CHAPTER

5

Privacy and Cyberspace

Of all the ethical issues associated with the use of cybertechnology, perhaps none has received more media attention than concern about the loss of personal privacy. In this chapter, we examine issues involving privacy and cybertechnology by asking the following questions:

- How are privacy concerns generated by the use of cybertechnology different from privacy issues raised by earlier technologies?
- What, exactly, is personal privacy, and why is it valued?
- How do computerized techniques used to gather and collect information, such as Internet "cookies" and radio frequency identification (RFID) technology, raise concerns for personal privacy?
- How do the transfer and exchange of personal information across and between databases, carried out in computerized merging and matching operations, threaten personal privacy?
- How do tools used to "mine" personal data exacerbate existing privacy concerns involving cybertechnology?
- Can personal information we disclose to friends in social networking services (SNS), such as Facebook and Twitter, be used in ways that threaten our privacy?
- How do the use of Internet search engines and the availability of online public records contribute to the problem of protecting "privacy in public"?
- Do privacy-enhancing tools provide Internet users with adequate protection for their online personal information?
- Are current privacy laws and data protection schemes adequate?

Concerns about privacy can affect many aspects of an individual's life—from commerce to healthcare to work to recreation. For example, we speak of consumer privacy, medical and healthcare privacy, employee and workplace privacy, and so forth. Unfortunately, we cannot examine all of these categories of privacy in a single chapter. So we will have to postpone our analysis of certain kinds of privacy issues until later chapters in the book. For example, we will examine some ways that medical/genetic privacy issues are aggravated by cybertechnology in our discussion of bioinformatics in Chapter 12, and

we will examine some particular employee/workplace privacy issues affected by the use of cybertechnology in our discussion of workplace surveillance and employee monitoring in Chapter 10. Some cyber-related privacy concerns that conflict with cybersecurity issues and national security interests will be examined in Chapter 6, where privacy-related concerns affecting "cloud computing" are also considered. In our discussion of emerging and converging technologies in Chapter 12, we examine some issues that affect a relatively new category of privacy called "location privacy," which arise because of the use of embedded chips, RFID technology, and global positioning systems (GPS).

Although some cyber-related privacy concerns are specific to one or more spheres or sectors—i.e., employment, healthcare, and so forth—others cut across multiple dimensions of our lives, affecting virtually all persons regardless of their employment or health status. The privacy issues involving cybertechnology examined in this chapter affect each of us, whether or not we have ever owned or even used a networked computer. Consider that in carrying out many of our day-to-day activities, we supply information to organizations that use computers to record, store, and exchange those data. These activities can include information we provide in filling out various forms, or they can include information acquired from our commercial transactions in a bank or a store. Also consider that many people now engage in online commerce activities, and this raises some additional consumer-related privacy worries. But users who navigate the Web solely for recreational purposes are also at risk with respect to their privacy. For example, personal data about one's interests and preferences can be acquired by organizations and by individuals whose need for this information is not always obvious. Furthermore, personal data about us collected via our online activities and transactions can then be sold to third parties.

Also consider that applications such as Google Street View (a feature of Google Earth and Google Maps) make use of satellite cameras and GPS software that enable Internet users to zoom in on your house or place of employment and potentially record information about you. Additionally, closed circuit television cameras (CCTVs) located in public places and in shopping malls record many of your daily movements as you casually stroll through those environments. So even if you have never used a computer, cell phone, (Internet-enabled) electronic device, etc., your privacy is threatened in ways that were not possible in the past.

In this chapter, we examine a wide range of privacy concerns affecting the day-to-day activities of ordinary individuals carried out in both online and offline contexts. We also note, however, that cybertechnology is not the first technology to threaten personal privacy. We begin by looking at some ways to distinguish current issues associated with cybertechnology from privacy concerns involving earlier technologies.

▶ 5.1 ARE PRIVACY CONCERNS ASSOCIATED WITH CYBERTECHNOLOGY UNIQUE OR SPECIAL?

Concerns about personal privacy existed long before the advent of computers and cybertechnology. Prior to the information era, for example, technologies such as the camera and the telephone presented challenges for privacy. So we can ask: what, if anything, is special about the privacy concerns that are associated with cybertechnology?

