being a single snapshot of a person. It tells you something about the person, but in isolation its value is limited. By drawing upon large numbers of records, data mining allows an organization to build an accurate profile of an individual from a myriad of snapshots.

The first time you rent a movie from a video rental store, it takes a long time. You have to fill out an application asking for a lot of personal information, such as your name, address, and phone number. After the store has approved your application, renting movies is quick. You identify yourself to the clerk, and he accesses your file on the computer. The clerk scans your choices, takes your money, and you are on your way. The primary use of the information you provided was to allow you to rent movies from this particular video store.

Frequently, however, information is put to another purpose. This is called a **secondary use** of your data. Companies can look through a series of transactions in order to create more personal relationships with their customers [87]. For example, **collaborative filtering** algorithms draw upon information about the preferences of a large number of people to predict what an individual may enjoy. An organization performing collaborative filtering may determine people's preferences explicitly, through rankings, or implicitly, by tracking their purchases. The filtering algorithm looks for patterns in the data. Perhaps many people who purchase item X also purchase item Y. If a new customer selects X or Y, the collaborative filtering software will suggest the customer may also like the other item. Collaborative filtering software is used by online retailers and DVD-rental sites to make recommendations [88].

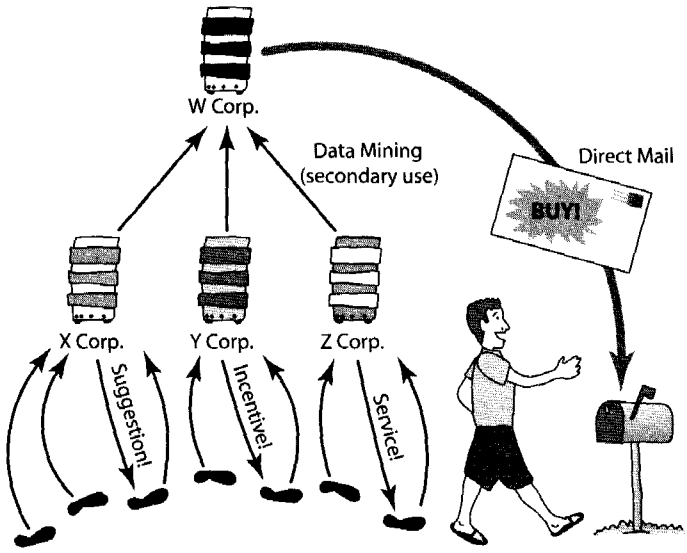


FIGURE 5.6 Companies use computers to record information about their customers and their buying habits. They analyze this information to suggest additional purchases, provide incentives, and deliver better service. They may also sell this information to other companies. By combining information from various sources, a company can build sophisticated profiles of individuals and target its direct mail advertising to those people most likely to be interested in its products.

Information about customers has itself become a commodity. Organizations sell or exchange information with other organizations (Figure 5.6). This is another secondary use of data, and it is a common way for organizations to gather large databases of information they can mine.

For example, a company selling time-share condominiums purchases from a hotel chain the names and addresses of people who have vacationed in a resort area in the past two years. From another organization it purchases a database that gives the approximate annual household income of a family, based on that family's nine-digit ZIP code. Combining these lists allows the time-share agency to target people most likely to have both the interest and the financial resources to purchase a share of a vacation condominium. It uses direct mail to send brochures to these people.

Data mining can be surprisingly powerful. Suppose a government agency managing tollbooths sells information records of the form

⟨transponder number⟩ ⟨date⟩ ⟨time⟩ ⟨location⟩ ⟨charge⟩

The agency does not reveal the names of the owners of the cars, so it believes it is protecting their anonymity. However, many people have an account set up so that their tollbooth payments are automatically charged to their credit cards. If a credit card company buys these records from the tollbooth agency, it can match the date, time, and

amount of the tollbooth payments with the date, time, and charge on its credit cards to determine the identity of the person driving a vehicle with a particular transponder number. Once this has been done, the credit card company can figure out which customers are driving the most miles and are likely to purchase new cars more frequently. It can then sell this information to banks interested in soliciting automobile loan applications [37].

Advances in information technology have led to a drop in the cost of acquiring information. Meanwhile, the value of information continues to rise, as organizations refine their data mining techniques. The result of these trends is that organizations have increased incentives to acquire information, making it more difficult for individuals to protect their privacy [24]. Still, people can and do fight back when they feel an organization has gone too far. A case in point is Lotus Development's failure with its Marketplace: Households project.

5.9.1 Marketplace: Households

Lotus Development Corporation spent $8 million developing a CD with information on 120 million people, along with software that would help the purchaser produce mailing lists based on various criteria, such as household income. Lotus hoped to sell the CD, which it called "Marketplace: Households," to small businesses. When consumers found out about the CD, they complained loudly and vigorously, with more than 30,000 letters, phone calls, and emails. Lotus dropped plans to sell the CD [89].

5.9.2 IRS Audits

To identify taxpayers who have paid less than they owe, the IRS uses computer matching and data mining strategies. First, it matches information on the tax form with information provided by employers and financial institutions. This is a straightforward way to detect unreported income.

Second, the IRS audits a couple of million tax returns every year. Its goal is to select the most promising returns—those containing errors resulting in underpayment of taxes. The IRS uses a computerized system called the discriminant function (DIF) to score every tax return. The DIF score is an indicator of how many irregularities there are on a tax form, compared to carefully constructed profiles of correct tax returns. About 60 percent of tax returns audited by the IRS are selected due to their high DIF scores.

5.9.3 Syndromic Surveillance System

Another application of data mining by the government is protecting society from imminent dangers.

New York City has created the Syndromic Surveillance System, which analyzes more than 50,000 pieces of information every day, including 911 calls, visits to emergency rooms, and purchases of prescription drugs. The purpose of the system is to find patterns that might indicate the onset of an epidemic, an environmental problem leading to illnesses, or bioterrorism. In the fall of 2002, the system detected a surge in people

seeking treatment for vomiting and diarrhea. These symptoms were the first signs of an outbreak of a Norwalk-type virus. The alert generated by the system allowed city officials to warn doctors about the outbreak and advise them to be particularly careful about handling the highly contagious body fluids of their affected patients [90].

5.9.4 Telecommunications Records Database

Shortly after September 11, several major telecommunications providers began providing the phone call records of tens of millions of Americans to the National Security Agency, without a court order. The NSA was not monitoring or recording the actual conversations; instead, it was analyzing calling patterns in order to detect potential terrorist networks. [91].

After *USA Today* revealed the existence of the database in May 2006, more than a dozen class-action lawsuits were filed against the telecommunications companies. In August 2006 a federal judge in Detroit ruled the program to be illegal and unconstitutional, violating several statutes as well as the First and Fourth Amendments to the U.S. Constitution [92]. In July 2007 the U.S. Court of Appeals for the Sixth Circuit overturned the ruling on the grounds that the plaintiffs did not have standing to bring the suit forward. In other words, the plaintiffs had not produced any evidence that they personally were victims of warrantless wiretapping.

5.9.5 Total Information Awareness

The Total Information Awareness (TIA) project, proposed by the Information Awareness Office of the U.S. Defense Advanced Research Projects Agency, is an example of data mining taken to a high level. The idea of the project is to detect potential terrorists by capturing everyone's "information signature" and using sophisticated computer algorithms to detect terrorist-like patterns of activity. TIA databases would contain financial, medical, communication, travel, and other records. The use of biometric technology to identify people from video images would allow TIA databases to incorporate person/location/time information as well [93].

The Total Information Awareness program received a skeptical reception from the U.S. Congress. In February 2003 Congress suspended funding for the domestic surveillance portion of the program [94]. Subsequently, DARPA changed the name of the program to Terrorist Information Awareness [95].

5.9.6 Criticisms of the TIA Program

In an open letter to John Warner and Carl Levin, ranking members of the Senate Committee on Armed Services, a group of computer scientists voiced objections to the Total Information Awareness program [96]. The letter, written on behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (ACM), agrees with the notion that advances in information technology can contribute to public safety and national defense. However, the letter suggests that the Total Information Awareness program will have more harms than benefits.

The all-encompassing databases suggested by the TIA program would represent large security and privacy risks. They would contain a great deal of sensitive (and valuable) information about individuals. Hence the databases themselves would become targets for criminals and terrorists. In addition, tens of thousands of system administrators, law enforcement people, and intelligence officers would have access to the data, creating many opportunities for the security of the database to be compromised.

These databases would increase the risk of identity theft by putting in a single place a host of personal information. If terrorists could get access to the data, it would be easier for them to assume false identities.

Because the information in the TIA databases was secret, citizens would not have the ability to verify that the information stored about them is correct.

The TIA program may hurt the competitiveness of U.S. companies in the worldwide e-commerce. Non-Americans who do not wish their consumer profiles to become part of a TIA database may choose to purchase their goods from non-U.S. sources.

Identity theft is a growing problem. Transactions performed by people who have stolen the identities of others will introduce "noise" into the TIA database, giving a false impression of the activities of the actual person.

The goal of the TIA program is to identify patterns of behavior that indicate a person is a terrorist. It is inevitable that such a system will generate some "false positives"—labeling innocent persons as potential terrorists. Even a 99 percent accuracy rate could result in millions of Americans being incorrectly identified.

Finally, knowing about the existence of TIA will modify people's behavior. Terrorists will do everything possible to make sure their behavior looks "normal." Innocent people may avoid certain activities, even though they are legal, out of fear of being targeted by the system.

5.9.7 Who Should Own Information about a Transaction?

Does a person buying a product or service have the right to control information about the transaction? Does the seller have this right? Consider the following hypothetical example.

Dr. Knowitall, a computer science professor, takes his broken computer to the Computer Shop so that 18-year-old Andy can fix it for him. Dr. Knowitall is embarrassed that he can't fix the computer himself, and he doesn't want anybody to find out that he must pay someone to fix it. Dr. Knowitall certainly isn't going to tell anyone, but does he have the right to prevent Andy from telling anyone? Or maybe Andy wants to keep the transaction a secret, because he's embarrassed it took him so long to fix the computer and he doesn't want anyone to find out he was in over his head. Does Andy have the right to keep Dr. Knowitall from talking about it?

It seems that neither person can claim the right to control information about this transaction. Since information about the transaction becomes public information if either party discloses it, keeping the transaction private is more difficult (hence more valuable) than making it public.

If Dr. Knowitall wants to keep the transaction private, he should be willing to pay for it. He may tell Andy, "I'll give you an extra 20 bucks if you promise you won't tell anybody that you fixed my computer." At this point Dr. Knowitall has purchased control over the information about this transaction. Andy is obliged to keep his mouth shut, not because of Dr. Knowitall's right to privacy, but because of his right to expect the agreement will be upheld.

5.9.8 Opt-in Versus Opt-out

What rules should govern the secondary use of information collected by organizations selling products or services? Two fundamentally different policies are called opt-in and opt-out.

The **opt-in** policy requires the consumer to explicitly give permission for the organization to share the information with another organization. Opt-in policies are preferred by privacy advocates.

The **opt-out** policy requires the consumer to explicitly forbid an organization from sharing information with other organizations. Direct marketing associations prefer the opt-out policy, because opt-in is a barrier for new businesses. New businesses do not have the resources to go out and collect all the information they need to target their mailings to the correct individuals. In an opt-out environment, most people will not go through the effort required to actually remove themselves from mailing lists. Hence it is easier for new businesses to get access to the mailing lists they need to succeed [97]. Another argument for opt-out is that companies have the right to control information about the transactions they have made. Information is a valuable commodity. An opt-in policy takes this commodity away from companies.

