BOOKS AND ARTICLES

Many of these references include topics that are covered throughout this book. Some of the references in Chapter 10 also include topics covered throughout this book.

- Richard A. Spinello and Herman T. Tavani, eds., Reading in CyberEthics, Jones and Bartlett, 2001.

ORGANIZATIONS AND WEBSITES

- Herman Tavani, ed., "The Tavani Bibliography of Computing, Ethics, and Social Responsibility": cyberethics.cbi.msstate.edu/biblio
2.1 The Impact of Computer Technology

2.1.1 INTRODUCTION

After the fall of the communist government in East Germany, people examined the files of Stasi, the secret police. They found that the government had used spies and informers to build detailed dossiers on the opinions and activities of roughly six million people, a third of the population. The informers were neighbors, coworkers, friends, and even family members of the people they reported on. The paper files filled an estimated 125 miles of shelf space. Computers were not used at all.1

Medical and financial information, details of purchases, and evidence of romantic affairs can all be found by going through someone’s garbage. Before the digital age, surveillance cameras watched shoppers in stores and employees at work.

Computers are not necessary for the invasion of privacy. However, we discuss privacy at length in this book because the use of computers has made new threats possible and old threats more potent. Computer technology has had a profound impact on what information is collected about us (sometimes without our permission or knowledge), who has access to it, and how they use it. Computer technology allows search and surveillance of huge numbers of people, often without our knowledge. Privacy is probably the “computer issue” that worries people most.

There are three key aspects of privacy:

- freedom from intrusion—being left alone
- control of information about oneself
- freedom from surveillance (from being followed, watched, and eavesdropped upon)

It is clear that we cannot expect complete privacy. We usually do not accuse someone who initiates a conversation of invading our privacy. Many friends and slight acquaintances know what you look like, where you work, what kind of car you drive, and whether you are a nice person. They need not get your permission to observe and talk about you. It is often said that if you live in a small town, you have no privacy, everyone knows everything about you. In a big city, you are more nearly anonymous. But if people know nothing about you, they may be taking a big risk if they rent you a place to live, hire you, lend you money, sell you an automobile or medical insurance, cash your checks, accept your credit card, and so on. We give up some privacy for the benefits of dealing with strangers. We can choose to give up more in exchange for other benefits.

For the most part, in this book, we view privacy as a good thing. In this chapter and several others, we see a frequent tension between law enforcement and the privacy of innocent people. Critics of privacy argue that it gives cover to deception, hypocrisy, and wrongdoing. It allows fraud. It protects the guilty. Concern for privacy may be regarded with a suspicious “What do you have to hide?” Privacy involves a balancing act. Privacy scholar Alan Westin describes the factors to be balanced as follows:

- safeguarding personal and group privacy, in order to protect individuality and freedom against unjustified intrusions by authorities
- collecting relevant personal information essential for rational decision-making in social, commercial, and governmental life
- conducting the constitutionally limited government surveillance of people and activities necessary to protect public order and safety.4

In Sections 2.1.2–2.4, we look more closely at collection and use of personal information by businesses, governments, and organizations and at privacy issues and risks that result. (Although we discuss private sector and government issues in separate sections, there is often overlap. We look at intentional, institutional uses of personal information (primarily law enforcement and tax collection in the government sector and marketing in the private sector by both businesses and non-profit organizations); unauthorized use by “insiders,” the people who maintain the information; and inadvertent leakage of information through negligence or carelessness. In Section 2.2, we also consider issues of search and surveillance by governments. In Sections 2.5–2.6, we discuss a variety of approaches to protecting privacy and controversies about them.

Privacy issues arise in many different contexts. More topics with privacy implications appear in later chapters. Communications privacy is the central topic of Chapter 3. Anonymity, which can protect both privacy and freedom of speech, but makes crime easier, is discussed more fully in Chapter 5. We also discuss spam, the intrusion of online junk mail, in that chapter. We address the problem of intruders and hackers in Chapter 7. These activities threaten privacy. In Chapter 7, we examine some methods for reducing such crimes as fraud and the release of computer viruses; we find privacy threats in some of these methods, such as the use of biometrics for identification. Privacy of employees in the workplace is discussed in Chapter 8. Privacy comes up again in Chapter 10, where we focus on the responsibilities of computer professionals.

We use the term personal information often in this chapter. In the context of privacy issues, it includes any information relating to or traceable to an individual person. It is not restricted solely to what we might think of as sensitive, private information, although it includes that. It also includes information associated with a particular person’s “handle,” user name, online nickname, identification number, or e-mail address. Nor is it restricted to text data; it extends to any information from which a living individual can be identified, including images.

The man who is compelled to live every minute of his life among others and whose every thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. [He] merges with the mass. . . . Such a being, although sentient, is fungible; he is not an individual.

—Edward J. Bloustein5
CHAPTER 2 PRIVACY AND PERSONAL INFORMATION

It's important to realize that privacy preserves not personal secrets, but a sense of safety within a circle of friends so that the individual can be more candid, more expressive, more open with "secrets."—Robert Ellis Smith

2.1.2 RISKS OF THE TECHNOLOGY

Computers and the Internet and World Wide Web make the collection, searching, analysis, storage, access, and distribution of large amounts of information much easier, cheaper, and faster than before. The sentence you just read appeared in Section 1.3.1, where the context made it clear that these were great benefits. But when the information is about our activities, opinions, and personal characteristics, the same capabilities threaten our privacy. Today there are thousands of databases, both government and private, containing personal information about us. Some of this information, such as our specific purchases in supermarkets and bookstores, was simply not recorded before. Some, including government documents like divorce and bankruptcy records, was in public archives and took a lot of time and effort to access before. In the past, conversations disappeared when people finished speaking, and personal communications were normally read by only the sender and the recipient. Now that we communicate by e-mail and electronic discussion groups, our words are recorded and can be copied, distributed, and read by others even years later. We browse in libraries and bookstores with anonymity and can buy all sorts of magazines and newspapers for cash, but, on the Web, a record can be kept of every page we visit.

INVISIBLE INFORMATION GATHERING

Invisible information gathering describes collection of personal information about someone without the person's knowledge. The important ethical issue is that, if someone is not aware that the information is being collected or of how it will be used, he or she has no opportunity to consent or withhold consent for its collection and use. Examples of invisible information gathering include satellite surveillance (discussed in more detail in Section 2.2.2) and automatic identification of a person's telephone number when he or she calls an 800 or 900 number. Invisible information gathering is common on the Web; we will describe a variety of examples shortly.

Most people who used supermarket club cards several years ago did not know that the store collected and kept a record of everything they bought when they swiped their card at the checkout stand. Now more people know, and they know that at some stores they are trading a degree of privacy for discounts. Thus, whether a particular example of personal data collection is invisible information gathering can depend on the level of public awareness and the knowledge of the particular person. Even when we know that Web sites can collect information, we often are not aware of just what information a particular site is collecting.

THE IMPACT OF COMPUTER TECHNOLOGY

An Internet service provider (ISP) manages the connection between a user and the sites he or she is visiting. Thus the ISP "knows" every site we visit. Yahoo! for example, collects four terabytes of log data daily. Logos are useful for determining customer needs, allowing advertising resources, improving services, and advertising. ISP and Web site logs are used for tracking and collecting evidence about criminals. They include such details of our online activities as where we went, what we did, and how long we stayed at a particular page.