Consider the impact that changes involving this technology have had on privacy with respect to the

- *amount* of personal information that can be collect,
- *speed* at which personal information can be transmitted,
- *duration* of time that the information can be retained,
- *kind* of information that can be acquired and exchanged.

Cybertechnology makes it possible to collect and store much more information about individuals than was possible in the precomputer era. The *amount* of personal information that could be collected in the precomputer era was determined by practical considerations, such as the physical space required to store the data and the time and difficulty involved in collecting the data. Today, of course, digitized information that can be stored electronically in computer databases takes up very little storage space and can be collected with relative ease.

Consider the *speed* at which information is exchanged and transferred between databases. At one time, records had to be physically transported between filing destinations; the time it took to move them depended upon the transportation systems—e.g., motor vehicles, trains, airplanes, and so forth—that carried the records. Now, of course, records can be transferred between electronic databases in milliseconds through wireless technologies, high-speed cable lines, or even ordinary telephone lines.

With so much information being collected and transferred so rapidly, many have expressed concerns about its accuracy as well as the difficulties in tracking down and correcting any inaccuracies that might have been transferred. In an interview conducted for the BBC TV series *The Machine that Changed the World*, Harvard law professor Arthur Miller points out that trying to correct such information is like "chasing a greased pig"—you may get your hands on the pig, but it is very difficult to keep the pig firmly in your grip.[1] Although issues concerning the accuracy of personal information are clearly distinguishable from those concerning privacy *per se*, accuracy issues are frequently associated with privacy issues, and both are impacted by cybertechnology.

Also, consider the *duration* of information—that is, how long information can be kept. Before the information era, information was manually recorded and stored in file cabinets and then in large physical repositories; it is unlikely that report cards my parents received as high school students still exist somewhere as physical records in file cabinets, for at that time, report cards were not computerized but instead existed, literally, as ink marks on paper. But the report cards my daughter received when she was a high school student were both generated and stored using computer technology. As an electronic record, her report card can be kept indefinitely, and the grades she received as a high school student (as well as the grades she received in elementary school and in college) can follow her throughout her life.

In the past, practices involving the retention of personal data were perhaps more "forgiving." Because of practical limitations, such as physical storage space, that affected how long personal data could be kept on file, much of the personal information collected and stored had to be destroyed after a certain number of years. Since information could not be archived indefinitely, people with blemished records sometimes had the opportunity to start over again by physically relocating. Today, however, one's electronic dossier would likely follow, making it very difficult, if not impossible, for that person to start over

with a clean slate. We can argue whether the current means of data retention is a good thing, but it is difficult to dispute the claim that now, because of cybertechnology, most of us have what Arthur Miller calls a "womb-to-tomb dossier."

Cybertechnology has also generated privacy concerns because of the *kind* of personal information that can now be collected. For example, every time you engage in an electronic transaction, such as making a purchase with a credit card or withdrawing money from an ATM, transactional information is collected and stored in several computer databases; this information can then be transferred electronically across commercial networks to agencies that request it. Personal information, retrieved from transactional information that is stored in computer databases, has been used to construct electronic dossiers containing detailed information about an individual's commercial transactions, including purchases made and places traveled—information that can reveal patterns in a person's preferences and habits.

Additionally, we should note that cybertechnology raises privacy concerns because of the myriad ways in which it enables our personal information to be *manipulated* (e.g., merged, matched, and "mined") once it has been collected. For example, unrelated pieces of information about us that reside in separate databases can be *merged* together to construct electronic personal dossiers or profiles. Also, information about us included in one database can be *matched* against records in other databases that contain information about us. Furthermore, our personal information can be *mined* (from databases, as well as from our activities on the Web) to reveal patterns in our behavior that would have been very difficult to discern in the precomputer era. (We examine controversies associated with data merging, matching, and mining practices in Sections 5.5 and 5.6.) Of course, our personal data could have been, and in some instances was, manipulated in the precomputer era as well. But there were practical limitations to the amount of information merging, matching, and mining that could be done manually by humans.