Some have suggested that the relationship between a consumer and a company is similar to the relationship between a patient and a doctor. A doctor is not supposed to reveal information about her patients. So-called **Hippocratic databases** contain rules about who should have access to the data and how long it should be stored. When users of a Hippocratic database enter information, they can see this information about the use and duration of the data and decide whether or not to actually submit the information [98].

5.9.9 Platform for Privacy Preferences (P3P)

The World Wide Web Consortium has developed an industry standard called Platform for Privacy Preferences (P3P) Project (www.w3.org/P3P). The goal of this project is to provide users with an automated way to control the use of personal information on the Web sites they visit. Participating sites disclose their privacy policies in a machine-readable format. The user's browser can compare these policies with the user's preferences. The user can then decide whether to visit the site.

Critics of P3P point out the P3P is a voluntary standard. Web sites are not required to disclose their privacy policies in a P3P-compatible format. Even worse, P3P cannot monitor whether a site is actually abiding by its stated policy.

5.10 Identity Theft

5.10.1 Background

Dorothy Denning defines **identity theft** as "the misuse of another person's identity, such as name, Social Security number, driver's license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, get access to information, or issue documents and letters under the victim's identity" [99].

The leading form of identity theft in United States is credit card fraud. Identity thieves either take out a new credit card in someone else's name or commandeer an existing account [100]. By changing the billing address of existing accounts, a thief can run up large debts before the victim becomes aware of the problem. These activities can blemish the target's credit history. As a result, victims of identity theft may have applications for credit cards, mortgage loans, and even employment denied. If the impostor shows false credentials to the police, the victim may even be saddled with a false criminal record or outstanding arrest warrants.

Financial institutions contribute to the problem of identity theft by making it easy for people to open up new accounts. Since information brokers on the Web are selling driver's license numbers, Social Security numbers, and credit card information, it's easy for an identity thief to gather a great deal of information about another person. Assuming another person's identity is made simpler by banks allowing people to open accounts online [101].

According to Privacy Rights Clearinghouse, about 37 million Americans were victims of identity theft between 2003 and 2007. The frequency of identity theft is decreasing; there were 10.1 million identity theft victims in 2003 and 8.4 million identity theft victims in 2007. The average loss in 2004 was $5,720 per victim in 2007 [102].

Fortunately, United States law says that a consumer's liability for losses due to credit card fraud are limited to $50 if reported promptly. Many financial institutions do not even collect this amount [103]. However, victims of identity theft typically spend hundreds of hours cleaning up their financial records [102].

Most cases of identity theft are not the result of someone using computers to break into a database containing information about a target. Instead, identity thieves are much more likely to use low-tech methods to gain access to the personal information they need. Two popular sources of information are mailboxes and lost or stolen wallets. One in six cases of identity theft are traced to family members, friends, or coworkers [102].

Some identity thieves engage in **dumpster diving**—looking for personal information in garbage cans or recycling bins. Old bills, bank statements, and credit card statements contain a wealth of personal information, including names, addresses, and account numbers. Another simple way to get information is through **shoulder surfing**—looking over the shoulders of people filling out forms.

Skimmers (**wedges**) are another way thieves steal credit card data. A skimmer is a small, battery-powered credit card reader. Identity theft rings use skimmers to collect hundreds of credit card numbers, then use these numbers to manufacture counterfeit

credit cards. Credit card numbers are collected by waiters or store clerks, who match each legal swipe through a cash register with an illegal swipe through a skimmer. In one case, someone attached a skimmer to an ATM along with a sign requesting customers to use the "card cleaner" before putting their card in the ATM [104].

Some thieves send out spam messages designed to look like they originated from PayPal, eBay, or another well-known Internet-active business. Through these messages they hope to con unsuspecting recipients into revealing their credit card numbers or other personal information. Gathering financial information via spam is called **phishing** (pronounced "fishing").

Pharming (pronounced "farming") is the creation of an authentic-looking Web site with the intention of fooling people into revealing personal information. Identity thieves often link phishing and pharming. For example, a victim might receive an email message purportedly from PayPal, asking the person to go to the PayPal Web site to confirm a transaction. The email message contains a hypertext link. When the victim clicks on the link, he is connected to the counterfeit PayPal site.

Large institutions that store personal data are tempting targets for information thieves. Between 2003 and 2005 criminals used stolen passwords to access LexisNexis databases 59 times, retrieving the Social Security numbers and other financial information of more than 300,000 people [105]. ChoicePoint disclosed that it accidentally gave con artists access to about 150,000 personal financial dossiers, and Bank of America lost computer tapes containing information about more than a million federal employees [106]. A hacker broke into a T-Mobile database and downloaded the photographs and personal information of at least 400 customers [106].

The Identity Theft and Assumption Act of 1998 makes identity theft a federal crime. In 2004 Congress passed the Identity Theft Penalty Enhancement Act, which lengthened prison sentences for identity thieves [107]. A variety of law enforcement agencies investigate alleged violations of this law: the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Office of the Inspector General of the Social Security Administration [108]. Unfortunately, the probability that a particular case of identity theft will result in an arrest is about 1 in 700 [109].

The rapid increase in the number of identity theft victims is prompting new questions about how people identify themselves. In the United States, the Social Security number is a common form of identification, even though that was not how it was originally conceived.

5.10.2 History and Role of the Social Security Number

The Social Security Act of 1935 established two social insurance programs in the United States: a federal system of old-age benefits to retired persons, and a federal-state system of unemployment insurance. Before the system could be implemented, employers and workers needed to become registered. The Social Security Board contracted with the U.S. Postal Service to distribute applications for Social Security cards. The post office collected the forms, typed the Social Security cards, and returned them to the applicants. In this way, over 35 million Social Security cards were issued in 1936–1937 [110].

The U.S. government initially stated that Social Security numbers (SSNs) would be used solely by the Social Security Administration, and not as a national identification card. In fact, from 1946 to 1972, the Social Security Administration put the following legend on the bottom of the cards it issued: "FOR SOCIAL SECURITY PURPOSES—NOT FOR IDENTIFICATION." However, use of the SSN has gradually increased. President Roosevelt ordered in 1943 that federal agencies use SSNs as identifiers in new federal databases. In 1961 the Internal Revenue Service began using the SSN as the taxpayer identification number. Because banks report interest to the IRS, people must provide their SSN when they open a bank account. The SSN is typically requested on applications for credit cards. Motor vehicle departments and some other state agencies received permission to use SSNs as identification numbers in 1976. Many universities use the SSN as an identification number for faculty and students. The IRS now requires parents to provide the SSNs of their children over one year old on income tax forms in order to claim them as dependents. For this reason, children now get a SSN soon after they are born. Many private organizations ask people to provide SSNs for identification. The SSN has become a de facto national identification number in the United States.

Unfortunately, the SSN has serious defects that make it a poor identification number. The first problem with SSNs is that they are not unique. When Social Security cards were first issued by post offices, different post offices accidentally assigned the same SSN to different people. In 1938 wallet manufacturer E. H. Ferree included sample Social Security cards in one of its products. More than 40,000 people purchasing the wallets from Woolworth stores thought the cards were real and used the sample card's number as their SSN [111].

A second defect of SSNs is that they are rarely checked. Millions of Social Security cards have been issued to applicants without verifying that the information provided by the applicants is correct. Many, if not most, organizations asking for a SSN do not actually require the applicant to show a card, making it easy for criminals to supply fake SSNs.

A third defect of SSNs is that they have no error-detecting capability, such as a check digit at the end of the number. A check digit enables computer systems to detect common data entry errors, such as getting one digit wrong or transposing two adjacent digits. If someone makes one of these mistakes, the data-entry program can detect the error and ask the person to retype the number. In the case of SSNs, if a person accidentally types in the wrong number, there is a high likelihood that it is a valid SSN (albeit one assigned to a different person). Hence it is easy to contaminate databases with records containing incorrect SSNs [112]. Similarly, without check digits or another error-detection mechanism, there is no simple way for a system to catch people who are simply making up a phony SSN.

5.10.3 Debate over a National ID Card

The events of September 11, 2001, resurrected the debate over the introduction of a national identification card for Americans.

Proponents of a national identification card point out numerous benefits to its adoption:

1. *A national identification card would be more reliable than existing forms of identification.*

   Social Security cards and driver's licenses are too easy to forge. A modern card could incorporate a photograph as well as a thumbprint or other biometric data.

2. *A national identification card could reduce illegal immigration.*

   Requiring employers to check a tamper-proof, forgery-proof national identification card would prevent illegal aliens from working in the United States. If illegal aliens couldn't get work, they wouldn't enter the United States in the first place.

3. *A national identification card would reduce crime.*

   Currently it's too easy for criminals to mask their true identity. A tamper-proof national identification card would allow police to positively identify the people they apprehend.

4. *National identification cards do not undermine democracy.*

   Many democratic countries already use national ID cards, including Belgium, France, Germany, Greece, Luxembourg, Portugal, and Spain.

Opponents of a national identification card suggest these harms may result from its adoption:

1. *A national identification card does not guarantee that the apparent identity of an individual is that person's actual identity.*

   Driver's licenses and passports are supposed to be unique identifiers, but there are many criminals who produce fake driver's licenses and passports. Even a hard-to-forge identification card system may be compromised by insiders. For example, a ring of motor vehicle department employees in Virginia was caught selling fake driver's licenses [113].

2. *It is impossible to create a biometric-based national identification card that is 100 percent accurate.*

   All known systems suffer from false positives (erroneously reporting that the person does not match the ID) and false negatives (failing to report that the person and ID do not match). Biometric-based systems may still be beaten by determined, technology-savvy criminals [113].

3. *There is no evidence that institution of a national ID card actually leads to a reduction in crime.*

   In fact, the principal problem faced by police is not the inability to make positive identifications of suspects, but the inability to obtain evidence needed for a successful prosecution.

4. *A national identification card makes it simpler for government agencies to perform data mining on the activities of its citizens.*

According to Peter Neumann and Lauren Weinstein, "The opportunities for overzealous surveillance and serious privacy abuses are almost limitless, as are opportunities for masquerading, identity theft, and draconian social engineering on a grand scale . . . The road to an Orwellian police state of universal tracking, but actually *reduced* security, could well be paved with hundreds of millions of such [national identification] cards" [113].

5. *While most people may feel they have nothing to fear from a national identification card system, since they are law-abiding citizens, even law-abiding people are subject to fraud and the indiscretions and errors of others.*

   Suppose a teacher, a doctor, or someone else in a position of authority creates a file containing misleading or erroneous information. Files created by people in positions of authority can be difficult to remove [114].

   In a society with decentralized record-keeping, old school or medical records are less likely to be accessed. The harm caused by inaccurate records is reduced. If all records are centralized around national identification numbers, files containing inaccurate or misleading information could haunt individuals for the rest of their lives.

5.10.4 The REAL ID Act

In May 2005 President George W. Bush signed the REAL ID Act, which significantly changes driver's licenses in the United States. The motivation for passing the REAL ID Act was to make driver's licenses a more reliable form of identification. Critics, however, say the act is creating a de facto national ID card in the United States.