Cookies are files a Web site stores on each visitor's computer. The site stores in the cookie and then uses information about the visitor's activity. For example, a retail site may store the contents of our virtual "shopping cart" in a cookie. On subsequent visits, the site retrieves information from the cookie. Cookies were developed as a customer convenience; by using information in the cookie, a site avoids having to ask a user to type the same information each time he or she visits. Most big Web sites use cookies; they help companies provide personalized customer service and target advertising to the interests of each visitor. At first, cookies were controversial because the very idea that Web sites were storing files on the user's hard drive without the user's knowledge was startling and disturbing to many people. If a Web site we visit can read cookies, what else on our computers can it read? Also, cookies can be used to track our activities on many sites. A site that has our name and address can link the information together. Now more people are aware of cookies, but many Web sites do not inform visitors when they are being used.

The software and sophisticated tools that Web sites use allow information about a visitor to be collected by advertisers on a site, not just the site sponsor itself. In some cases this is intentional, and the information supplied to the advertiser is limited. The complexity and obscurity of software can make it difficult to determine that information is being collected and where it is going. In some cases, personal information was sent to an advertiser as an accidental side effect of the complex design of the software that manages the information and connections between sites. Several companies discovered that such leaks, called data spillage, were occurring in their systems. A few examples: DoubleClick, a Web advertising company, received people's financial information from a Quicken Web site. E-Loan, an online loan business, put a lot of money and effort into ensuring privacy of the financial data entered by customers; then the company discovered that software in the systems of other companies it bought or had partnering agreements with was collecting its customer information.

Some companies monitor the hard drives and search queries of people who use peer-to-peer systems to trade music and other files. The information is used for targeted marketing. QuickClick, a service of NBCI that enables the user to click on "any word, anywhere" and get information about it, collected more than just the word clicked on and transmitted a user identification number with each selected word. NBCI said it did not use the extra information and was not interested in tracking user behavior, but the point is that information is collected invisibly—and a company's policies might not always be benign.) A company offered a free program that changed a Web browser's cursor
CHAPTER 2 PRIVACY AND PERSONAL INFORMATION

into a cartoon character or other image; millions of people installed the program, then later discovered that the program sent to the company a report of the Web sites its users visited, along with the customer's serial number. RealNetworks' program RealJukebox, which helps users manage and play digital music files, sent to RealNetworks information about the music played and copied by its users. Jukebox software provided by other companies collects similar information but informs the users and lets them turn off the data collection. This last example illustrates that the data collection itself is not always sinister or dangerous. Some people don't mind giving the information; some are trading information for a free service or other benefit. The critical point is whether the user is told and thus can make an informed choice about using the software.

SECONDARY USE, COMPUTER MATCHING, AND PROFILING

The ease of copying, distributing, and analyzing data resulting from the use of computers and computer networks led to a huge increase in secondary use of personal information, that is, use of information for a purpose other than the one for which it was supplied. It is difficult for individuals to control their personal information if it is collected by one business, organization, or government agency and shared with or sold to others.

We will see many examples throughout this chapter. They include sale of consumer information to marketers or other businesses, use of information in various databases to deny someone a job, use of numerous databases by the Internal Revenue Service to find people with high incomes, purchase of drivers' license photographs from state motor-vehicle departments by a company providing security services, and the use of a supermarket's customer database to show alcohol purchases by a man who sued the store because he fell down.

Usenet newsgroups provide an early example of the risks of invisible information gathering and the power of storage and search technology to use information in ways utterly unanticipated at the time it was provided. Beginning more than 20 years ago, Usenet eventually had thousands of groups, many of a technical or otherwise nonpersonal nature, but some covering sensitive political, sexual, health, and religious topics. Although participants largely knew that outsiders could log on and read any newsgroup, the likelihood was small; the presumption was that only a relatively small group of people who shared common problems or interests read the postings. The volume of postings, roughly a gigabyte a day by the mid-1990s, made it impossible for most sites to store them for longer than a few days. Participants thought their postings were ephemeral as a conversation. But there were archives, some going back many years. The archives, especially for the technical newsgroups, form a valuable historical research source. Companies that developed some of the first search engines for the Web collected the archives and used them to demonstrate the power of their search tools. It quickly became popular for people to search for the names of their acquaintances and find all the messages they had posted. Some employers reviewed postings of job applicants. One company's software

*Usenet newsgroups were early discussion forums on the Internet, before the World Wide Web.

allowed creation of user profiles describing the subjects a person frequently wrote about. (In 2001, Google acquired a Usenet archive with 630 million postings from about 35,000 newsgroups.)

Computer matching means combining and comparing information from different databases (usually by using a person's Social Security number to match records). Businesses use the technique to form consumer dossiers, and government uses it primarily for detecting fraud and enforcing the law in other ways. Computer profiling means using data in computer files to determine characteristics of people most likely to engage in certain behavior. Businesses use profiling to find people who are likely customers for specific products and services. A few dozen federal agencies use computer profiling to identify people to watch—people who have committed no crime but might have a "propensity" to do so. Computer matching and profiling are, in most cases, examples of secondary use of personal information.

LOCATION, LOCATION, LOCATION

Computer technology has increased the power and scope, while reducing the size and cost, of surveillance devices such as cameras and locating devices. In Section 1.3, we saw several benefits of tracking and location technologies. Here's the other side: Global positioning system (GPS) technology, satellites, and computer chips make it possible to track our movements and determine a person's current location. If, when you lock your keys in your car, the car company can remotely unlock it for you with a radio signal, the car company can determine your location. The cell phones and other wireless appliances many people now carry allow our location to be determined. Devices installed in rental cars, to locate them if they are stolen, can also be used to monitor or track drivers. (A rental car agency fined a man for speeding, based on information from a tracking device in the car. A company sells wireless watchband transmitters for children, so parents can monitor them. The federal government ordered that all wireless and cell phones have tracking capabilities to locate a phone making a 911 call. This is obviously useful for emergencies, but once the tracking technology is there, what else will it be used for? Some worry that we will be pestered with advertising calls as we walk or drive past a store having a sale. Some worry about abuse by government, saying that the government's ability to track and locate everyone by accessing the wireless telephone provider's system, the rental car system, and so forth, is a threat to our freedom. Will there be options for owners to turn off tracking features? It is essential that such questions be considered early in the development of new technologies and applications so that privacy concerns can influence both the technical design and the laws mandating particular features.

2.2 "Big Brother Is Watching You."

When the American Republic was founded, the framers established a libertarian equilibrium among the competing values of privacy, disclosure,
CHAPTER 2 PRIVACY AND PERSONAL INFORMATION

and surveillance. This balance was based on the technological realities of eighteenth-century life. Since torture and inquisition were the only known means of penetrating the mind, all such measures by government were forbidden by law. Physical entry and eavesdropping were the only means of penetrating private homes and meeting rooms; the framers therefore made eavesdropping by private persons a crime and allowed government to enter private premises only for reasonable searches, under strict warrant controls. Since registration procedures and police dossiers were the means used to control the free movement of "controversial" persons, this European police practice was precluded by American governmental practice and the realities of mobile frontier life.