Although the privacy concerns that we now associate with cybertechnology may not be totally new, or even altogether different in kind, from those we associate with earlier technologies, few would dispute the claim that cybertechnology has exacerbated them. In Sections 5.4–5.7, we examine specific uses of cybertechnology that raise concerns for personal privacy. First, however, we examine the concept of personal privacy to better understand what privacy is and why we value it.

▶ 5.2 WHAT IS PERSONAL PRIVACY?

Although many definitions of privacy have been put forth, there is no universally agreed upon definition of this concept. To illustrate this point, consider some of the metaphors that are typically associated with privacy. Sometimes we speak of privacy as something that can be *lost* or *diminished*, suggesting that privacy can be understood in terms of a repository of personal information that can be either diminished altogether or gradually eroded. Contrast this view with descriptions of privacy as something that can be *intruded upon* or *invaded*, where privacy can be understood in terms of a spatial metaphor, such as a zone, that deserves protection. Alternatively, privacy is sometimes described as something that can be violated or breached, when we think of it in terms of either a right or an interest that deserves legal protection. Because of these different conceptions of privacy, we will see that it is useful to distinguish between the notions of one's having

privacy (in a descriptive sense) and one's having a (normative) right to privacy. We will say more about this distinction in Section 5.2.4.

Privacy analysts have pointed out that in the United States, the meaning of privacy has evolved since the eighteenth century. Initially, privacy was understood in terms of freedom from (physical) intrusion. Later it became associated with freedom from interference into one's personal affairs, including one's ability to make decisions freely. Most recently, privacy has come to be closely identified with concerns affecting access to and control of personal information—a view that is also referred to as "informational privacy." Although the main emphasis in this chapter is on informational privacy, we also briefly examine the other two views.

5.2.1 Accessibility Privacy: Freedom from Unwarranted Intrusion

In a seminal paper on privacy, Samuel Warren and Louis Brandeis suggested that privacy could be understood as "being let alone" or "being free from intrusion." Appearing in the *Harvard Law Review* in 1890, the Warren and Brandeis article made the first explicit reference to privacy as a legal right in the United States. Many Americans are astonished to find out that there is no explicit mention of privacy in either the Constitution or its first ten amendments, the Bill of Rights. However, some legal scholars believe that a right to privacy can be inferred from the Fourth Amendment, which protects citizens against unreasonable searches and seizures of personal affects (i.e., papers, artifacts, etc.) by the government. Many legal scholars believe that the Fourth Amendment also provides legal grounds for a right to privacy protection from nongovernmental intrusion as well.

Warren and Brandeis also suggested that our legal right to privacy is grounded in our "right to inviolate personality." In part, they were responding to a certain use of a new technology—not the computer, of course, but rather the camera—which had begun to threaten individual privacy in new ways.[2] Photographs of people began to appear in newspapers, for example, in gossip columns, along with stories that were defamatory and sometimes even false. Warren and Brandeis believed that individuals have a (legal) right not be intruded upon in this manner. Because this definition of privacy as freedom from unwarranted intrusion focuses on the harm that can be caused through physical access to a person or to a person's possessions, Judith DeCew (1997) and others have described this view as *accessibility privacy*.

5.2.2 Decisional Privacy: Freedom from Interference in One's Personal Affairs

Privacy is also sometimes conceived of as freedom from interference in one's personal choices, plans, and decisions; some refer to this view as *decisional privacy*. This kind of privacy has also been associated with reproductive technologies having to do with contraception. In *Griswold v. Connecticut* (1965), the court ruled that a person's right to get counseling about contraceptive techniques could not be denied by state laws. The view of privacy as freedom from external interference into one's personal affairs has since been appealed to in legal arguments in a series of controversial court cases, such as those involving abortion and euthanasia. For example, this view of privacy was appealed to in the landmark Supreme Court decision on abortion (*Roe v. Wade* 1973), as well as in a state court's decision involving Karen Ann Quinlan's right to be removed from life-support systems and thus her "right to die."[3] Because it focuses on one's right not to be

interfered with, decisional privacy can be distinguished from both accessibility privacy and informational privacy.

5.2.3 Informational Privacy: Control over the Flow of Personal Information

Because of the increasing use of technology to gather and exchange personal information, many contemporary analysts view privacy in connection with one's ability to restrict access to and control the flow of one's personal information. Privacy concerns are now often framed in terms of questions such as: Who should have access to one's personal information? To what extent can individuals control the ways in which information about them can be gathered, stored, mined, combined, recombined, exchanged, and sold? These are our primary concerns in this chapter, where we focus on *informational privacy*.