The REAL ID Act requires that every state issue new driver's licenses. These licenses will be needed in order to open a bank account, fly on a commercial airplane, enter a federal building, or receive a government service, such as a Social Security check. The law makes it more difficult for impostors to get driver's licenses, by requiring applicants to supply four different kinds of documentation and requiring state employees to verify these documents using federal databases. Because the driver's license contains a biometric identifier, it is supposed to be a stronger credential than current licenses [115].

Although each state is responsible for issuing new driver's licenses to its own citizens, these licenses must meet federal standards. The license must include the person's full legal name, date of birth, gender, driver's license number, digital photograph, legal address, and signature. All data on the license must be in machine-readable form. The license must have physical security features designed to prevent tampering, counterfeiting, or duplication [116]. The federal government estimates the total cost of implementing REAL ID nationwide to be more than $23 billion—or more than $100 per driver's license.

Supporters of the measure say making the driver's license a more reliable identifier will have numerous benefits. Law enforcement is easier when police can be more certain that a driver's license correctly identifies the individual carrying it. Society is better off when parents ducking child support and criminals on the run cannot change their

identities by crossing a state border and getting a new driver's license under a different name [117].

Some critics fear having machine-readable information on driver's licenses will aggravate problems with identity theft. Each state is required to share all this information with every other state and the federal government. American Civil Liberties Union lawyer Timothy Sparapani said, "We will have all this information in one electronic format, in one linked file, and we're giving access to tens of thousands of state DMV employees and federal agents" [118].

Proponents of the bill say such fears are unjustified. They suggest that the personal information actually available on the new driver's license is relatively insignificant compared with all the other personal information circulating around cyberspace [117].

The transformation of driver's licenses in the United States is still in doubt. Some states have embraced the provisions of the REAL ID Act, but other states have resisted its implementation. California and North Carolina have taken active steps to implement new driver's licenses meeting the specifications of REAL ID. On the other hand, the governors of Idaho, Maine, Montana, New Hampshire, Oklahoma, South Carolina, and Washington have signed bills refusing to comply with the provisions of the REAL ID Act. Six other states have passed measures expressing some form of opposition to the new driver's license standard [119]. The Department of Homeland Security has pushed back the deadline for implementing the new driver's licenses from 2008 to 2013 [120].

5.11 Encryption

Encryption is the process of transforming a message in order to conceal its meaning. In an age in which information is easily captured and rebroadcast, encryption is a valuable tool for maintaining privacy. Even if someone should get a copy of an encrypted message, it is worthless unless the person can decode it.

5.11.1 Symmetric Encryption

In a traditional **symmetric encryption scheme**, a single key is needed to encrypt and decrypt a message. Suppose Smith wants to send a message to Jones. Smith and Jones are the only two people to know the key. Smith uses the key to encrypt the message into cipher. Jones uses the key to decrypt the cipher back into the message. Since no one else has the key, even if the cipher should fall into the wrong hands, it cannot be read. The weakness of symmetric encryption schemes is that it does not solve the problem of how Smith gets the key to Jones. If a hostile outsider should get a copy of the key as it is transmitted, the security of the system is broken.

5.11.2 Public-Key Cryptography

The key transmission problem was solved by Whitfield Diffie and Martin Hellman, who published an alternative scheme, called **public-key cryptography**, in 1976. Public-key encryption is an example of **asymmetric encryption** because it uses two keys instead

of one. Each person has a public key and a private key. A message encrypted with the public key can only be decrypted with the private key. That means everybody who wants to *receive* encrypted messages announces their public keys. If Smith wants to send an encrypted message to Jones, he uses *Jones's* public key. After Jones receives the cipher, he uses his private key to decrypt it. Public-key cryptography eliminates the Achilles heel of symmetric encryption schemes, because no longer is there a need for people to exchange keys. Figure 5.7 illustrates how the RSA public-key encryption algorithm works.

There is a mathematical relationship among the public and private keys, and it is theoretically possible to determine the private key from the public key. The time needed to determine the private key increases with the length of the key. We say encryption is weak if a computer can guess the private key from the public key in a reasonably small amount of time. In contrast, encryption is strong if the amount of time needed by a computer to guess the private key is so long that decryption is essentially impossible. For example, it may be possible for a computer to decipher a strongly encrypted message in 2,000 years, but by that time it probably will make no difference. Strong encryption is possible by choosing a long enough public key.

As we have seen, various federal agencies perform surveillance operations to fight crime and maintain the national security. The work of these agencies is simplified if they have the ability to read domestic and foreign messages. If messages are weakly encrypted, their work is still possible because they have high-speed computers that can decipher the messages. However, if messages are strongly encrypted, their work is made much more difficult. The traditional policy of the United States has been to regulate the use of cryptography within the United States and to forbid the exportation of strong encryption technology.

5.11.3 Pretty Good Privacy

In 1991 the U.S. Senate debated Senate Bill 266, a crime-fighting measure. Buried in the bill was a statement that all manufacturers of communications devices using cryptography would have to provide a "back door" enabling government agencies to read the ciphers. Phil Zimmerman was alarmed by this statement. He wrote:

> If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable military grade public-key cryptographic technology. Until now. [121]

Zimmerman created a public key cryptography program called PGP, which stands for Pretty Good Privacy. He made the program freely available on several Internet sites in the United States. Many people, both inside and outside the United States, downloaded the program. For the next several years the U.S. government threatened legal action against Zimmerman for violating laws against exporting encryption technology. The government's view was that posting the code on the Internet was equivalent to exporting it.

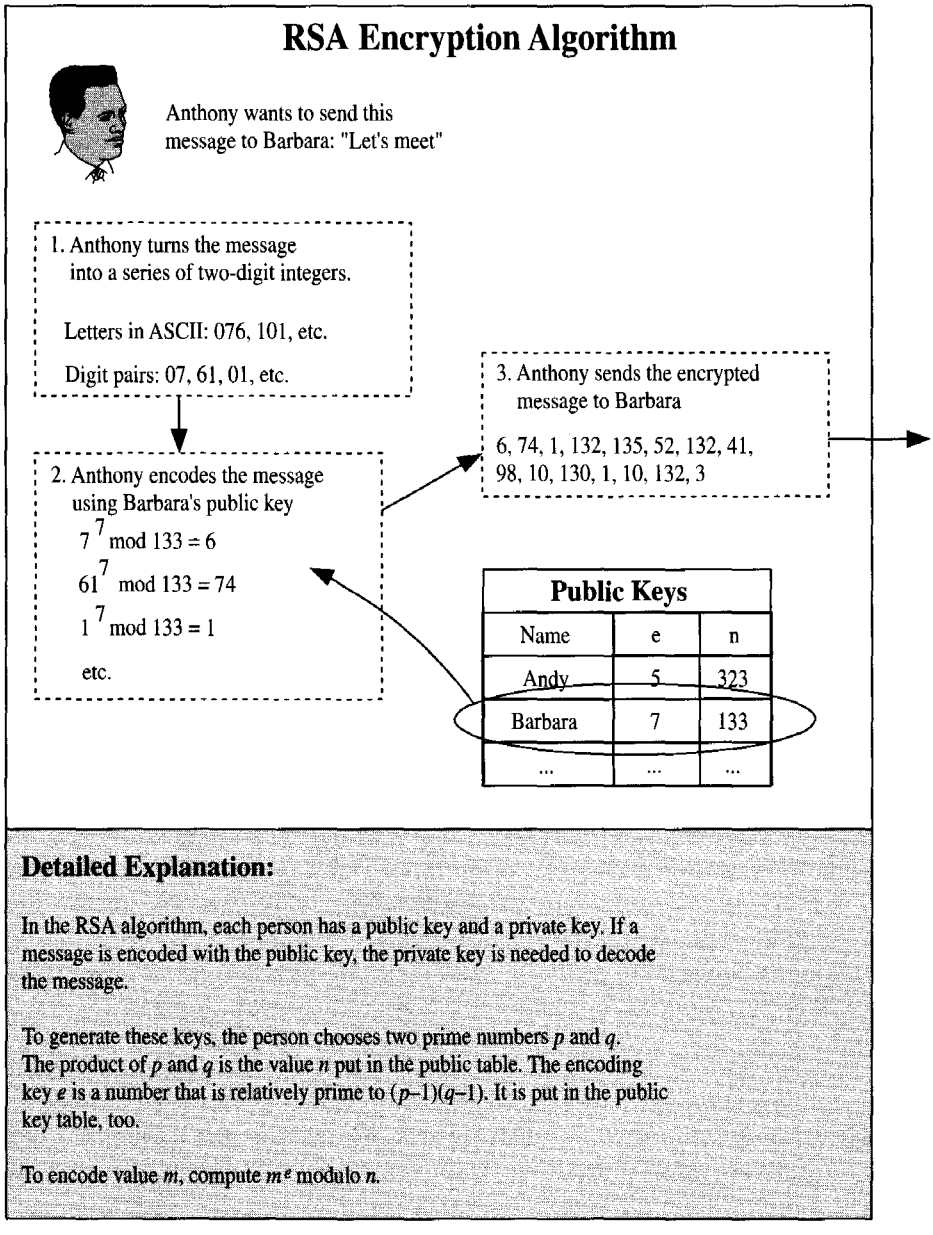
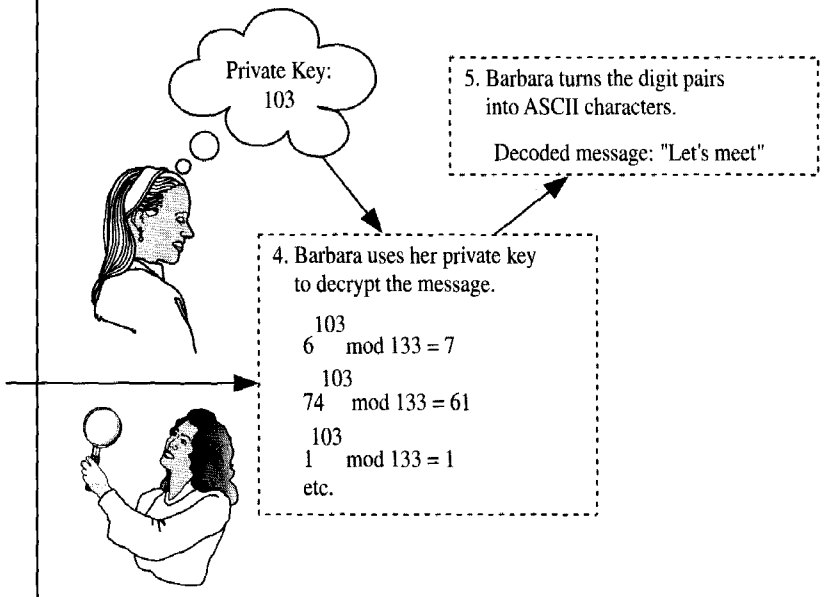


FIGURE 5.7 Illustration of the RSA public-key encryption algorithm, named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.



Anthony can *send* Barbara a message without knowing her private key, but an eavesdropper can't *read* the message without knowing the private key. Since Barbara doesn't have to reveal her private key to anyone, it can't be intercepted by an eavesdropper.

In this simple example Barbara has chosen $p = 11$ and $q = 13$. Since $n = pq$, n has the value 133. The encrypting key $e = 7$, which is relatively prime to $(p-1)(q-1)$, or 120.