—Alan F. Westin, Privacy and Freedom, 1968

In George Orwell's dystopian novel 1984, Big Brother (the government) watched everyone virtually all the time via "teleseens" in all homes and public places. There was little crime and little political dissent—and no love and no freedom. Today, the government does not have to watch every move we make, because so many of our activities leave data trails in databases available to government agencies. The use of myriad personal-data systems to investigate or monitor people is sometimes called data surveillance, short for "data surveillance." When Big Brother wants to take a direct look at us and our activities, he uses sophisticated new surveillance tools. We examine some of these databases and tools and consider their compatibility with constitutional and legal protections from government intrusions.

2.2.1 DATABASES

Federal government agencies maintain thousands of databases containing personal information. As far back as 1982, it was estimated that federal agencies had approximately 3.5 billion personal files, an average of 45 files for every American in the United States. Many are now accessible via computer networks, and other government agencies as well as private organizations use the information. Now, the federal government has access also to the huge trove of data in business databases, much of which it can get without a court order.

Government databases help government agencies perform their functions efficiently, determine eligibility for government jobs and benefits programs, detect fraud, recover payments on delinquent debts (e.g., student loans and child support payments), collect taxes, and catch criminals. Fraud in programs such as welfare, Medicare, and worker's compensation and defaults on guaranteed student loans cost billions of dollars each year. Restrictions on the government's access to and use of personal data would encourage more fraud and waste. However, because of the scope of the government's activities and the mass of data available to it, the use and misuse of personal data by government agencies pose serious threats to the liberty and personal privacy of all of us.

The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988 are two of the main laws that regulate the federal government's use of personal data. Congress passed the Privacy Act of 1974 in response to abuses by the federal government

"BIG BROTHER IS WATCHING YOU."

- Restricts the data in federal government records to what is "relevant and necessary" to the legal purpose for which it is collected.
- Requires federal agencies to publish a notice of their record systems in the Federal Register so that the public may learn about what databases exist.
- Allows people to access their records and correct inaccurate information.
- Requires procedures to protect the security of the information in databases.
- Prohibits disclosure of information about a person without his or her consent (with several exceptions).

Figure 2.1 Provisions of the Privacy Act of 1974

in the 1960s and early 1970s, to allay concern about the government's use of computer technology to invade citizens' privacy. In the 1960s and 1970s, the FBI secretly used its National Crime Information Center (NCIC) database to track the movements of thousands of people not wanted for any crime; many were opponents of the Vietnam war. The FBI kept files on civil rights activists, celebrities, and many other Americans. Other abuses included wiretappings, mail openings, burglaries, harassment of individuals for political purposes, and questionable use of personal records. The provisions of the Privacy Act are summarized in Figure 2.1. Although this law was an important step in attempting to protect our privacy from abuse by federal agencies, it has problems. It has, to quote one expert on privacy laws, "many loopholes, weak enforcement, and only sporadic oversight."

The Computer Matching and Privacy Protection Act of 1988 requires government agencies to follow a review process before doing computer matching for various purposes. An investigation by an agency of Congress several years later found that government agencies were quite careless about following the provisions of the law.

The Internal Revenue Service (IRS) uses computers to match tax data on individuals and small businesses with a variety of federal and state government records. It scans vehicle registration records for people who own expensive cars and boats; it searches professional license records for people who are likely to have large incomes. It searches a database of "suspicious" cash transactions, examining transaction information of millions of taxpayers. (Banks and other businesses are required to report all large, and suspicious small, cash transactions to the government.)

In the 1990s, both the IRS and the FBI announced plans to drastically expand their databases. The IRS wanted to build a huge database of individuals, combining information from federal, state, and commercial sources, including motor-vehicle departments, credit bureaus, state and local real-estate records, newspapers, federal employment files, federal licensing data, and so on. Privacy advocates objected for several reasons, one being that the proposed system would use records that are often inaccurate. (What if the IRS matches tax returns with files of a computerized dating service that include possibly exaggerated information on income? If this example seems frivolous or unlikely, consider that...
suspicious may be detained by police, lose benefits, or be ordered to pay additional taxes. Innocent people are subject to embarrassing searches and expensive investigations and sometimes to arrest and jail. Do databases and search technologies simply make the work of law-enforcement agencies more efficient, or do they fundamentally change the relationship between citizen and government?

**OBEYING THE RULES**

Quis custodiet ipsos custodes? (Who will guard the guards themselves?)

—Juvenal

Several studies have found that government agencies do not adequately protect personal information, often in violation of laws passed to protect privacy and reduce government abuse of data. The General Accounting Office (GAO) is Congress "watchdog agency." One of its tasks is to monitor the government's privacy policies. In 1990, the GAO released a major study showing lack of compliance with the Privacy Act of 1974. In 1996 Congress investigated a "secret" database maintained by the Internal Revenue Service containing the names and addresses of 200,000 people with more than a hundred fields of data for each person, including ethnic and political information. A 1997 study looked at privacy policies of government Web sites. It found that more than 80% of federal government Web sites linked from the White House Web page violated provisions of the Privacy Act. In response to this study, a few agencies stopped placing cookies on the hard drives of visitors to their sites. Dozens of agencies, including the White House's Office of National Drug Control Policy, the Justice Department, the Defense Department, and the Energy Department continued to use cookies, although they probably violate the Privacy Act. A GAO study of 65 government Web sites in 2000 found that only 3% of the sites fully comply with the "fair information" standards for notice, choice, access, and security established by the Federal Trade Commission for commercial Web sites. The FTC itself was one of the sites that did not comply. There are many specific cases of leakage of information from government files. According to another GAO report, abuses of the FBI's NCIC by employees of law-enforcement agencies include selling information to private investigators, snooping on political opponents, and altering or deleting information. In one case, a former law-enforcement officer used NCIC to track down his ex-girlfriend; he then murdered her. The Los Angeles Police Department found that a significant number of employees illegally snooped for criminal records on people they knew or were considering hiring for such jobs as baby-sitter. Employees of the Social Security Administration and other federal agencies have been arrested for selling data on thousands of people, both to collection agencies and to a credit-card fraud ring. A high-ranking IRS official was indicted for selling information from tax files. Year after year, hundreds of IRS employees are investigated for unauthorized snooping in people's tax files. It is likely that most such activity goes undetected. An IRS employee who was a Ku Klux Klan member read tax records of members of his Klan group, looking for income information that would indicate that someone was an undercover agent. This and other abuses led to a 1997 law with tough penalties for government employees who snoop through people's tax information without authorization. However, a 1999 GAO report found that while the IRS had made significant improvements over prior years, the tax agency still failed to adequately protect people's financial and tax information. Unauthorized IRS employees were able to alter and delete data; disks with sensitive taxpayer information were disposed of without the files being erased; and hundreds of tapes and diskettes were missing. Computers provide a new enormously powerful tool for investigation, surveillance, and intrusion into our personal lives. We should expect government to meet an especially high standard for privacy protection, because it is coercive by nature. It has the power to arrest people, jail them, and seize assets from them. We have no choice, in most cases, about providing our personal information to the government. A former director of the ACLU Privacy and Technology Project commented that, "Particularly where the government is involved, consent [to use of personal information] is coerced and meaningless." 22

**2.2.2 THE FOURTH AMENDMENT AND EXPECTATION OF PRIVACY**

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.