Table 5.1 summarizes the three views of privacy.

5.2.4 A Comprehensive Account of Privacy

James Moor (2000) has introduced an account of privacy that incorporates important elements of the nonintrusion, noninterference, and informational views of privacy. According to Moor,

> An individual [has] privacy *in a situation* with regard to others if and only if in that situation the individual [is] *protected from intrusion*, *interference*, and *information access* by others.[4]

An important element in this definition is Moor's notion of "situation," which he deliberately leaves broad so that it can apply to a range of contexts, or zones, that can be "declared private." For example, a situation can be an "activity" or a "relationship," or it can be the "storage and access of information" in a computer.

Central to Moor's theory is a distinction between *naturally private* and *normatively private* situations, enabling us to differentiate between the conditions required for (a) having privacy and (b) having a right to privacy. This distinction, in turn, enables us to differentiate between a loss of privacy and a violation of privacy. In a naturally private situation, individuals are protected from access and interference from others by natural means, for example, physical boundaries such as those one enjoys while hiking alone in the woods. In this case, privacy can be *lost* but not *violated*, because there are no norms—conventional, legal, or ethical—according to which one has a *right*, or even an expectation, to be protected. In a normatively private situation, on the other hand, individuals are protected by conventional norms (e.g., formal laws and informal policies) because they involve certain kinds of zones or contexts that we have determined to need

TABLE 5.1 Three Views of Privacy

Accessibility privacy	Privacy is defined as one's physically being let alone, or being free from intrusion into one's physical space.
Decisional privacy	Privacy is defined as freedom from interference in one's choices and decisions.
Informational privacy	Privacy is defined as control over the flow of one's personal information, including the transfer and exchange of that information.

normative protection. The following two scenarios will help us to differentiate between normative and natural (or descriptive) privacy.

▶ **SCENARIO 5–1:** Descriptive Privacy

Mary arrives in the computer lab at her university at 11:00 PM to work on a paper that is due the next day. No one else is in lab at the time that Mary arrives there, and no one enters the lab until 11:45 PM, when Tom—the computer lab coordinator—returns to close the lab for the evening. As Tom enters, he sees Mary typing on one of the desktop computers in the lab. Mary seems startled as she looks up from her computer and discovers that Tom is gazing at her. ■

Did Mary lose her privacy when Tom entered the lab and saw her? Was her privacy violated? Before Tom noticed her in the lab, we could say that Mary had privacy in the descriptive, or natural, sense of the term because no one was physically observing her while she was in the lab. When Tom entered and noticed that Mary was typing on a computer, Mary lost her natural (or descriptive) privacy in that situation. However, we should not infer that her privacy was violated in this incident, because a university's computer lab is not the kind of situation or zone that is declared normatively private and thus protected.

▶ **SCENARIO 5–2:** Normative Privacy

Tom decides to follow Mary, from a distance, as she leaves the computer lab to return to her (off-campus) apartment. He carefully follows her to the apartment building, and then stealthily follows Mary up the stairway to the corridor leading to her apartment. Once Mary is safely inside her apartment, Tom peeps through a keyhole in the door. He observes Mary as she interacts with her laptop computer in her apartment. ■

Has Mary's privacy been violated in this scenario? In both scenarios, Tom observes Mary interacting with a computer. In the first scenario, the observation occurred in a public place. There, Mary may have lost some privacy in a descriptive or natural sense, but she had no expectation of preserving her privacy in that particular situation. In the second scenario, Mary not only lost her privacy but her privacy was violated as well, because apartments are examples of zones or "situations" that we, as a society, have declared normatively private.

We have explicit rules governing these situations with respect to privacy protection. Note that it was not merely the fact that Tom had observed Mary's interactions with a computer that resulted in her privacy being violated in the second scenario. Rather, it was because Tom had observed her doing this in a normatively protected situation. So, there was nothing in the information *per se* that Tom acquired about Mary that threatened her privacy; it was the situation or context in which information about Mary was acquired that caused her privacy to be violated in the second scenario.