The private, decoding key d is the unique number such that $de = 1$ modulo $(p-1)(q-1)$. Here, the decrypting key $d = 103$, since 7 times 103 is 721, which has a remainder of 1 when divided by $(p-1)(q-1)$, or 120.

To decode value m, compute m^d modulo n.

In the real world, primes p and q should be hundreds of digits long, making it impractical to discover the private key, even with the aid of a supercomputer. (Note: This explanation ignores other important, but more technical, considerations.)

FIGURE 5.7 *(continued)*

5.11.4 Clipper Chip

In September 1992 AT&T announced plans to sell for $1,100 a telephone encryption device called the Surity 3600. The FBI and NSA were concerned that this device would compromise their ability to listen in on telephone calls. The Justice Department approached AT&T and suggested that it replace its own encryption scheme with NSA's encryption technology. The code name for this technology was called "Clipper."

The reason the U.S. government wanted AT&T to use the Clipper chip was that the government had the Clipper's mathematical decryption key. With the key in hand, the government would be confident it could listen in on conversations encrypted with the Clipper. AT&T agreed to the Justice Department's proposal, hoping that the U.S. government would make Clipper a national standard for telephone encryption and giving AT&T an edge over its competitors.

In March 1993 President Clinton made a decision to go ahead with the Clipper plan. Two weeks later he publicly announced his support for making the Clipper a national standard. The Justice Department ordered 9,000 Clipper-equipped phones from AT&T. It issued guidelines for control of the keys: two government agencies connected with law enforcement and the intelligence community would have copies of the keys. While the agencies were not supposed to release the keys without proper authorization, there were no penalties for improper release of the keys. The Justice Department did not provide citizens a way to object to the release of the keys or to suppress information gathered, even if the law enforcement or intelligence agency had violated the guidelines.

When the American public became aware of what the government was proposing, the reaction was overwhelmingly negative. A Time/CNN poll showed that 80 percent of the public was opposed to the Clipper proposal [122]. In February 1994 the Clinton administration retreated, proposing that Clipper encryption be named a voluntary standard. The Department of Justice and the NSA continued to urge manufacturers to use Clipper technology rather than other encryption schemes. Incredibly, the NSA also attempted to persuade other countries to make Clipper their standard encryption technology! Needless to say, foreign governments were more than a little reluctant to use an encryption scheme for which the NSA held the decryption key. In the end, the U.S. government's effort to standardize around Clipper failed.

5.11.5 Effects of U.S. Export Restrictions

While the U.S. government prevented American companies from exporting products using strong encryption, this ban did not prevent companies in other countries from developing products that did use strong encryption. Soon after its release on the Internet, the source code to PGP was downloaded to computers outside the United States. It didn't take long for thousands of international software packages to incorporate PGP encryption. American software companies were allowed to manufacture software products using strong encryption for sale inside the United States. Eventually pirated versions of these programs became available outside the United States.

The U.S. State Department ban on selling software with strong encryption outside the United States resulted in an additional burden on the software industry. Each

software maker was faced with a difficult choice. The more expensive alternative was to create and maintain two versions of each software product: the strong-encryption version for sale in the United States and the weak-encryption version for export. The less expensive alternative was to develop only a single version of the software product, the one based on weak encryption, and sell this inferior version both in the United States and internationally.

The ban reduced the international competitiveness of United States companies. U.S. companies forbidden from selling products with strong encryption lost sales to foreign companies that were able to use this technology.

In 1999 and 2000 two different federal appeals courts ruled that the export restrictions violated freedom of speech. In one of the rulings, the court lauded encryption as a way of protecting privacy. Since these rulings, the U.S. State Department has dropped export restrictions on encryption technology.

For decades the National Security Agency has been associated with high-speed computing to fulfill its mission of creating unbreakable codes and breaking the codes of other organizations. According to James Bamford, the NSA now has computers capable of performing a quintillion (1,000,000,000,000,000,000) operations a second [123]. Sara Baase raises an interesting conjecture: Perhaps the U.S. State Department dropped its export restrictions because by 1999 the NSA finally had computers fast enough to decrypt ciphers created using strong encryption [124].

5.11.6 Digital Cash

Glyn Davies defines **money** as "anything that is widely used for making payments and accounting for debts and credits" [125]. Various societies have used cattle, beads, precious metals, coins, paper currency, and many other objects as money. Today, money is often represented electronically. For example, banks routinely use electronic funds transfer to settle debts with each other. Electronic money is an alternative to physical coins and currency. Various systems have been devised that allow people to store electronic money in smart cards or on computer disks.

Electronic money relies upon public-key encryption. Earlier we stated that in a public-key encryption system, a message encrypted with a public key can be decrypted with the associated private key. It's also true that a message encrypted with a private key can be decrypted with the associated public key. When issuing electronic money, a bank signs it with its private key. Customers and merchants can use the bank's public key to verify that the money is authentic. In a similar way, bank customers can use their private key to withdraw funds. The bank uses the customer's public key to verify the identity of the customer.

Implementations of electronic money fall into two categories. In an **identified electronic money** system, the bank can trace the use of the money back to the person who withdrew it from the bank. In an **anonymous electronic money** system, there is no way for a bank to determine what the person who withdrew the money used it for. Anonymous electronic money is also called **digital cash.** Like the physical coins and currency

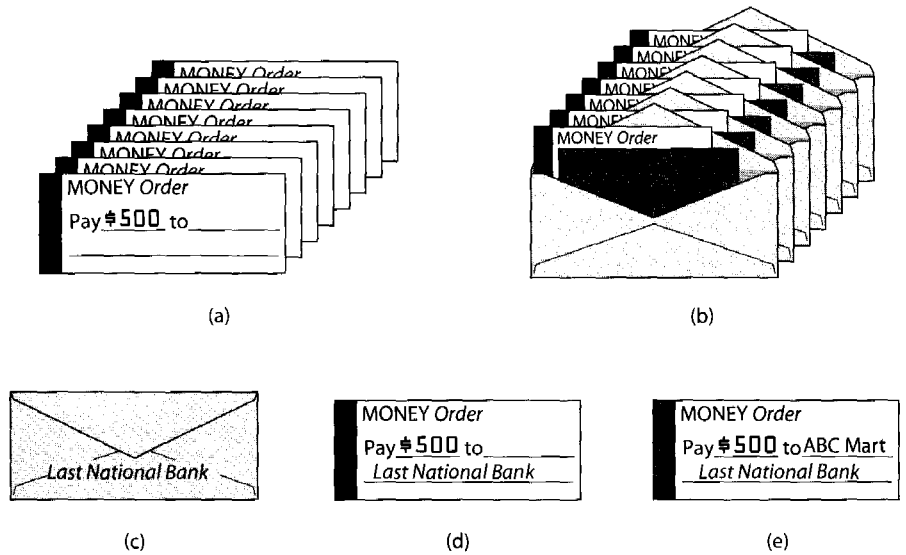


FIGURE 5.8 Bruce Schneier uses this physical analogy to explain how a blind signature protocol works: (a) Ann prepares 100 postal orders for $500, leaving the payee field blank. (b) Ann assembles 100 sealed envelopes. Each contains a postal order and a piece of carbon paper. She takes the envelopes to her bank. (c) The bank opens 99 of the sealed envelopes and sees that each contains a blank money order for $500. The bank is 99 percent sure that the last envelope also contains a money order for $500. It deducts $500 from Ann's account and signs the outside of the last envelope. The carbon paper transfers the signature to the money order. (d) Ann removes the signed money order from the last envelope. (e) Ann uses the money order to purchase $500 worth of goods from ABC Mart. ABC Mart takes the money order to the bank, which credits $500 to its account. The bank has never seen the money order before, so it cannot trace it back to Ann. However, the bank does know the money order is valid, because it recognizes its unique signature. What keeps Ann from trying to swindle the bank by putting $500,000 on one of the purchase orders? She knows she has only a one percent chance of getting away with it; the bank has a 99 percent chance of opening the $500,000 money order. If the bank opens the envelope with the $500,000 money order, she will be prosecuted. The high chance of punishment deters Ann from cheating the bank [126].

we are familiar with, digital cash allows people to preserve their privacy by conducting transactions without leaving an electronic trail behind.

A digital cash system relies upon a **blind signature** protocol that prevents the bank from putting its mark on the electronic cash it issues a customer. Figure 5.8 illustrates a physical analogy created by Bruce Schneier that demonstrates how a bank can confidently sign a purchase order that it has never seen [126].

Digital cash systems can be divided into online and off-line systems. In an **online** system, the merchant communicates with the bank at the time of the sale, as most modern credit card transactions are handled. In an **off-line** system, there is no requirement that the merchant communicate with the bank at the time of the sale. Instead, the mer-

chant collects information from many transactions and contacts the bank periodically to have the funds transferred into its account.

As we have seen in earlier chapters, digital information is simple to duplicate. Suppose Ann has $500 of digital cash. What keeps her from making 1,000 perfect copies of it and going on a wild spending spree?

An online system would catch Ann as soon as she attempted to spend the money the second time. The bank keeps a database of digital cash serial numbers. It knows which digital cash is still out in circulation and which has been spent. When the merchant seeks authorization from the bank, the bank will refuse payment, and the merchant can identify Ann as the person attempting to spend duplicated digital cash.

Even off-line cash systems can prevent people from spending the same cash twice. An observer chip can be placed in the smart card containing the digital cash. The observer chip maintains its own database of digital cash serial numbers, and it can prevent a person from spending the same money twice. Tampering with the observer chip results in the loss of all the information on the chip (i.e., the destruction of the digital cash).

Another off-line digital cash protocol does not prevent a person from spending the same money twice, but it does allow banks to catch those responsible for duplicating digital cash. This protocol has the amazing characteristic that it allows a bank to positively identify someone who has spent two copies of the same digital cash, while it maintains the anonymity of honest people who have spent their digital cash only once. This protocol is more complicated than the one illustrated in Figure 5.8. Bruce Schneier describes it in his book [126].

Finally, digital cash systems can be divided into electronic coins and electronic checks. **Electronic coins** have a fixed value. Combinations of electronic coins allow people to purchase items of arbitrary value. **Electronic checks** are good for purchases up to the value of the check. The unspent portion must be refunded to the purchaser.

Proponents of digital cash point to its privacy benefits. People can use their smart cards or digital computers to spend digital cash with the same anonymity associated with physical coins and currency. Digital cash enables people to conduct electronic transactions without leaving an electronic trail.

Opponents of digital cash note that it will facilitate illicit transactions. Digital cash will make it easier for criminals to launder money. Law enforcement agencies and the IRS will find it more difficult to detect and prosecute criminals.

Consumers and merchants failed to embrace digital cash in pilot projects run by Citibank and Chase Manhattan Bank in New York in the late 1990s. For the time being, customers seem comfortable with their current options: cash, credit cards, and debit cards.

Summary

This chapter has focused on privacy issues brought to the forefront by the introduction of information technology. The issues of privacy and intellectual property are similar in the sense that both issues relate to how information ought to be controlled.

Modern information technology makes it much easier to collect and transmit information, whether it be a song or a Social Security number. Information has become a valuable commodity.

Privacy can be seen as a balancing act between the desires of the individual and the needs of society. The individual seeks to restrict access. Society must decide where to draw the line between what ought to be private and what should be public. While privacy has both costs and benefits, the benefits of providing people at least some privacy exceed the costs. People do not have a natural right to privacy. Instead, it is a prudential right. We choose to give each other some privacy for our mutual good.