—Fourth Amendment, U.S. Constitution

The U.S. Constitution protects a right to privacy from intrusion by government, most explicitly in the Fourth Amendment. The Supreme Court has interpreted other parts of the Bill of Rights to provide a constitutional right to privacy from government in other areas as well. England has a similar tradition, as expressed in William Pitt's colorful statement in 1763: "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be fail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter—but the King of England cannot enter ...." 24 Here we look at how databases and surveillance technology challenge this right.

**WEAKENING THE FOURTH AMENDMENT**

The Fourth Amendment sets limits on the government's rights to legally search our homes and businesses and seize documents. It requires that the government have "probable cause" for the search and seizure; that is, there must be a good reason for the specific search. The trouble is that now so much personal information is not safe in our homes or in the individual offices of our doctors and financial advisors. It is in huge databases outside of our control. Many laws allow law enforcement agencies to get information from nongovernment databases without a court order. For example, the FBI may get certain information from credit reports without a court order (though not a person's
complete credit history). It can get student records and many other records without a court order, in emergencies. The comprehensive federal medical privacy rules issued in 2001 allow law enforcement agencies to access medical records without court orders. The USA PATRIOT Act of 2001 lets the government collect information from financial institutions on any transactions that differ from a customer's usual pattern and ease government access to many other kinds of personal information (without a court order). What level of access should the FBI have to those logged by ISPs and Web sites we visit?

As we consider all the personal information available to government agencies now, we can reflect on the worries of Supreme Court Justice William O. Douglas about the potential abuse just from government access to the records of someone's checking account. In 1968, he said:

In a sense a person is defined by the checks he writes. By examining them agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. These are all tied in to one's social security number, and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subservient or potential or likely candidates.

Today's readers should not miss the irony of the last sentence: 190 million was the whole population of the U.S. at the time.

The next few examples illustrate more ways technology erodes Fourth Amendment protection. Courts sometimes use the notion of "expectation of privacy" to determine when the Fourth Amendment applies. We will explain this concept and its weaknesses.

**SATELLITE SURVEILLANCE AND THERMAL IMAGING**

Satellites use various computer technologies to take detailed photographs of the earth, detailed enough to show our homes and backyards. The federal government sells the images to state governments, which use them to catch people who are growing . . . What? Are you expecting "marijuana"? No doubt, satellites have looked for that, but they are also used to catch people growing cotton without appropriate permits. Some state governments use the photos to detect building or property improvements that would raise property taxes; some plan to use them to find people who have built backyard porches without all the required building permits.

Is this an intrusion into our personal space, a search of our homes, that the Fourth Amendment should prohibit without a warrant? The Supreme Court has already said "maybe" in a side comment in a decision that permitted surveillance from an airplane, but so far there has been no direct legal challenge of satellite imaging. The constitutional status of searching by satellite remains open, and government agencies continue to use the images.

In 2001, the Supreme Court ruled that police could not use thermal imaging devices to search a home from the outside without a search warrant. The Court stated that where "government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search,' and requires a search warrant." This reasoning makes sense when a technology becomes more widely used, the government may use it for surveillance without a warrant. This standard may allow time for markets, public awareness, and technologies to develop to provide privacy protection against the new technology. Is it a reasonable standard, or should the government have to satisfy the requirements of the Fourth Amendment for any search of a home (in nonemergency situations)?

**AUTOMATED TOLL COLLECTION AND ITEMIZED PURCHASE RECORDS**

Many bridges, tunnels, and toll roads now use automated toll-collection systems. Sensors read a device in the car as it goes by without stopping, and the owner's credit card or bank account gets billed for the toll. These systems save time for drivers and reduce the costs of collection. Their flexibility also allows the implementation of variable charges for different times of the day to improve traffic flow. The database used for billing drivers contains a record of where and when a person traveled (and, in some cases, how fast). The privacy concern is that marketers and government agencies can use this information to track people. Some toll-road operators have an option allowing drivers to pay cash in advance, avoiding billing records. Currently, however, most of the systems do not provide anonymity.

Police use toll records in investigations. A bridge and tunnel authority in New York had a policy that it would not disclose a driver's travel information except when required by law or when presented with a court order by a law-enforcement agency. A judge ruled that police could get such information without a court order. The judge said that traffic movement is in public view, a person does not have a reasonable expectation that information about his or her travel is private, and therefore the Fourth Amendment does not protect it. Let's look at this reasoning and its implications.

Yes, it is true that when we drive in public, anyone might see us. Someone could stand near a bridge and write down the license plate number of each car that passes by. If the police assigned an officer to do this, there might be a fuss. In any case, it simply was not done, not at all bridges and toll roads, 24 hours a day. We expected that our travel was mostly anonymous; strangers saw but did not recognize us, and no record remained after we passed by. The automated toll systems change the situation fundamentally. They keep a detailed, computerized record, 24 hours a day, of every vehicle using the system.

When we shop in a supermarket or a bookstore, we may be observed, and someone we might occasionally remember what we bought. Before computerized checkout systems, no one recorded our specific purchases. If the judge's argument in the toll case were to apply, would the police have access, without a court order, to lists of all the books we buy? In fact, law enforcement agencies have asked bookstores and online seller Amazon.com to turn
over records of books purchased by particular people, sometimes with a search warrant, sometimes without one. These requests raise First Amendment issues as much as Fourth Amendment issues. The head of the American Booksellers Association commented that “From a First Amendment perspective, having the government be able to go in and review an individual’s buying or reading patterns will have an incredible chilling effect.”

SUPREME COURT DECISIONS AND EXPECTATION OF PRIVACY

Several Supreme Court cases addressed the impact of technology on Fourth Amendment protection in earlier contexts. In Olmstead v. United States, in 1928, the government had used wiretaps on telephone lines without a court order. The Supreme Court used a literal interpretation of the Fourth Amendment, ruling that it applied only to physical intrusion and only to search or seizure of material things, not conversations. Justice Louis Brandeis dissented, arguing that the authors of the Fourth Amendment did all they could to protect liberty and privacy, including privacy of conversations, from intrusions by government based on the technology available at the time. He believed that the Fourth Amendment should be interpreted as requiring a court order even when the technology gave the government access to our personal papers and conversations without entering our homes.

In Katz v. United States, in 1967, the Supreme Court reversed its position and ruled that the Fourth Amendment does apply to conversations and that it applies in public places in some situations. In this case, law-enforcement agents had attached an electronic listening and recording device on the outside of a telephone booth to record a suspect’s conversation. The court said that the Fourth Amendment “protects people, not places,” and that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” To intrude in places where a reasonable person has a reasonable expectation of privacy, government agents need a court order.

Although the Supreme Court’s decision in Katz v. United States strengthened Fourth Amendment protection in some ways, there is significant risk in relying on reasonable “expectation of privacy” to define the areas where a court order is needed. We saw that a judge used this notion to decide that law enforcement agents have access, without a court order, to all the detailed tracking information collected by surveillance systems. We used to have a reasonable expectation of privacy while driving around in our cars or, rarely, in our own backyards, but as well-informed people come to understand the capabilities of modern surveillance tools and the mass of information in databases, we might no longer expect privacy from government, in a practical sense. Does that mean we should not have it? The Court recognized this problem in Smith v. Maryland, in which it noted that, if law enforcement reduces actual expectation of privacy by actions “alien to well-recognized Fourth Amendment freedoms,” this should not reduce our Fourth Amendment protection. However, the Supreme Court has interpreted “expectation of privacy” in a very restrictive way. For example, it ruled that if we share information with businesses such as our bank, then we have no reasonable expectation of privacy for that information (United States v. Miller, 1976). Law-enforcement agents do not need a court order to get the information. This interpretation seems absurd. We do expect privacy of the financial information we supply a bank or other financial institution, as we do for many kinds of information we share with a few, sometimes carefully selected, others.