5.2.5 Privacy as "Contextual Integrity"

We have seen the important role that a situation, or context, plays in Moor's privacy theory. But some critics argue that the meaning of a situation or context is either too broad or too vague. Helen Nissenbaum (2004a, 2010) elaborates on the notion of a

context in her model of privacy as "contextual integrity," where she links adequate privacy protection to "norms of specific contexts." She notes that the things we do, including the transactions and events that occur in our daily lives, all take place in some context or other. In her scheme, contexts include "spheres of life" such as education, politics, the marketplace, and so forth.

Nissenbaum's privacy framework requires that the processes used in gathering and disseminating information (a) are "appropriate to a particular context" and (b) comply with norms that govern the flow of personal information in a given context.[5] She refers to these two types of informational norms as follows:

1. Norms of appropriateness.
2. Norms of distribution.

Whereas norms of appropriateness determine whether a given type of personal information is either appropriate or inappropriate to divulge within a particular context, norms of distribution restrict or limit the flow of information within and across contexts. When either norm has been "breached," a violation of privacy occurs; conversely, the contextual integrity of the flow of personal information is maintained when both kinds of norms are "respected."[6]

As in the case of Moor's privacy model, Nissenbaum's theory demonstrates why we must always attend to the context in which information flows, and not to the nature of the information itself, in determining whether normative protection is needed. To illustrate some of the nuances in her framework of privacy as contextual integrity, consider the following scenario in which a professor collects information about students in his seminar.

▶ SCENARIO 5–3: Preserving Contextual Integrity in a University Seminar

Professor Roberts teaches a seminar on social issues in computing to upper division undergraduate students at his university. Approximately half of the students who enroll in his seminar each semester are computer science (CS) students, whereas the other half are students majoring in humanities, business, etc. At the first class meeting for each seminar, Professor Roberts asks students to fill out an index card on which they include information about their major, their year of study (junior, senior, etc.), the names of any previous CS courses they may have taken (if they are non-CS majors), their preferred e-mail address, and what they hope to acquire from the seminar. Professor Roberts then records this information in his electronic grade book. ■

Has Professor Roberts done anything wrong in requesting and collecting this information? For the most part, it is information that he could have gathered from the registrar's office at his university—e.g., information about which CS courses the students took, and so forth. But Roberts finds it much more convenient to collect information in the classroom, and he informs the students that he uses that information in determining which kinds of assignments he will decide to give to the class in general, and which kinds of criteria he will use to assign students to various group projects.

Because Professor Roberts has informed the students about how the information they provided to him will be used in the context of the classroom, and because the students have consented to give him the information, no privacy violation seems to have occurred. In fact, the process used by Professor Roberts satisfies the conditions for Nissenbaum's norm of appropriateness with respect to contextual integrity.

Next, suppose that Professor Roberts has lunch a few weeks later with a former student of his, Phil, who recently graduated and now has a job as a software engineer for a publishing company. Phil's company plans to release its first issue of a new magazine aimed at recent CS graduates, and it has launched an advertising campaign designed to attract undergraduate CS majors who will soon graduate. Phil asks Professor Roberts for the names of the CS majors in the seminar he is teaching. Professor Roberts is initially inclined to identify some students that Phil would likely know from classes that he had taken the previous year at the university. But should Professor Roberts reveal those names to Phil?

If he did, Professor Roberts would violate the privacy norm of distribution within the context of the seminar he is teaching. Consider that the students gave information about themselves to Professor Roberts for use in the context of that seminar. While his use of that information for purposes of the seminar is context-appropriate, passing on (i.e., distributing) any of that information to Phil is not, because it would violate the integrity of that context. Even though the information about the students that Professor Roberts has collected is not highly sensitive or confidential information, it was given to him for use only in the context of the seminar he is teaching. Insofar as Professor Roberts uses the information in that context, he preserves its integrity. But if he elects to distribute the information outside that context, he violates its integrity and breaches the privacy of his students.

► 5.3 WHY IS PRIVACY IMPORTANT?