There is a tension between privacy and trust. We desire privacy, but we also want to be able to trust those we interact with each day. We trust those with good reputations. Good reputations are established through ordeals and credentials, which require that people reveal information about themselves.

Information can be put into three categories: personal information, public information, and public records. A public record is a piece of information collected by a government agency. Public information is information possessed by an organization that has the right to share it with other organizations. Personal information is information about an individual that is not yet public information or part of a public record. Sometimes public information is gained through voluntary disclosures. At other times people make information public as part of a commercial transaction. Certain activities, such as getting arrested or buying a house, result in the creation of a public record. Finally, organizations can collect information covertly.

People make information about themselves public in a variety of ways. The U.S. government has responded to the general desire for privacy by passing a variety of laws that regulate the collection and distribution of information gathered by private enterprises. These include: the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Family Education Rights and Privacy Act, the Employee Polygraph Protection Act, the Video Privacy Protection Act, the Financial Services Modernization Act, the Children's Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

Three federal agencies have collected a great deal of information about American citizens: the Census Bureau, the Internal Revenue Service, and the FBI. Concern about abuses of public record-keeping systems led to a report containing the Code of Fair Information Practices. Many European countries enacted laws incorporating the principles of this code. Congress's response to the code was the Privacy Act of 1974. The Privacy Act is supposed to protect the privacy of U.S. citizens by giving individual citizens access to public records about themselves, limiting the use of public records, and requiring that the records be accurate. However, the law has so many loopholes that many privacy advocates feel it is a weak piece of legislation.

Overt data collection by the U.S. government has been complemented by covert surveillance by various law enforcement organizations and the National Security Agency. In the name of national security or crime prevention, these agencies have routinely violated federal law in order to eavesdrop on telegraph and telephone conversations.

The U.S. Supreme Court has ruled that electronic eavesdropping without a court order violates the Fourth Amendment to the Constitution.

The USA PATRIOT Act, passed in response to the terrorist attacks of September 11, 2001, amended many existing laws. It allows the use of pen registers and trap-and-trace devices to monitor Internet activity, allows a single judge to authorize wiretaps across the country, and broadens the number of circumstances under which roving surveillance can take place. The Patriot Act also makes it easier for the FBI to collect records from businesses, doctors, schools, libraries, and religious institutions. Citing concerns about possible violations of the Bill of Rights, more than a hundred cities and several states have passed anti–Patriot Act resolutions. A follow-on bill granting law enforcement agencies even greater powers was circulated in 2003, but it was not passed by Congress. In 2006 Congress voted to make permanent all but two of the Patriot Act's provisions: one allowing roving wiretaps, and the other allowing the FBI to seize records from financial institutions, libraries, doctors, and businesses.

Data mining allows an organization to create a complex profile of a person from a collection of individual facts. It is a powerful tool for commerce. Companies use data mining to direct advertising to the most promising customers. Governments also use data mining. The IRS has used it for years to identify suspicious tax returns. The National Security Agency has used records of domestic phone calls to look for calling patterns indicating the presence of terrorist networks.

Data mining is possible because organizations handling transactions have the right to sell information about these transactions to other organizations. Some people believe that such transactions should be private by default. In other words, if Smith buys something from Acme Corp., Acme cannot reveal anything about the transaction to another company without Smith's permission. This is called an opt-in policy. Others believe it ought to be the other way around. Acme should have the right to share or sell information about the transaction unless Smith explicitly forbids Acme from doing so. This is called an opt-out policy.

Identity theft is a significant crime problem in the United States. The leading form of identity theft is credit card fraud. Typically, thieves use fairly simple methods to get access to credit card numbers. They look through mailboxes, garbage cans, or lost or stolen wallets. Some thieves get credit card information through fraudulent telephone calls, email messages, or Web sites. Others have targeted the computerized databases of large institutions, gaining access to hundreds of thousands of personal financial records.

The rapid rise in identity theft has highlighted the inadequacies of the Social Security number (SSN) as an identifier. Originally, use of the SSN was restricted to the Social Security Administration. Over time, however, it has become an important identification number in the United States. Unfortunately, it has many flaws that make it a poor choice for an identification number. Some have proposed the option of a new, national identification card for the United States. They suggest it will reduce illegal immigration and criminal activity. Others say any identification card can be forged, and the creation of a national identification card will make data mining simpler.

The United States has created a new standard for driver's licenses. Even though they will be issued by the states, every state's license must meet the national standard, and the driver's license databases of the individual states will be connected, deterring fraud. The new driver's licenses, to be issued by 2013, will be required for opening bank accounts, traveling on commercial airplanes, and receiving federal services. They are likely to become the most trusted form of identification in the United States, a de facto national identification card.

Encryption is one way people can prevent eavesdroppers from reading the messages they send. In the past, only governments and large businesses had access to powerful cryptography systems. Public-key cryptography systems, such as PGP, have given small businesses and individuals this power. For many years, the U.S. State Department enforced a ban on selling software with strong encryption outside the United States, even though PGP had already been downloaded to computers around the world. In 1999 and 2000 two different federal appeals courts ruled that the export restrictions were unconstitutional, and the State Department dropped its ban.

Digital cash is an anonymous electronic money system that combines the strengths of credit cards and physical currency. Digital cash would be stored on a small, credit card–shaped smart card. A consumer would present this card to pay for goods or services. However, the transaction would be completely anonymous, like a cash transaction. To date, digital cash systems have not been well received. Consumers seem comfortable using cash, credit cards, and debit cards.

Review Questions

1. How is Google's Phonebook service able to produce a map to a person's home, given only that person's phone number?
2. Give an example of a piece of information that a person should not have to reveal to anyone else. Give an example of a piece of information that society should be able to demand that a person reveal.
3. Is privacy a negative right or a positive right?
4. What right is guaranteed by the Third Amendment to the U.S. Constitution?
5. What does it mean when the author says privacy is a prudential right?
6. Give three examples of ways in which an inhabitant of New York City in 2003 has more privacy than an inhabitant of New York City in 1903.
7. What is the difference between a public record and public information?
8. Which is easier for a person to control: public records or public information?
9. List five pieces of information about a person that are public records.
10. Provide an example (not already given in the book) of a situation where people must disclose personal information in order to get something they want.
11. Provide an example (not already given in the book) of a situation where people must reveal personal information, whether or not they consent.

12. Provide an example (not already given in the book) of a situation where information about people is gathered without their knowledge.
13. What is the difference between a digital video recorder and a traditional VCR?
14. Why does enhanced 911 service raise new concerns about privacy?
15. What is spyware? Why does it raise privacy concerns?
16. The Fair Credit Report Act says that information which may negatively affect an individual's credit rating must be removed after seven years. What are two exceptions to this guideline?
17. How does the Fair and Accurate Credit Transactions Act help consumers verify the accuracy of their credit reports?
18. What are the rights provided by the Family Education Rights and Privacy Act?
19. How does the Video Privacy Protection Act enhance privacy?
20. How does the Employee Polygraph Protection Act help job applicants and company employees maintain their privacy? What is the most significant loophole in the Employee Polygraph Protection Act?
21. Summarize the major provisions of the Financial Services Modernization Act.
22. What is the purpose of the Children's Online Privacy Protection Act?
23. Describe the privacy protections resulting from the Health Insurance Portability and Accountability Act.
24. Give two examples of the Census Bureau illegally revealing census data to other federal agencies.
25. Why did consumer groups complain about H&R Block's Web-based Free File tax filing service?
26. Name two notable successes claimed by the National Crime Information Center.
27. What is the purpose of the OneDOJ database? What are its weaknesses, according to the critics of this database?
28. Robert Bellair has said, "The Privacy Act, it turns out, is no protection at all. You can drive a truck through the Privacy Act" [57]. Explain why Bellair and other privacy advocates feel the Privacy Act of 1974 is a weak piece of legislation.
29. What right is guaranteed by the Fourth Amendment to the U.S. Constitution?
30. Explain the significance of the U.S. Supreme Court decision in *Katz v. United States*.
31. What are the key provisions of the Patriot Act?
32. What are we referring to when we talk about a secondary use of data?
33. What is collaborative filtering? Who uses it?
34. Give two examples of government data mining projects currently in operation.
35. What is the Platform for Privacy Preferences? What are the strengths and the weaknesses of this system?
36. What is the most common kind of identity theft?
37. Can a private company legally ask you for your Social Security number?

38. What are the problems with using the Social Security number as an identification number?
39. Name two benefits and two harms that may result from the passage of the REAL ID Act.
40. What is the most significant difference between a public-key encryption scheme and a traditional symmetric encryption scheme?
41. Why did the United States government attempt to stop the distribution of the Pretty Good Privacy (PGP) program?
42. Why did the Justice Department advocate adoption of the Clipper chip?
43. Name three ways that criminals can steal personal information at ATMs.
44. What is digital cash? How does it differ from a credit card? How does it differ from ordinary cash?
45. What is a blind signature protocol? Why are blind signatures needed in a digital cash system?
46. Which pieces of legislation discussed in this chapter increased personal privacy rights? Which laws gave the government greater surveillance powers?

Discussion Questions

47. If people value privacy so much, why do they put so much personal information on their FaceBook pages and in their blogs?
48. Section 5.1 describes the case of the Maryland banker who used information from a state medical records database to identify customers who had cancer. He then called in the loans of these customers. The banker broke no laws and received no legal penalties for his action. Did the banker do anything wrong? Why or why not?
49. Warren and Brandeis argued that it is a violation of a person's privacy to take their photograph without their consent. Do you agree with their position? Why or why not?
50. What is the difference between privacy and anonymity?
51. Critics of grocery club cards give examples of card-member prices being equal to the regular product price at stores without customer loyalty programs. In other words, customers who want to get food at the regular price must use the card. Customers pay extra if they don't want to use the card. Is it fair for a store to charge us more if we don't want to use its loyalty card? Explain your reasoning.
52. Some consumers give phony personal information when they apply for rewards or loyalty cards at stores. Others take it a step further by regularly exchanging their cards with those held by other people. Are these people doing anything wrong? Why or why not?
53. If you voluntarily have your body scanned at a department store, who should own that information, you or the store? Should the store have the right to sell your body measurements to other businesses? Explain your reasoning.
54. TiVo keeps detailed information about the television viewing habits of customers who subscribe to its service.

a. Should your television viewing habits be private information?
b. Do you care if anyone else knows what television shows or pay-per-view movies you have watched in the past year?
c. Do voters have the right to know the viewing habits of people running for elected office?

55. You are sitting on a jury. A driver of a car has been charged with manslaughter for killing a pedestrian. The prosecution presents evidence collected from the automobile's "black box" that indicates the car was traveling at 45 miles per hour before the accident. The defense presents four eyewitnesses to the accident, all of whom testify that the car could not have been going faster than 30 miles per hour. Are you more inclined to believe the eyewitnesses or the data collected from the "black box"? Explain your reasoning.

56. Enhanced 911 service allows cell phone companies to track the locations of active cell phone users within 100 meters.
a. Who should have access to location information collected by cell phone companies?
b. How long should this information be kept?
c. If this information could be used to help you establish an alibi, would you want the cell phone company to be able to release it to the police?
d. How would you feel about the cell phone company releasing compromising information about your whereabouts to the police?
e. Should the police be able to get from the cell phone company the names of all subscribers using their phones close to a crime scene around the time of the crime?