Should the capabilities of new technology give government agencies access to formerly private or ephemeral information without the protection of the Fourth Amendment? The notion of “expectation of privacy,” as now interpreted by the Supreme Court, offers weak protection. Whether we preserve the spirit, or only the words, of the Fourth Amendment remains an open question. Eternal vigilance, we have been warned, is the price of liberty. This vigilance in the context of computerized information and surveillance systems means giving careful thought to what information we allow the government to collect and access and how we allow it to be used.

2.2.3 MORE SEARCH AND SURVEILLANCE TOOLS

ELECTRONIC BODY SEARCHES

Several airports use an X-ray device that displays on a computer screen the image of a person’s body without clothes. Weapons and packets of drugs hidden under clothing are visible in the image. The U.S. Customs Service first used the device to examine travelers it suspected of smuggling drugs. People singled out for search were given a choice of using the machine or undergoing a “pat-down” search. After the terrorist attacks in 2001, the Federal Aviation Administration ordered the machines for airport security.

What are the advantages and disadvantages of these devices? How does the computer technology change the impact of a search? A scan by the machine is faster, more thorough, and less physically intrusive than a pat-down search. On the other hand, the display shows the person’s body in detail; a director of the American Civil Liberties Union (ACLU) described a scan by the machine as “an electronic strip search.” Once the computer captures the image, it can store and copy it.

There are slightly different questions to consider, depending on whether officials use the device only on people singled out as suspects for other reasons, or on all passengers. If it is used only on suspects, we might well ask how many innocent people’s privacy we are willing to trade for the chance of catching a criminal. Would you consider it a reasonable trade-off if 95% of the people the Customs Service selected for drug scanning were actually carrying drugs, and only 5% were not? What if only 50% of the people scanned were carrying them? Only 10%! Is our attitude about the legitimacy of using this technology affected by our perception of how likely we are to be its innocent victims? Among the poorest people, 95% were actually carrying drugs.

One company that makes the airport body scanners plans for the machines to X-ray passengers as they move along on a conveyor belt—similar to the current screening method for carry-on luggage. The ease of searching people with this technology means...
that more people will be searched. Is routinely exposing images of our naked bodies to guards an acceptable trade-off of privacy for security?

The government is funding development of a variety of devices that can search through a person’s clothing from a distance, without the person’s knowledge or cooperation, to detect hidden weapons. These devices have valuable security applications, but the technology can be used for random searches, without search warrants or probable cause, on unsuspecting people. Clearly, guidelines are needed for acceptable uses of such machines.

**WHO’S GOT YOUR PICTURE?**

We are used to security cameras in banks and convenience stores. They deter crime and help in investigations of crimes. Prisons use video surveillance systems (sometimes called CCTV, for closed circuit television) for security; gambling casinos use them to watch for known cheaters. Video surveillance systems monitor traffic and catch vehicles and individuals in the act making7

Cameras alone raise some privacy issues. When combined with face-recognition systems, they raise even more. We describe some applications of face recognition and some relevant privacy and civil-liberties issues.

In 1999, a private company bought the digitized driver photos maintained by the motor-vehicle departments in several states. The company said it was buying the photos and building the database, which included other personal information such as Social Security numbers, to provide security services, for example to protect against credit fraud. Drivers had no choice about whether their photos were sold. Later it was disclosed that the U.S. Secret Service provided technical assistance and $1.46 million in funding for the project. The Secret Service supported the project to fight terrorism, illegal immigration, and “identity crimes.”

Publicity about the project generated public protest, and some states decided not to sell their driver photos.7

The Tampa, Florida police used a computer system to scan the faces of all 100,000 fans and employees who entered the 2001 Super Bowl (causing some reporters to dub it Snoopers Bowl). The system searched computer files of criminals for matches, giving results within seconds. People were not told they were being photographed. Later Tampa installed a similar system in a neighborhood of popular restaurants and nightclubs. Police in a control room zoom in on individual faces and check for matches in their database of suspects. After September 11, 2001, several airports installed face-recognition systems, and police cameras in Washington, D. C. zoomed in on individuals a half mile away.

The ACLU has compared the use of the face-recognition system at the Super Bowl to a computerized police lineup, to which innocent people were subject without their knowledge or consent. Face-recognition systems had an accuracy rate of little more than 50% in the early 2000s. (Photos in databases tend to be old, and the systems do not perform well on images taken from different angles and in different lighting conditions.)

---

7 The Secret Service has responsibility for investigating some kinds of financial and computer crime, in addition to its better-known role of protecting the President.

Harvard research fellow David Banisar argued that the low accuracy rate could result in the detention of many innocent people. The accuracy will likely improve, but other issues will remain.

There are more than 500,000 CCTV cameras in England, many outdoors in public places to deter crime. A Londoner is likely to be recorded dozens of times a day. Government officials in a suburb of London said the CCTV’s were responsible for 500 arrests in one year. Others argue that the cameras have not reduced crime. Defense lawyers complain that prosecutors sometimes destroy footage that might clear a suspect. A study by a British university found a number of abuses by operators of surveillance cameras, including collecting salacious footage, such as people having sex in a car, and showing it to colleagues. A traffic monitoring system in Florida was removed after engineers were observed zooming in on individual pedestrians unrelated to traffic flow.

Is enforcing a 9 PM curfew for young people, one of the uses of public cameras in England, important enough to accept the potential abuses? Even if one thinks government curfews for young people are reasonable (and many do not), this application suggests the kind of monitoring and control of special populations made easy by cameras. Banisar asks whether face-recognition systems would be used to track political dissidents, journalists, political opponents of powerful people—the kinds of people who were targeted for illegal or questionable surveillance in the past. More fundamentally, is this level of surveillance, with its potential for abuse, compatible with our notions of privacy and a free society? Not to 500 people who complained when the California Department of Transportation photographed their license plates and then contacted them for a survey on traffic in the area where they drove. These people objected vehemently to what they considered unacceptable surveillance by a government agency even when it was only their license plates, not their faces, being photographed for a survey, not a police action. Several city governments considered using cameras in public places, but decided not to. Toronto city officials refused to let police take over their traffic cameras to monitor a protest march and identify its organizers. In a controversial statement, the Privacy Commissioner of Canada argued that the country’s Privacy Act required a “demonstrable need for each piece of personal information collected” to carry out government programs and therefore recording activities of large numbers of the general public was not a permissible means of crime prevention.

Many applications of CCTV and face-recognition systems are reasonable, positive uses of the technology for security and crime prevention. But there is a clear need for controls, guidelines, and some limitations. How should we distinguish appropriate from inappropriate uses? Should international events such as the Olympics, which are sometimes terrorist targets, use such a system? Should technologies like face-recognition systems be used only to catch terrorists and suspects in serious crimes, or should they be used in public places to screen for people with unpaid parking tickets? Should people be informed when cameras are in use? If we consider these issues early enough, we can design some privacy-protecting features into the technology and consider appropriate privacy-protecting legislation before, as the Supreme Court of Canada worries in the quote that follows, “privacy is annihilated.”
CHAPTER 2 PRIVACY AND PERSONAL INFORMATION

To permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society. ... We must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.