Of what value is privacy? Why does privacy matter, and why should we care about it? In 1999, Scott McNealy, then CEO of Sun Microsystems, uttered his now famous remark to a group of reporters: "You have zero privacy anyway. Get over it." Is the idea of personal privacy merely a relic of the past? Michael Froomkin (2000) and Simson Garfinkel (2000) both speak of the "death of privacy." But not everyone has conceded defeat in the battle over privacy. Some privacy advocates staunchly believe that we should be vigilant about retaining what little privacy we may still have. Others note that we do not appreciate the value of privacy until we lose it, and by then it is usually too late. They point out that once privacy has been lost, it is difficult, if not impossible, to get back. So perhaps we should heed their warnings and try to protect privacy to the degree that we can.

We might also question whether the current privacy debate needs to be better understood in terms of differences that reflect generational attitudes. For many so-called Millennials, who are now college-aged, privacy does not always seem to be of paramount importance. Most Millennials, as well as many members of Generations X and Y, seem all too eager to share their personal information widely on social networking services such as Facebook, and many also seem willing to post "away messages" on AIM or Skype that disclose their whereabouts at a given moment to a wide range of people. But for many older Americans, including Baby Boomers, privacy is something that is generally still valued. So the relative importance of privacy may vary considerably among the generations; however, we will proceed on the assumption that privacy has value and thus is important.

Is privacy universally valued? Or is it valued mainly in Western, industrialized societies where greater importance is placed on the individual? It has been argued that

some non-Western nations and cultures do not value individual privacy as much as we do in the West. Alan Westin believes that countries with strong democratic political institutions consider privacy more important than do less democratic ones.[7] Nations such as Singapore and the People's Republic of China seem to place less importance on individual privacy and greater significance on broader social values, which are perceived to benefit the state's community objectives. Even in countries such as Israel, with strong democratic systems but an even stronger priority for national security, individual privacy may not be as important a value as it is in most democratic nations. So, even though privacy has at least some universal appeal, it is not valued to the same degree in all nations and cultures. As a result, it may be difficult to get universal agreement on privacy laws and policies in cyberspace.

5.3.1 Is Privacy an Intrinsic Value?

Is privacy something that is valued for its own sake—that is, does it have intrinsic value? Or is it valued as a means to an end, in which case it has only instrumental worth? Recall our discussion of intrinsic and instrumental values in Chapter 2. There we saw that happiness has intrinsic value because it is desired for its own sake. Money, on the other hand, has instrumental value since it is desired as a means to some further end or ends.

While few would argue that privacy is an intrinsic value, desired for its own sake, others, including Charles Fried (1990), argue that privacy is not merely an instrumental value or instrumental good. Fried suggests that unlike most instrumental values that are simply one means among others for achieving a desired end, privacy is also essential, that is, necessary to achieve some important human ends, such as trust and friendship. We tend to associate intrinsic values with necessary conditions and instrumental values with contingent, or nonnecessary conditions; so while privacy is instrumental in that it is a means to certain human ends, Fried argues that it is also a necessary condition for achieving those ends.

Although agreeing with Fried's claim that privacy is more than merely an instrumental value, James Moor (2004) takes a different approach to illustrate this point. Like Fried, Moor argues that privacy itself is not an intrinsic value. Moor believes that privacy is an articulation, or "expression" of the "core value" *security*, which in turn is essential across cultures, for human flourishing. (We examine the concept of security as it relates to privacy in Chapter 6.) And like Fried, Moor shows why privacy is necessary to achieve certain ends. Moor further suggests that as information technology insinuates itself more and more into our everyday lives, privacy becomes increasingly important for expressing (the core value) security.

Does privacy play a key role in "promoting human well-being," as Richard Spinello (2010) claims? Perhaps one way it does is by serving as a "shield" that protects us from interference. Judith DeCew (2006), who believes that the value of privacy lies in the "freedom and independence" it provides for us, argues that privacy shields us from "pressures that preclude self-expression and the development of relationships."[8] She claims that privacy also acts as a shield by protecting us from coercion and the "pressure to conform." In her view, the loss of privacy leaves us vulnerable and threatened because we are likely to become more conformist and less individualistic.