57. Should parents implant microchips in their children to make them easier to identify in case they are lost or kidnapped? Why or why not?

58. Florida, Missouri, Ohio, and Oklahoma have passed laws that require lifetime monitoring of some convicted sex offenders after they have been released from prison. The offenders must wear electronic ankle bracelets and stay close to small GPS transmitters, which can be carried on a belt or in a purse. Computers monitor the GPS signals and alert law enforcement officials if the offenders venture too close to a school or other off-limits area. Police interested in the whereabouts of a monitored person can see his location, traveling direction, and speed plotted on a map [127].

Do these laws represent an unacceptable weakening of personal privacy, or are they sensible public safety measures? Should they be repealed? Should people convicted of other crimes also be monitored for life? Would there be less crime if everyone in society were monitored?

59. Why do you think AOL would want to provide its customers with software tools enabling them to detect and eliminate spyware?

60. Before offering a job candidate a position, some potential employers do a criminal background check of the candidate. What are the pros and cons of this policy?

61. You are applying for an account at a video rental store. The clerk asks you to fill out the application form completely. One of the fields asks for your Social Security number. You leave that field blank. The clerk refuses to accept your application without the field filled in. You ask to speak to the manager, and the clerk says the manager is not available. Would it be wrong in this situation to fill in a fake Social Security number? Explain your reasoning.

62. A company discovers that some of its proprietary information has been revealed in Internet chat rooms. The disclosure of this information results in a substantial drop in the price of the company's shares. The company provides Internet service providers with the screen names of the people who posted the confidential information. It asks the ISPs to disclose the actual identities of these people. Should the ISPs comply with this request? Explain your reasoning. (This scenario is adapted from an actual event [128].)

63. Think about what you do when you get up in the morning. How would you act differently if you knew you were being watched? Would you feel uncomfortable? Do you think you would get used to being watched?

64. Discuss these responses to the revelation that telecommunications companies have been providing domestic phone call records to the National Security Agency [129].

    President George Bush: "Al-Qaeda is our enemy, and we want to know their plans."

    Senator Patrick Leahy of Vermont: "Are you telling me tens of millions of Americans are involved with al-Qaeda?"

    Senator Jon Kyl of Arizona: "We are in a war, and we have got to collect intelligence on the enemy."

    Senator Chuck Grassley of Iowa: "Why are the telephone companies not protecting their customers? They have a social responsibility to people who do business with them to protect our privacy as long as there isn't some suspicion that we're a terrorist or a criminal or something."

65. Was the U.S. government's $2 million settlement with Brandon Mayfield just, or was it excessive?

66. Should states implement the provisions of the REAL ID Act or work for its repeal?

67. In order to combat the counterfeiting of currency, the U.S. Secret Service convinced several color laser printer manufacturers to add a secret code to every printed page. The code is invisible to the human eye but can be seen under a microscope. When decrypted, it reveals the serial number of the printer and the time and date the page was printed [130].

    By agreeing to secretly insert the codes, did the printer manufacturers violate the privacy rights of their customers?

In-class Exercises

68. What does your "ladder of privacy" look like? How does it compare to those of your classmates?

69. Canadian science fiction author Robert Sawyer argues that we need privacy because we have "silly laws" that attempt to make people feel ashamed for indulging in certain harmless activities. He suggests that if there were no privacy, people would insist these laws be overturned [46]. Do you agree with Sawyer's position? Why or why not?

70. Do you agree with the author that it is more difficult to know whom to trust in modern society than it was in a small village of a few centuries ago? Why or why not?

71. Divide the class into two groups. The first group should come up with reasons supporting the proposition, "We live in a global village." The second group should come up with reasons supporting the proposition, "We live in a world of strangers."

72. When you purchase a product or service using a credit card, the merchant has information linking you to the transaction. Divide the class into two groups (pro and con) to debate the proposition that merchants should be required to follow an opt-in policy. Such a policy would require the consumer to explicitly give permission before a merchant could share information about that consumer with another organization.

73. The Code of Fair Information Practices applies only to government databases. Divide the class into two groups to debate the advantages and disadvantages of extending the Code of Fair Information Practices to private databases managed by corporations.

74. While the cost of automobile insurance varies from person to person, based on the driving record of each individual, health insurance premiums are typically uniform across groups of people, such as all of the employees of a company. However, a majority of health care costs are incurred by a minority of the population.

    Today it is possible to take a blood sample from a person and to extract a genetic profile that will reveal that person's disposition to certain diseases. Debate the proposition that health insurance rates should be tailored to reflect each individual's propensity to illness.

75. Divide the class into two groups (pro and con) to debate the proposition that every citizen of the United States ought to carry a national identification card.

76. Debate the following proposition: By creating the Threat and Local Observation Notices (TALON) database, which enabled citizens to report on each other's activities, the U.S. government effectively reduced freedom of speech.

Further Reading

James Bamford. *The Puzzle Palace: A Report on America's Most Secret Agency*. Penguin Books, New York, NY, 1983.

Whitfield Diffie and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. The MIT Press, Cambridge, MA, 1998.

Steven L. Nock. *The Costs of Privacy: Surveillance and Reputation in America*. Aldine de Gruyter, New York, NY, 1993.

George Orwell. *1984*. Knopf, New York, NY, 1992.

Ellen Frankel Paul, Fred D. Miller, Jr., and Jeffrey Paul, editors. *The Right to Privacy*. Cambridge University Press, Cambridge, England, 2000.

Priscilla M. Regan. *Legislating Privacy*. The University of North Carolina Press, Chapel Hill, NC, 1995.

Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. 2nd ed. John Wiley & Sons, New York, NY, 1996.

Ferdinand David Schoeman, editor. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, Cambridge, England, 1984.

Charles J. Sykes. *The End of Privacy*. St. Martin's Press, New York, NY, 1999.

References

[1] Amy Harmon. "Some Search Results Hit Too Close to Home." *The New York Times*, April 13, 2003.

[2] Scott Carlson. "To Guard 3 Students' Privacy, Georgetown U. Expunges Thousands of E-mail Messages." *The Chronicle of Higher Education*, February 7, 2003.

[3] Noah Robischom. "Rx for Medical Privacy." *Netly News*, September 3, 1997.

[4] Aaron Nicodemus. "Agents' Visit Chills UMass Dartmouth Senior." *The Standard-Times (MA)*, December 20, 2005.

[5] Jamie Prime. "Privacy vs. Openness." *Quill*, 82(8), October 1994.

[6] Edmund F. Byrne. "Privacy." In *Encyclopedia of Applied Ethics*, volume 3, pages 649–659. Academic Press, 1998.

[7] Edward J. Bloustein. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, pages 156–202. Cambridge University Press, Cambridge, England, 1984.

[8] Ferdinand Schoeman. "Privacy: Philosophical Dimensions of the Literature." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, pages 1–33. Cambridge University Press, Cambridge, England, 1984.

[9] Edmund Ronald Leach. *A Runaway World?* British Broadcasting Corporation, London, England, 1967.

[10] Marie Hartwell-Walker. "Why Dysfunctional Families Stay That Way." *Amherst Bulletin*, January 28, 1994.

[11] Morton H. Levine. "Privacy in the Tradition of the Western World." In *Privacy: A Vanishing Value?* edited by William C. Bier, S.J., pages 3–21. Fordham University Press, New York, NY, 1980.

[12] Jeffrey H. Reiman. "Privacy, Intimacy, and Personhood." *Philosophy & Public Affairs*, 6(1):26–44, 1976. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. D. Schoenan, Cambridge University Press, 1984.

[13] Stanley I. Benn. "Privacy, Freedom, and Respect for Persons." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, pages 223–244. Cambridge University Press, Cambridge, England, 1984.

[14] Charles J. Sykes. *The End of Privacy*. St. Martin's Press, New York, NY, 1999.

[15] Gini Graham Scott. *Mind Your Own Business: The Battle for Personal Privacy*. Insight Books / Plenum Press, New York, NY, 1995.

[16] Constance T. Fischer. "Privacy and Human Development." In *Privacy: A Vanishing Value?* edited by William C. Bier, S.J., pages 37–45. Fordham University Press, New York, NY, 1980.

[17] Robert C. Neville. "Various Meanings of Privacy: A Philosophical Analysis." In *Privacy: A Vanishing Value?* edited by William C. Bier, S.J., pages 22–33. Fordham University Press, New York, NY, 1980.

[18] Joseph G. Keegan, S.J. "Privacy and Spiritual Growth." In *Privacy: A Vanishing Value?* edited by William C. Bier, S.J., pages 67–87. Fordham University Press, New York, NY, 1980.

[19] Charles Fried. "Privacy: A Moral Analysis." *Yale Law Review*, 77:475–493, 1968. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. D. Schoeman, 1984.

[20] James Rachels. "Why Privacy Is Important." *Philosophy & Public Affairs*, 4(4):323–333, 1975. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. D. Shoeman, Cambridge University Press, 1984.

[21] Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review*, 4(5), December 15, 1890.

[22] William L. Prosser. "Privacy: A Legal Analysis." *California Law Review*, 48:338–423, 1960. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, F. D. Shoeman, ed., Cambridge University Press, 1984.

[23] Judith Jarvis Thomson. "The Right to Privacy." *Philosophy & Public Affairs*, 4(4):295–314, 1975. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. F. D. Schoeman, Cambridge University Press, 1984.

[24] Alexander Rosenberg. "Privacy as a Matter of Taste and Right." In *The Right to Privacy*, edited by Ellen Frankel, Jr., Fred D. Miller, and Jeffrey Paul, pages 68–90. Cambridge University Press, Cambridge, England, 2000.

[25] Humphrey Taylor. "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits." HarrisInteractive, March 19, 2003. The Harris Poll #17.

[26] James Toedtman. "Court Unblocks Do Not Call Registry in Latest Ruling." *Sun-Sentinel (Fort Lauderdale, FL)*, October 8, 2003.

[27] Heather Fleming Phillips. "Consumers Can Thank Do-Not-Underestimate FTC Chairman for Do-Not-Call Peace." *San Jose (CA) Mercury News*, January 2, 2004.

[28] Steven L. Nock. *The Costs of Privacy: Surveillance and Reputation in America.* Aldine de Gruyter, New York, NY, 1993.

[29] Michael L. Sankey and Peter J. Weber, editors. *Public Records Online: The National Guide to Private & Government Online Sources of Public Records*. 4th ed. Facts on Demand Press, Tempe, AZ, 2003.

[30] Jeffrey Rosen. "Being Watched: A Cautionary Tale for a New Age of Surveillance." *The New York Times on the Web*, October 7, 2001.

[31] Michael Liedtke. "New Shopping Technology Could Breed Supermarket Bias." *Kansas City Star*, December 1, 2002.

[32] John Vanderlippe. "Supermarket Cards: An Overview of the Pricing Issues." *Consumers Against Supermarket Privacy Invasion and Numbering*, 2003. www.nocards.org/overview.

[33] Elizabeth Weise. "Identity Swapping Makes Privacy Relative." *USA Today*, June 6, 2000.

[34] Amy Tsao. "So, We'll Take It In . . . " *Retail Traffic*, May 1, 2003.

[35] Amy Harmon. "TiVo Plans to Sell Information on Customers' Viewing Habits." *NYTimes.com*, June 2, 2003.