—Supreme Court of Canada, 1990

FIGHTING TERRORISM

For a while after the terrorist attack on the World Trade Center and the Pentagon on September 11, 2001, attitudes about surveillance technologies and policies changed drastically in the United States. Many people wanted to use all available tools to catch terrorists and prevent future terrorist attacks. In this book, we focus on the uses and abuses of technology, not all the very difficult, wider issues related to terrorism. High-tech surveillance technologies are helpful but are not a panacea. A face-recognition system will not stop a terrorist whose photo is not in the database of suspected terrorists. Airport security before the terrorist attacks could detect small knives and box cutters, but the rules permitted them. The core of the security failure in 2001 was that U.S. intelligence agencies did not know that the attack was planned.

The fundamental issues have not changed. The difficult task of choosing the right tools to use and the right trade-off between security and the privacy, freedom, and convenience of innocent people remains. We do not want to live in a "police state," nor are such places guaranteed to be safe. People in prison, the ultimate police state, manage to get weapons and illegal drugs; they rape and murder other prisoners. Security will never be complete. Certainly some high-tech security systems can help reduce terrorism, but, if used without sufficient care and protection for civil liberties and privacy, they turn us all into prisoners.

2.3 Consumer Information

2.3.1 DATABASES AND MARKETING

If you enter a contest or fill out a warranty questionnaire, information about you will be entered into a database and probably made available to direct marketers. If you buy a bicycle, you might get a solicitation from a magazine about bicycle touring. If you buy baby clothes, you will get many mailings about other baby products. Nonprofit organizations, from the Sierra Club to the National Rifle Association, use mailing lists to solicit contributions, members, and action in support of their causes. If you file a change-of-address notice with the U.S. Postal Service, your name and new address are provided to mailing-list managers who sell the lists to mass mailers. The ads you see on your computer screen while visiting certain Web sites are different from the ads seen by others; they are chosen for you by software, based on your previous activity at the site (or other sites).

Catalogs and other advertising arrive in our mailbox. Telemarketers disturb our peace with their annoying telephone sales pitches. Web pages are splattered with ads. E-mail users receive spam, or unsolicited, mass e-mail. The target lists and sometimes the sales pitches themselves are computer generated.

Businesses use powerful hardware and software to analyze consumer data, government records, and any other useful information to determine who might be a new customer. This is an application of a process called data mining, the searching of masses of data to find new information or knowledge. Marketers use thousands of criteria to decide who gets a specific catalog or promotional mailing. Long-distance telephone companies use lists of subscribers to foreign-language newspapers or Web sites to find potential customers for special telephone service deals; they send the ads in the customer's language. American Express mines hundreds of billions of bytes of data on how customers have spent hundreds of billions of dollars. They send discount coupons and special promotions for the specific stores where customers shop. Online book and music sellers make recommendations to you that are based on prior purchases by you and other people with similar buying patterns. Some supermarket chains store a year's worth of data on the details of customer purchases. Airlines send incentives to frequent fliers who are flying less frequently. Cruise lines send ads to people who have gone on cruises before. A pasta company sends coupons to people who buy its competitor's products. A company sells lists of e-mail addresses of people who post to newsgroups on the Internet; the lists are organized by interest areas, including general interests, hobbies, religion and "adult." This kind of marketing was not possible without computers and was not possible even with the technology of about 15 years ago. Marketers were limited to studying buying habits of people in broad categories, such as women from 25 to 49.

DoubleClick, an online advertising service that sells ads on 1500 Web sites, caused a highly publicized controversy in 2000 by planning to combine its huge database of Web-surfing activity with a huge database of offline purchases and real names and addresses. Faced with strong criticism by angry privacy advocates and investigations by government agencies, DoubleClick dropped the plan. However, some other ad companies mix online and offline data to target ads. Most people do not distinguish between mailings generated by sophisticated computer mining of databases and mailings addressed to "occupant." Both infringe on the first aspect of privacy: being free from intrusion. The sale of personal data and the building of detailed profiles of a consumer's opinions, preferences, and activities infringe on the second aspect of privacy: control of information about oneself (if the person has not given permission). As one journalist said, "it gives some people the creeps." We now consider some potential problems and some perspectives.

A purchase of pasta or the fact that someone reads weather reports on the Web is not particularly personal or sensitive. An immigrant may appreciate getting ads in his or her native language. 'But would a customer be happy being on a list of people considered likely to buy a product for adults who are incontinent'? One company compiled such a list
gave consent to the distribution of her name. Is there anything about computerization of marketing lists that contributes to the woman's pain in such a case? Yes. The ease of copying computer files means that a large number of businesses could have bought her name. It might take a huge effort to track down every company that now has her name and ask each to stop sending mail. Consent to distribution of our names and addresses for marketing purposes is a decision that is difficult to revoke.

2.3.2 CHILDREN ON THE WEB

There are two main privacy issues related to children on the Web, one of which is linked to safety: Child molestors use the Web to find children, win their confidence via e-mail and chat, then arrange meetings. The second issue is the collection of personal information by the many Web sites designed for children. Adults can make decisions about what information they want to give out, or what degree of tracking they want to allow in exchange for discounts or access to certain sites. Young children are not likely to understand the risks and trade-offs. Children give out family income data and other personal family information on the Web. Aside from the general problems of consumer data and the activity profiles we have already mentioned, detailed profiles about children, including their hobbies, nicknames, names of friends, and so forth, are a treasure for child predators. Parents and privacy advocates, concerned about the safety of children, criticized Netromail for providing a service, intended for marketers but available to others, that included names, addresses, and ages of children.48

In 1998, a Federal Trade Commission (FTC) study found that 89% of Web sites aimed at children collected personal information, and only 23% of the sites asked children to get consent from their parents before providing the information. Later that year, Congress passed the Children's Online Privacy Protection Act (COPPA) ordering the FTC to set up rules for protecting children under age 13. The rules (which went into effect in 2000) prohibit Web sites from collecting personal information from children under 13 without "verifiable parental consent." The sites must prominently post their policy telling what information they collect and how it is used.

2.3.3 CREDIT BUREAUS

Credit-bureau databases are one of the best examples of the observation that data collected for one purpose almost inevitably will be used for other, unexpected purposes. The three major credit-reporting companies, Experian, Equifax, and Trans Union, receive and process millions of records daily. In addition to bill-paying history, a credit report may contain information from public records, such as lawsuits, bankruptcies, and liens. The primary purpose of the credit bureau is to provide a central storehouse of information for evaluating applicants for credit. Some employers (including the federal government) also use credit bureaus as part of a background check on job applicants.

2.3.4 PRINCIPLES FOR DATA COLLECTION AND USE

The Fair Credit Reporting Act of 1970 (FCRA) was, according to Privacy Journal, the first law, anywhere in the world, to establish regulations for use of consumer information by private businesses.49 It restricts credit bureaus to disclosing credit information only to employers, the government, insurance companies, and others who need it for legitimate business purposes involving the consumer.50 That last category is vague and easy to circumvent. It was relatively easy to get someone's credit report for other purposes. Credit reports have embarrassed political candidates and undermined spouses in divorce cases. In 1996, Congress amended the FCRA, setting stronger standards to reduce access to credit records and making access under false pretenses a felony.