5.3.2 Privacy as a Social Value

Based on the insights of DeCew and others, one might infer that privacy is a value that simply benefits individuals. However, some authors have pointed out the social value that privacy also provides, noting that privacy is essential for democracy. Priscilla Regan (1995) points out that we often frame debates over privacy simply in terms of how to balance privacy interests as individual goods against interests involving the larger social good; in such debates, Regan believes, interests benefiting the social good will generally override concerns regarding individual privacy. If, however, privacy is understood as not solely concerned with individual good but as contributing to the broader social good, then in debates involving the balancing of competing values, individual privacy might have a greater chance of receiving equal consideration.

Since privacy can be of value for greater social goods, such as democracy, as well as for individual autonomy and choice, it would seem that it is important and worth protecting. But privacy is increasingly threatened by new cyber and cyber-related technologies. In Sections 5.4–5.6, we examine how privacy is threatened by three different kinds of practices that use cybertechnology:

a. *Data gathering* techniques used to collect and record personal information, often without the knowledge and consent of users.

b. *Data exchange* techniques used to transfer and exchange personal data across and between computer databases, typically without the knowledge and consent of users.

c. *Data mining* techniques used to search large databases in order to generate consumer profiles based on the behavioral patterns of certain groups.

▶ 5.4 GATHERING PERSONAL DATA: MONITORING, RECORDING, AND TRACKING TECHNIQUES

Collecting and recording data about people is hardly new. Since the Roman era, and possibly before then, governments have collected and recorded census information. Not all data gathering and data recording practices have caused controversy about privacy. However, cybertechnology makes it possible to collect data about individuals without their knowledge and consent. In this section, we examine some controversial ways in which cybertechnology is used to gather and record personal data, as well as to monitor and track the activities and locations of individuals.

5.4.1 "Dataveillance" Techniques

Some believe that the greatest threat posed to personal privacy by cybertechnology lies in its capacity for surveillance and monitoring. Others worry less about the monitoring *per se* and more about the vast amounts of transactional data recorded using cybertechnology. Roger Clarke uses the term *dataveillance* to capture both the surveillance (data monitoring) and data recording techniques made possible by computer technology.[9] There are, then, two distinct controversies about dataveillance: one having to do with surveillance as a form of data monitoring, and one having to do with the recording and

processing of data once the data are collected. We examine both controversies, beginning with a look at data monitoring aspects of surveillance.

First, we should note the obvious, but relevant, point that privacy threats associated with surveillance are by no means peculiar to cybertechnology. Long before the advent of cybertechnology, individuals (e.g., private investigators and stalkers) as well as organizations, including governmental agencies all over the world, have used both electronic and nonelectronic devices to monitor individuals and groups.

Telephone conversations have been subject to government surveillance by wiretapping, but phone conversations have also been monitored in the private sector as well; for example, telephone conversations between consumers and businesses are frequently monitored, sometimes without the knowledge and consent of the consumers who are party to them. So surveillance is neither a recent concern nor one that should be associated exclusively with the use of cybertechnology to monitor and record an individual's online activities. However, surveillance has clearly been exacerbated by cybertechnology. Consider that video cameras now monitor consumers' movements while they shop at retail stores, and scanning devices used by "intelligent highway vehicle systems," such as E-ZPass, subject motorists to a type of surveillance while they drive through tollbooths. And Sue Halpern (2011) notes that approximately 500 companies are now able to monitor and track all of our movements online.

In the past, it was not uncommon for companies to hire individuals to monitor the performance of employees in the workplace. Now, however, there are "invisible supervisors," that is, computers, that can continuously monitor the activities of employees around the clock without failing to record a single activity of the employee. We will examine workplace monitoring in detail, including some arguments that have been used to defend and to denounce computerized monitoring, in Chapter 10, where we consider some impacts that cybertechnology has for the contemporary workplace. In the remainder of this section, we consider surveillance techniques that involve non-workplace-related monitoring and recording of personal data in both off- and online activities.

Although users may not always realize that they are under surveillance, their online activities are tracked by Web site owners and operators to determine how frequently users visit their sites and to draw conclusions about the preferences users show while accessing their sites. We next consider some controversies associated with a type of online surveillance technology known as *cookies*.