[36] Ian Austen. "Your Brake Pads May Have Something to Say (by E-mail)." *NYtimes.com*, March 27, 2003.

[37] Jay Warrior, Eric McHenry, and Kenneth McGee. "They Know Where You Are." *IEEE Spectrum*, pages 20–25, July 2003.

[38] Charles J. Murray. "Privacy Concerns Mount over Retail Use of RFID Technology." *Electronic Engineering Times*, (1298), December 1, 2003.

[39] Meg McGinty. "RFID: Is This Game of Tag Fair Play?" *Communications of the ACM*, 47(1):15–18, January 2004.

[40] Thomas Wailgum. "Is Big Brother Coming to Your Wallet?" *CIO*, July 1, 2005.

[41] Kristi Heim. "New Computerized Passport Raises Safety Concerns." *The Seattle (WA) Times*, January 3, 2005.

[42] "American Passports to Get Chipped." *Wired News*, October 21, 2004.

[43] "Owners of Dogs Lacking Implants Face Fines." *The China Post*, September 1, 2000.

[44] Amal Graafstra. "How Radio-Frequency Identification and I Got Personal." *IEEE Spectrum*, March 2007.

[45] Duncan Graham-Rowe. "Clubbers Choose Chip Implants to Jump Queues." *NewScientist*, May 21, 2004. www.newscientist.com.

[46] Robert J. Sawyer. "Privacy: Who Needs It?: We're Better Off without It, Argues Canada's Leading Sci-Fi Writer." *Maclean's (Toronto Edition)*, page 44, October 7, 2002.

[47] Alexander P. Pons. "Biometric Marketing: Targeting the Online Consumer." *Communications of the ACM* 49(8):60–66, August 2006.

[48] Edward C. Baig. "Keep Spies from Skulking into Your PC." *USA Today*, January 22, 2004.

[49] Privacy Rights Clearinghouse. "Fact Sheet 24: Protecting Financial Privacy," July 14, 2005. www.privacyrights.org.

[50] Department of Health of Human Services, USA. "Protecting the Privacy of Patients' Health Information," April 14, 2003. www.hhs.gov/news.

[51] United States General Accounting Office. "IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Risk," December 1998. GAO/AIMD-99-38.

[52] Jean Ann Fox, Chi Chi Wu, Edmund Mierzwinski, Chris Hoofnagle, and Shelley Curran. *Letter to Ms. Pamela F. Olson, Assistant Secretary, U.S. Treasury Department*. Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, National Consumer Law Center, and U.S. Public Interest Research Group, March 24, 2003.

[53] Stephanie L. Hitt. "NCIC 2000." *FBI Law Enforcement Bulletin*, 69(7), July 2000.

[54] Dan Eggen. "Justice Dept. Database Stirs Privacy Fears." *The Washington Post*, December 26, 2006.

[55] U.S. Department of Health, Education and Welfare. *Secretary's Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens*, 1973.

[56] Simson Garfinkel. "Privacy and the New Technology." *Nation*, 270(8), February 28, 2000.

[57] William Petrocelli. *Low Profile: How to Avoid the Privacy Invaders*. McGraw-Hill, New York, NY, 1981.

[58] Whitfield Diffie and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. The MIT Press, Cambridge, MA, 1998.

[59] Priscilla M. Regan. *Legislating Privacy*. The University of North Carolina Press, Chapel Hill, NC, 1995.

[60] Supreme Court of the United States. *Dissenting Opinion in* Olmstead v. United States, 1928. 277 U.S. 438.

[61] Supreme Court of the United States. *Katz v. United States*, 1967. 389 U.S. 347.

[62] James Bamford. *The Puzzle Palace: A Report on America's Most Secret Agency*. Penguin Books, New York, NY, 1983.

[63] Heinz Tschabitscher. "How Carnivore Email Surveillance Worked." email.about.com.

[64] Holly E. Ventura, J. Mitchell Miller, and Mathieu Deflem. "Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power." *Critical Criminology* 13(1): 55–70, January 2005.

[65] U.S. District Court, Central District of California, Western Division. "In the Matter of the Application of the United States of America for an Order Authorizing the Installation of a Pen Register and Trap and Trace Device." Criminal No. 99-2713M, February 4, 2000.

[66] Kevin Poulsen. "FBI Retires Its Carnivore." *SecurityFocus*, January 14, 2005. www.securityfocus.com.

[67] James Risen and Eric Lichtblau. "Bush Lets U.S. Spy on Callers without Courts." *The New York Times*, December 16, 2005.

[68] Lisa Myers, Douglas Pasternak, Rich Gardella and the NBC Investigative Unit. "Is the Pentagon Spying on Americans?" MSNBC.com, December 14, 2005.

[69] American Civil Liberties Union. "No Real Threat: The Pentagon's Secret Database on Peaceful Protest." www.aclu.org, January 17, 2007.

[70] Siobhan Gorman. "Intelligence Policies Shift: Pentagon Spy Chief Rolling Back Some of Rumsfeld's Strategies." *Baltimore Sun*, May 26, 2007.

[71] Samantha Henig. "Pentagon Surveillance of Student Groups Extended to Scrutinizing E-Mail." *The Chronicle of Higher Education*, July 21, 2006.

[72] Nancy Gohring. "FCC Inflates CALEA." *Telephony*, 237(10), September 6, 1999.

[73] Charlotte Twight. "Conning Congress." *Independent Review*, 6(2), Fall 2001.

[74] Kirk Laughlin. "A Wounded CALEA Is Shuttled Back to the FCC." *America's Network*, 104(15), October 1, 2000.

[75] Federal Communications Commission. "FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps," August 5, 2005. www.fcc.gov.

[76] "USA Patriot Act: Major Provisions of the 2001 Antiterrorism Law." *Congressional Digest*, 82(4), April 2003.

[77] David Sarasohn. "Patriots vs. the Patriot Act." *Nation*, 277(8):23, September 22, 2003.

[78] American Civil Liberties Union, New York, NY. "PATRIOT Act Fears Are Stifling Free Speech, ACLU Says in Challenge to Law," November 11, 2003. www.aclu.org.

[79] American Library Association. "Resolution on the USA PATRIOT Act and Related Measures That Infringe on the Rights of Library Users," January 29, 2003. 2002–2003 CD #20.1, 2003 ALA Midwinter Meeting, www.ala.org.

[80] Lawrence Morahan. "'Patriot 2' Raises Concerns for Civil Liberties Groups." *CNSNews.com*, February 13, 2003.

[81] Tom Ridge. "Using the PATRIOT Act to Fight Terrorism." *Congressional Digest*, pages 266–268, November 2004.

[82] Ben Jacklet and Todd Murphy. "Now Free, Attorney Brandon Mayfield Turns Furious." *Washington Report on Middle East Affairs*, 23(6), July/August 2004.

[83] Dan Eggen. "Flawed FBI Probe of Bombing Used a Search Warrant." *The Washington Post*, April 7, 2005.

[84] Eric Lichtblau. "U.S. Will Pay $2 Million to Lawyer Wrongly Jailed." *The New York Times*, November 30, 2006. www.localnewsdaily.com.

[85] Andrew Murr, Michael Isikoff, Eric Pape, and Mike Elkin. "The Wrong Man." *Newsweek*, 143(23), June 7, 2004.

[86] James Rowley and Jeff St. Onge. "U.S. Senate Approves Extension of USA Patriot Act Law (Update1)." *Bloomberg.com*, March 2, 2006.

[87] L. A. Lorek. "Data Mining Extracts Online Gold; Stores Collect Information about Web Customers to Target Future Sales Pitches." *San Antonio Express-News*, December 15, 2002.

[88] "United We Find." *The Economist*, March 10, 2005.

[89] Ann Cavoukian and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World*. McGraw-Hill, New York, NY, 1996.

[90] Richard Peŕez-Peña. "An Early Warning System for Diseases in New York." *NYTimes.com*, April 4, 2003.

[91] Leslie Cauley. "NSA Has Massive Database of Americans' Phone Calls." *USA Today*, May 11, 2006.

[92] Wayne Rash. "Federal Court Finds NSA Wiretaps Unconstitutional." *eWeek.com*, August 18, 2006. www.eweek.com.

[93] "Total Information Awareness Program." *Congressional Digest*, 82(4), April 2003.

[94] Jonathan Riehl. "Lawmakers Likely to Limit New High-Tech Eavesdropping." *CQ Weekly*, 61(7):406–407, February 15, 2003.

[95] Nikki Swartz. "Controversial Surveillance System Renamed." *Information Management Journal*, 37(4):6, July 2003.

[96] Barbara Simons and Eugene H. Spafford. *Letter to The Honorable John Warner and the Honorable Carl Levin*. U.S. ACM Public Policy Committee (USACM), Association for Computing Machinery, January 23, 2003.

[97] Carolyn Hirschman. "Congress Sticks Its Nose into Online Privacy." *Telephony*, 241(7), August 13, 2001.

[98] Martyn Williams. "IBM Researcher Eyes Databases with a Conscience." *InfoWorld Daily News*, August 27, 2002.

[99] Dorothy E. Denning. *Information Warfare and Security*. Addison-Wesley, Boston, MA, 1999.

[100] States News Service. "FTC Testifies on Identify Theft, Impact on Seniors." July 18, 2002.

[101] Matt Richtel. "Financial Institutions May Facilitate Identity Theft." *NYTimes.com*, August 12, 2002.

[102] Privacy Rights Clearinghouse. *How Many Identity Theft Victims Are There? What IS the Impact on Victims?* August 27, 2007. www.privacyrights.org.

[103] Tom Shean. "Damage Done by Identity-Theft Ring Demonstrates Need for Consumer Care." *Virginian-Pilot (Chesapeake, Virginia)*, November 27, 2002.

[104] Roy Furchgott. "In a Single Swipe, a Wealth of Data (Beware of Thieves)." *NYTimes.com*, March 13, 2003.

[105] "LexisNexis Uncovers More Consumer Data Breaches." *Reuters*, April 12, 2005.

[106] Bruce Schneier. "Risks of Third-Party Data." *Communications of the ACM*, 48(5):136, May 2005.

[107] David McGuire. "Bush Signs Identity Theft Bill." *WashingtonPost.com*, July 15, 2004.

[108] Federal Trade Commission. "Take Charge: Fighting Back Against Identity Theft," February 2005. www.ftc.gov/bcp/conline.pubs.

[109] Gartner, Inc. "Gartner Says Identity Theft Is Up Nearly 80 Percent," July 21, 2003.

[110] Social Security Administration, USA. "A Brief History of Social Security," August 2000.

[111] Social Security Administration, USA. "Social Security Cards Issued by Woolworth." www.ssa.gov/history/ssn/misused.html.

[112] Office of Inspector General, Department of Health and Human Services, USA. "Extent of Social Security Number Discrepancies," January 1990. OAI-06-89-01120.

[113] Peter G. Neumann and Lauren Weinstein. "Risks of National Identity Cards." *Communications of the ACM*, page 176, December 2001.

[114] Richard Turner. Letter to the editor. *The Times (London)*, September 7, 2001.

[115] Declan McCullagh. FAQ: How Real ID will affect you. *The New York Times*, May 6, 2005.

[116] National Conference of State Legislatures. "REAL ID Act of 2005 Driver's License Title Summary." 2007. www.ncsl.org.