Credit information is of concern to privacy advocates because a bad credit report can prevent someone from getting a mortgage, a car loan, a job, or other services. (Privacy advocates and business people tend to disagree on the weight given to credit information when making decisions.) Sometimes an applicant is unaware that a credit report is the basis for a negative decision. The FCRA places limits on old negative information, about, for example, bankruptcies, criminal convictions, and civil judgments. Some see this as a privacy protection, whereas others see it as an unreasonable restriction on the flow of relevant information.

Some critics have strongly rebuked credit bureaus for selling mailing-lists to marketers. The bureaus used their databases and other sources to produce and sell lists of "elite retail shoppers," "highly affluent consumers," people in financial difficulties, and other specially targeted groups. Credit bureaus had catalogs describing and promoting the variety of lists that were available.51 As a result of public criticism and pressure, Equifax terminated its marketing mailing-list business in 1991. The Federal Trade Commission ruled that the practice violated the FCRA. Experian (then called TRW) agreed to stop. Trans Union fought in court, and eventually lost in 2001.52

For many years, credit bureaus sold "header" information from credit files, including name, address, phone number, Social Security number, and so on. Marketers, lawyers, and many others made many uses of this information. In 2001, a federal judge ruled that the law restricting sale of personally identifiable financial information included the headers on credit reports, and the credit bureaus could no longer sell header information without consumer consent.53 This ruling was a significant change in privacy protection.

---

* When I use the term "consumers," I include members, contributors, Web-site visitors, and others who would be in the domain of various businesses and organizations.
for many benefits, from borrowing a large amount of money for a home mortgage to convenient shopping on the Web. People vary in how much they value their privacy, how desirable or annoying they find advertising, and so forth. When people are informed about the data collection and use policies of a business or organization, they can decide whether or not to interact with that business or organization.

After informing people about what an organization does with personal information, the next simplest and most desirable policy is to give people a choice about whether data collected about them is distributed to other businesses or organizations and is used to send advertisements. The two most common forms for providing such choice are called opt out and opt in. Under an opt-out policy, one must check a box on a contract, membership form, or agreement, or call or write to the organization to request removal from distribution lists. If the consumer does not take action, the presumption is that his or her information may be used. Under an opt-in policy, personal information is not distributed to other businesses or organizations unless the consumer has explicitly checked a box or signed a form permitting disclosure. (Be careful not to confuse the two. Under an opt-out policy, more people are likely to be "in," that is, on the lists, and under an opt-in policy, more people are likely to be "out," because the default presumption is the opposite of the policy name.)

Until the late 1990s, neither policy was widely used. Many businesses indicated in small print in their customer agreements that they might use consumer data in various ways and exchange it with other businesses. Now, it is common for such agreements to have an opt-out box. (For some kinds of businesses, for example financial institutions, this is required by law.)

Some libraries have a policy of destroying the checkout record when a book is returned—the best protection against disclosure. Most databases cannot use this technique, but it is a good reminder of a goal. There is a tendency among people not to throw anything away, including information. A policy of destroying records that are old or no longer needed protects privacy.

Both the public and private sectors need to have strong sanctions against employees who release information without authorization. A vice president of Bell Atlantic (now Verizon) stated one example of a good policy. Someone who gives out information on a consumer is fired.

Figure 2.2 summarizes privacy principles for personal data. Many government statements and laws, recommendations from many privacy organizations, and many business policies include various versions of these principles. There is wide variation in interpretation and implementation of the principles. For example, businesses and privacy advocates disagree about what information businesses "need" for customer service, marketing, and decision making. Thus these are very reasonable as principles or guidelines, but attempts to enforce them in laws are controversial. We discuss some of the controversy in Section 2.6.

1. Collect only the data needed.
2. Inform people when data about them are being collected, what is collected, and how it will be used. (Do not use invisible information gathering techniques without informing people.)
3. Offer a way for people to opt out from mailing lists and from transfer of their data to other parties.
4. Provide stronger protection for sensitive data. For example, use an opt-in policy for disclosure of medical data.
5. Keep data only as long as needed.
6. Maintain accuracy and security of data.
7. Provide a way for people to access and correct data stored about them.

Figure 2.2 Privacy Principles for Personal Data

2.4 More Privacy Risks

2.4.1 SOCIAL SECURITY NUMBERS AND NATIONAL ID SYSTEMS

The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.

—U.S. Privacy Protection Study Commission, 1977

With the advent of smart cards (cards containing a microprocessor and memory), there are increasing proposals for establishment of a computerized national identification card system. In one year alone, there were reports that the U.S. Postal Service, the IRS, the Defense Department, the National Security Agency, and NASA were among the agencies working on ID card plans. We review the background of Social Security cards and some problems with them, then consider national ID cards.

SOCIAL SECURITY NUMBERS

We use our Social Security number (SSN) for identification for numerous services, yet its insecurity compromises our privacy and exposes us to fraud. Because the SSN is an identifier in so many databases, someone who knows your name and has your SSN can, with varying degrees of ease, get access to your work and earnings history, credit report, driving record, bank account, and other personal data. The potential for both privacy invasion and fraud (particularly identity theft, which we discuss in Chapter 7) is clear. SSNs appear on public documents and other openly available forms. Property deeds,
which are public records, often require SSNs. SSNs are the ID numbers for students and faculty at many universities; the numbers appear on the face of the ID cards. The state of Virginia included SSNs on published lists of voters until a federal court ruled in 1993 that its policy of requiring the SSN for voter registration was unconstitutional.\textsuperscript{34} Some states use the SSN as the driver's license number. (In 1999, Congress repealed an earlier law requiring that SSNs be included on drivers' licenses. However, it requires that states collect the SSN on driver-license applications and renewals.) Some employers use the SSN as an identifier and put it on badges or give it out on request. Many companies, hospitals, and other organizations to which we might owe a bill request our SSN to run a credit check. Some routinely ask for an SSN and record it in their files, although they do not actually need it. Although the risks of careless treatment of SSNs is high, government and businesses have only recently begun to treat them with appropriate security.

The history of the SSN illustrates how the use of a national identification system grows. When SSNs first appeared in 1936, they were for the exclusive use of the Social Security program. The government assured the public at the time that it would not use the numbers for other purposes. Only a few years later, in 1943, President Roosevelt signed an executive order requiring federal agencies to use the SSN for new record systems. In 1961, the IRS began using it as the taxpayer ID. So now employers and others who must report to the IRS require it. In 1976, state and local tax, welfare, and motor vehicle departments received authority to use the SSN. A 1988 federal law requires that parents provide their SSN to get a birth certificate for a child. The IRS requires taxpayers to report the SSN for each child over one year old claimed as a dependent (or provide other proof of the existence of the child). A 1996 law authorized use of SSNs for occupational licenses and marriage licenses.\textsuperscript{35} Although we were promised otherwise, the SSN has become a general identification number.

SSNs have little-known but serious flaws for their role as a person's ID number in many databases. They are not unique, and they do not identify people. In some cases, Social Security Administration offices in different areas issued the same numbers to different people. In some cases, the same number was issued to different people with the same name. There are a few numbers used by thousands of people because the numbers were on sample cards in new wallets. The Social Security Administration estimates that 10 million people have more than one number. Social security cards are made of paper. They are easy to forge, but that hardly matters, because people are rarely asked for the card, and numbers are rarely verified. The Social Security Administration itself used to issue cards without verification of the information provided by the applicant. In 1991, the agency's commissioner told Congress that more than 60% of SSNs were based on unverified information. While criminals have little trouble creating false identities, innocent, honest people suffer arrest, fraud, destruction of credit rating, and so on, because of problems with the SSN.

Because of the security and identity problems with Social Security numbers, designers of databases with personal information should not use the SSN as the record identifier unless there is a compelling reason to do so. There are techniques for designing more secure ID number systems that distinguish between valid and invalid numbers, thus reducing fraud and errors.

NATIONAL ID SYSTEMS

Proposed national ID cards would contain (on a magnetic strip or in a smart-card memory) a person's name, photo, Social Security number, other identifying information, and health, tax, financial, citizenship, employment, or other data, depending on the specific proposal and the government agency advocating it. It might include biometric information such as fingerprints or a retina scan. In many proposals, the cards would also access a variety of databases containing such information. The cards would allow accurate verification of a person's identity when interacting with government agencies and for transactions such as credit card purchases, government payments, medical treatment, and banking transactions.\textsuperscript{60}

Advocates of a national ID card describe several benefits. You would need the actual card, not just a number, to verify identity. The cards would be harder to forge than Social Security cards. A person would need to carry only one card, rather than separate cards for various services, as we do now. The authentication of identity would help reduce fraud both in private credit card transactions and in government benefit programs. Use of ID cards for verifying work eligibility would prevent people from working in the U.S. illegally. Criminals and terrorists would be easier to track and identify.

Opponents to these proposals argue that national ID cards are profound threats to freedom and privacy. "Your papers, please" is a demand associated with police states and dictatorships. In Germany under the Nazis, identification papers included the person's religion, making it easy to enforce restrictions on and imprisonment of Jews. Under the infamous pass laws of South Africa, people carried passes, or identification papers, that categorized them by race and controlled where they could live and work. Smart cards, with the large amount of personal information they can carry or access in national databases, have even more potential for abuse. Most people might not have access to the machinery that reads the cards; thus they would not always know what information they are giving others about themselves.

For several years in the 1990s, anti-immigration sentiment in the U.S. provided the most support for a national ID card. Consider the program to prevent illegal immigrants (or legal immigrants without work permits) from working in the United States. Every time any person applied for a job, the prospective employer would have to verify the person's right to work by checking with the Immigration and Naturalization Service (INS) database. For the scheme to succeed, each person would need a "fraud-proof" ID card. The immediate threat of such a system is the loss of liberty to work. "It is absolutely unprecedented," said congressman Steve Chabot, "to say that the government must grant affirmative permission every time any employee is hired."\textsuperscript{61} In a country with an active economy and as large and mobile a population as the U.S., such centralized power over people's freedom to work would not be possible without modern computer
and communications networks. In addition to the reduction of freedom, a serious flaw in the INS database illustrates potential practical problems with any ID card linked to a national database: It is riddled with errors. In experiments with the system, approval for 19% of (legal) workers was delayed for several weeks. Approximately 65 million people in the U.S. change jobs or enter the workforce every year, so a 1% error rate would mean denial of work for 650,000 people each year.\footnote{62}

After the terrorist attacks on the World Trade Center and the Pentagon in 2001, proposals arose again for requiring everyone in the U.S. to carry a national ID card. Many of the terrorist hijackers in 2001 had government-issued ID cards, some valid, some fake. There is no indication that accurate identification would have stopped them. Of course, there are many circumstances in which a secure ID card system would help catch criminals and terrorists. It would not stop anthrax attacks by mail or many kinds of terrorist attacks in public places. As usual, we must consider the trade-offs and not expect an ID card to accomplish things it cannot do.

Peter Neumann and Lauren Weinstein warned of the many risks that arise from the databases and communication complexes that would support a national ID card system: "card readers, real-time networking, monitoring, data mining, aggregation, and probably artificially intelligent inference engines of questionable reliability. 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."\footnote{63}

In Chapter 4 we will see that a woman could not get her tax refund after records mistakenly indicated she had died. She would still have been able to get a new job, withdraw money from her bank account, pay her rent, send e-mail, and go to her doctor while she was resolving the problem with the tax agency. What if the worker verification database had used the tax records? Or what if a mistake cancelled the one ID card required for all these transactions? A critc of a proposal for a national identification card in Australia described the card as a "license to exist."\footnote{64} Is that description literal or a metaphor?

2.4.2 PERSONAL HEALTH AND MEDICAL INFORMATION

Whatever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be raised about, I will keep silence thereon, counting such things to be as sacred secrets.

—From the Hippocratic Oath

Our health and medical information is personal. Some is very sensitive: information about alcoholism, sexually transmitted diseases, psychiatric treatment, and suicide attempts. We might strongly desire to keep other health problems private even if they do not have negative social connotations.

Large medical care providers and hospitals are replacing paper medical records with computer databases. In Chapter 1, we mentioned that computerized records can improve medical care and cut costs. They can help protect privacy too. Studies have shown that, when a person is in a hospital, approximately 75-80 people may read his or her record (doctors, nurses, lab technicians, billing clerks, etc.). In such an environment, it is easy for unauthorized people to see a paper record, and it is easy for people to read parts of it that they do not need to see. Various database-access controls for computerized records (some described in Section 2.5) increase a patient's privacy. On the other hand, many kinds of medical information in databases and on the Web face the same privacy risks as other personal data.

Marketers love medical information. Merromail, the mailing-list broker, sold lists of people with specific diseases, such as diabetes and angina, to the pharmaceutical industry. Merromail said it had obtained the health information it sold from voluntary responses to ads and questionnaires. Large drug companies have bought other companies that sell prescription drugs to consumers mainly to gain access to the customer lists.\footnote{65} The huge burst in growth of the World Wide Web included medical Web sites sponsored by a variety of organizations and businesses. According to a critical review of such sites, some do not follow their stated privacy policies and some provide customer information, including e-mail addresses, to advertisers.

Patients sell prescriptions and check results of lab tests on the Web. Patients correspond with doctors by e-mail. These are great conveniences that can lower medical costs and improve medical care, but they open up new risks of leaks. For example, it is very easy to send e-mail to the wrong place, and one HMO did. It accidentally sent several hundred doctor-to-patient e-mail messages to 17 patients who were not supposed to get them. Some of the messages discussed personal medical details and included patients' addresses and telephone numbers.

Aside from marketing and technology, two economic factors diminish our control over our medical records: Most of us do not pay directly for our medical care, and we get care from large medical organizations rather than individual, private doctors. We waive confidentiality of our medical records for insurance payments. The insurer needs access to the records to verify eligibility and amounts of payments and to check for fraud (by patients or doctors). The anonymity and impersonal nature of a system of third-party payers (e.g., insurance companies or government) make it an inviting target for fraud. (One father/son team collected $16 million in Medicaid claims for nearly 400,000 phony medical visits.\footnote{66} Preventing and detecting fraud requires access to medical and personal information about patients.

Because medical records can be available to insurance companies, employers, and government agencies, many people take measures to keep information out of their records. Some pay for certain medical services themselves, even if the treatment would be covered by insurance. They go to a different physician to keep the record entirely separate from insurance-paid medical care.\footnote{67} Psychiatric patients often pay cash and ask doctors not to keep notes of their sessions. When patients worry about the privacy of medical