[117] Dennis Bailey. "Debating Barry Steinhardt's UNREAL ID," August 7, 2005. www .opensocietyparadox.com.

[118] Joseph Menn. "Federal ID Act May Be Flawed." *The Los Angeles Times*, May 31, 2005.

[119] Eliott C. McLaughlin. "Federal ID Plan Raises Privacy Concerns." *CNN.com*, August 16, 2007.

[120] Martin H. Bosworth. "REAL ID Guidelines Issued, But Implementation Delayed." *ConsumerAffairs.com*, March 1, 2007.

[121] Phil Zimmerman. "Why Do You Need PGP?" www.pgpi.org/doc/whypgp/en/.

[122] Philip Elmer Dewitt. "Who Should Keep the Keys?" *Time*, March 14, 1993.

[123] James Bamford. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. Anchor Books, New York, NY, 2002.

[124] Sara Baase. *A Gift of Fire, Second Edition*. Prentice Hall, Upper Saddle River, NJ, 2003.

[125] Glyn Davies. *A History of Money: From Ancient Times to the Present Day*. University of Wales Press, Cardiff, Wales, 1994.

[126] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd ed. John Wiley & Sons, New York, NY, 1996.

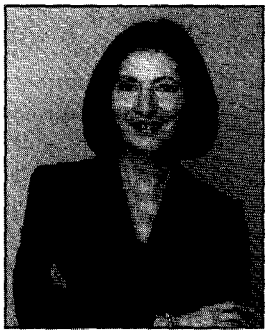
[127] David A. Lieb. "States Move on Sex Offender GPS Tracking." *Associated Press*, July 30, 2005.

[128] Stewart Deck. "Legal Thumbs-Up for Raytheon Employee Suit; Privacy Groups Chilled by ISP Subpoenas." *Computerworld*, April 12, 1999.

[129] Susan Page. "NSA Secret Database Report Triggers Fierce Debate in Washington." *USA Today*, May 11, 2006.

[130] John P. Mello Jr. "Codes Make Printers Stool Pigeons." *E-Commerce Times*, October 18, 2005. www.ecommercetimes.com.

AN INTERVIEW WITH



Ann Cavoukian

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She oversees the operations of the freedom of information and privacy laws in Ontario, Canada, in her role as Information and Privacy Commissioner (IPC). Dr. Cavoukian joined the Office of the IPC as its first Director of Compliance in 1987. Prior to joining the IPC, she headed the Research Services Branch for the provincial Attorney General. She received her M.A. and Ph.D. in Psychology from the University of Toronto, where she specialized in criminology and law, and lectured on psychology and the criminal justice system.

Her published works include *Who Knows: Safeguarding Your Privacy in a Networked World,* with Don Tapscott (McGraw-Hill, 1997), and *The Privacy Payoff: How Successful Businesses Build Consumer Trust,* with Tyler Hamilton (McGraw-Hill Ryerson, 2002).

What is information privacy?

Information privacy essentially revolves around personal control—an individual's right to control the collection, use, and disclosure of his or her personal information. Freedom of choice is vital. Personal information is information that relates to an "identifiable individual." Organizations that collect, use, and disclose personal information can protect an individual's right to privacy by implementing what are commonly referred to as "fair information practices." Fair information practices are a set of common standards that balance an individual's right to privacy with the organization's legitimate need to collect, use, and disclose personal information. In Canada, fair information practices are set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* (the CSA Code). At the international level, I chaired a working group of data protection and privacy commissioners convened for the purpose of creating a single Global Privacy Standard (GPS), which was formally tabled and accepted by Commissioners in 2006 at the 28th International Data Protection Commissioners Conference in the United Kingdom.

The CSA Code consists of ten principles. First, it requires the designation of at least one individual who is accountable for the organization's compliance with the other nine principles (**Accountability**). The organization must specify the purposes for which it collects personal information, at or before the time when the information is collected (**Identifying Purposes**). The consent of the individual must be obtained for the collection, use, or disclosure of personal information, except where it is not appropriate to obtain consent (**Consent**). The collection of personal information must be limited to that which is necessary to fulfill the specified purposes (**Limiting Collection**). Personal information must not be used or disclosed for purposes other than those for which it was collected, unless the individual consents or as required by law (**Limiting Use, Disclosure,** and **Retention**). Personal information must be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used (**Accuracy**). The organization must implement security safeguards that are appropriate for the level of sensitivity of the personal information (**Safeguards**). The organization must make readily available specific information about its policies and practices relating to the management of personal information (**Openness**). Individuals have a right to access and request correction of their own personal information (**Individual Access**). Finally, individuals must be able to challenge an organization's compliance with the privacy principles (**Challenging Compliance**).

The GPS is based on the same underlying principles as the *CSA Code:* Consent; Accountability; Purpose; Collection Limitation; Use, Retention, and Disclosure Limitation; Accuracy; Security; Openness; Access; and Compliance. However, with respect to the principle that the collection of personal information should be limited to that which is necessary for the specified purposes, the GPS goes further by emphasizing the need for data minimization. Data minimization requires the collection of personal information to be kept to a strict minimum. This means that the design of programs, information technologies and systems should begin with nonidentifiable interactions and transactions as the default. Wherever possible, the identifiability, observability and linkability of personal information should be minimized. Also, in terms of accountability the GPS goes further than the *CSA Code* by requiring the documentation and communication of privacy policies and procedures, as well as the designation of a responsible person, and by requiring organizations to seek equivalent privacy protection through contractual and other means when transferring personal information to third parties.

People often sacrifice information privacy for the sake of convenience. Is information privacy really important?

Consumers are sometimes willing to provide personal information in exchange for some benefit or service. For example, consumers are sometimes willing to register personal information on a Web site in exchange for useful information or a discount on merchandise. It is up to each individual consumer to weigh the cost and benefits of providing personal information in any given situation—it's his or her choice. As long as this collection of personal information takes place with the knowledge and consent of the individual, it is not an invasion of privacy—it is a matter of personal choice and control which is central to the concept of privacy. When information is collected, used or disclosed without the knowledge or consent of the individual, then privacy becomes an issue.

How has 9/11 affected people's attitudes toward information privacy?

Immediately after 9/11, people seemed willing to sacrifice civil liberties and privacy if necessary, in order to feel secure. There was a surge of support, particularly in the United States, for increasingly invasive security measures and expanding public surveillance. However, as time passed, heads cooled and the public began to think more rationally about these issues and whether or not the invasive security measures that were being implemented and contemplated would actually having the desired impact on national security. The public began to question whether the privacy sacrifice that we were all being asked to make was actually worth it. In June of 2007, federal, provincial and territorial privacy commissioners across Canada united in calling for the federal government to suspend its new no-fly list program until it could be overhauled to ensure strong privacy protections. The Passenger Protect Program involves the secretive use of personal information in a way that will profoundly impact privacy and other related human rights, without legally enforceable rights of appeal to independent adjudication or to compensation for expenses and damages.

The public's interest in protecting consumer privacy, however, did not diminish in the post-9/11 period. If anything, the value of trusted business relationships has increased.

Information about customers is a valuable commodity. Why should a business be concerned about protecting the privacy of its customers?

In Canada, it happens to be the law for private sector organizations, but a simple answer to the above question is that, "privacy is good for business!" This assertion is supported by a Harris/Westin Poll where in November 2001 and February 2002, it was found that if consumers had confidence in a company's privacy practices, they were much more likely to increase volume of business and frequency

of business with that company. Conversely, they were likely to stop doing business with a company if it misused personal information. Further, The Information Security Forum reported in 2004 that a company's privacy breaches can cause major damage to brand and reputation. Robust privacy policies and staff training were viewed as keys to avoiding privacy problems.

Organizations that do business in the U.S. may be subject to one or more recently enacted breach notification laws that require organizations to tell consumers when their personal information has been breached. These laws have helped to expose numerous serious privacy breaches. Such breaches can have serious consequences for both the individuals whose privacy is breached and the organization that is responsible for the breach. For example, the *Wall Street Journal* reported in May 2007 that following the TJ Maxx breach, involving the theft of 45.7 million credit and debit card numbers, banks could be forced to spend $300 million to replace cards and that the breach could result in $20 million in fraudulent transactions. The potential costs and harm to an organization's reputation provides a further incentive for organizations to think proactively to prevent privacy breaches.

Do you favour opt-in policies over opt-out policies?

As a general rule, opt-in policies are viewed as being more privacy-protective than opt-out policies. However, the type of consent that an organization should obtain (i.e., opt-in versus opt-out) depends on the circumstances in which personal information is being collected, used and disclosed. When it is reasonable in the circumstances to infer implied consent, an opt-out type of consent may be appropriate, particularly where the information is not considered to be sensitive. For example, the individual's name and address may not be considered to be sensitive, and the collection of this information for specified purposes may take place with an opt-out type of consent. On the other hand, opt-in consent should generally be obtained whenever sensitive personal information, such as medical information or financial information, is being collected, used or disclosed.

Is Canada ahead of the United States with respect to ensuring fair information practices?

Canada has more comprehensive privacy and data protection laws and statutory oversight/enforcement agencies. By contrast, the U.S. has a multitude of specialized, sectoral laws, regulations and self-regulation and more scope for private rights of action and financial penalties. There is strong evidence that Canadian organizations are more aware of privacy and much more likely to apply privacy principles throughout their operations than U.S. firms.

For example, in a benchmark study conducted by my office and the Ponemon Institute—a Tucson, Arizona–based "think tank" dedicated to the advancement of responsible information management practices within business and government—we compared the corporate privacy practices of Canadian and U.S. businesses. Some of the key findings of the study were that in comparison to U.S. companies, Canadian companies:

- are more likely to have a dedicated privacy officer and a privacy program with a clearly articulated mission,
- are more likely to have a formal redress process for customers to respond to queries and concerns about privacy,
- are more open to providing customers with the right to access and correct personal information,
- offer more choice to customers and consumers in terms of opting out (or opting in) to secondary uses and disclosures of personal information,
- are less likely to sell customer data,
- are more likely to offer privacy training or awareness programs for employees and contractors who handle sensitive personal information,

- hold their vendors and other third parties to higher standards or due diligence requirements,
- have a more aggressive data control orientation when collecting and retaining sensitive personal information,
- are more concerned about insider misuse than external penetration,
- require more rigorous data quality controls and monitoring requirements for transacting and moving of personal information about employees and customers, especially when the application involves transborder movement, and
- are more likely to have strict policies that protect the privacy of employees.

As you ponder new threats to information privacy, are there any emerging technologies you find particularly troubling?

A qualified answer would include item-level Radio Frequency Identification (RFID) tags; conventional biometric and other forms of authentication and identification; data mining; and video surveillance. If these emerging technologies are designed and implemented with fair information practices in mind, then they can enhance and enrich our lives immeasurably. But if used surreptitiously and without regard for privacy, they only hold the promise of an untenable scenario of ever-present surveillance and discrimination, the proverbial "Orwellian nightmare." It all depends on the design and configuration of a particular technology.

It is also important to note that there are emerging technologies that can actually help us to protect our privacy. Such technologies are generally referred to as Privacy Enhancing Technologies (PETs). For example, Biometric Encryption is a PET that allows you to use your biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications—to gain access to computers, to enter buildings, and to privately and securely prove identity, etc. This represents an enormous gain to privacy and heralds the growth of a new area of privacy-enhancing biometrics under the emerging category of untraceable biometrics.