5.4.2 Internet Cookies

Cookies are files that Web sites send to and retrieve from the computer systems of Web users, enabling Web site owners to collect information about an individual's online browsing preferences whenever a person visits a Web site. The use of cookies by Web site owners and operators has generated considerable controversy, in large part because of the novel way that information about Web users is collected and stored. Data recorded about the user are stored on a file placed on the hard drive of the user's computer system; this information can then be retrieved from the user's system and resubmitted to a Web site the next time the user accesses that site.

Those who defend the use of cookies tend to be owners and operators of Web sites. Proprietors of these sites maintain that they are performing a service for repeat users of a Web site by customizing the user's means of information retrieval. They also point out

that, because of cookies, they are able to provide a user with a list of preferences for future visits to that Web site. Privacy advocates, on the other hand, see the matter quite differently. They argue that activities involving the monitoring and recording of an individual's activities while visiting a Web site and the subsequent downloading of that information onto a user's computer (without informing the user) clearly cross the privacy line. Some privacy advocates also point out that information gathered about a user via cookies can eventually be acquired by online advertising agencies, which can then target that user for online ads.

Initially, you might feel a sense of relief in discovering that, generally, owners and operators of one Web site cannot access cookies-related information pertaining to a user's activities on another Web site. However, information about a user's activities on different Web sites can, under certain circumstances, be compiled and aggregated by online advertising agencies such as DoubleClick that pay to place advertisements on Web sites. DoubleClick can also acquire information about you from data that it retrieves from other Web sites you have visited and where DoubleClick advertises. The information can then be combined and cross-referenced in ways that enable a marketing profile of that user's online activities to be constructed and used in more direct advertisements.

Several privacy advocates have argued that because cookies technology involves monitoring and recording a user's activities while visiting Web sites (without the user's knowledge and consent) as well as the subsequent downloading of that information onto a user's computer system, it violates the user's privacy. To assist Internet users in their concerns about cookies, a number of privacy-enhancing tools, which are discussed in detail in Section 5.8, are available. In most Web browsers, users now also have an option to disable cookies, so that they can either opt-in or opt-out of cookies, assuming that they (i) are aware of cookies technology and (ii) know how to enable/disable that technology on their Web browsers. However, some Web sites will not grant users access unless they accept cookies.

Many privacy advocates object to the fact that the default status for most Web browsers is such that cookies will automatically be accepted unless explicitly overridden by the user. As we noted above, cookies technology involves downloading the information it gathers about users onto the user's computer system. So, cookies technology also raises concerns involving encroachment or intrusion into a user's physical space as well as privacy concerns regarding the clandestine method used to gather data about users who visit Web sites.

5.4.3 RFID Technology

Another mode of surveillance made possible by cybertechnology involves the use of RFID technology. In its simplest form, RFID technology consists of a tag (microchip) and a reader. The tag has an electronic circuit, which stores data, and an antenna that broadcasts data by radio waves in response to a signal from a reader. The reader also contains an antenna that receives the radio signal, and it has a demodulator that transforms the analog radio information into suitable data for any computer processing that will be done (Lockton and Rosenberg 2005).

Although the commercial use of RFIDs was intended mainly for the unique identification of real-world objects (e.g., items sold in supermarkets), the tags can

also be used to monitor those objects after they are sold. For example, Helen Nissenbaum notes that prior to the use of RFID tags

> . . . customers could assume that sales assistants, store managers, or company leaders recorded point-of-sale information. RFID tags extend the duration of the relationships, making available to . . . others a range of information about customers that was not previously available.[10]

In one sense, the use of these tags in inventory control would seem uncontroversial. For example, Simson Garfinkel (2002) notes that a company such as Playtex could place an RFID tag in each bra to make sure that shipments of bras headed for Asia are not diverted to New York. He also points out, however, that a man with a handheld (RFID) reader in his pocket who is standing next to a woman wearing such a bra can learn the make and size of her bra. Additionally, and perhaps more controversially, RFID technology can be used for tracking the owners of the items that have these tags. So, on the one hand, RFID transponders in the form of "smart labels" make it much easier to track inventory and protect goods from theft or imitation. On the other hand, these tags pose a significant threat to individual privacy. Critics of this technology, which include organizations such as the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU), worry about the accumulation of RFID transaction data by RFID owners and how those data will be used in the future.

RFID technology is already widely used—as Garfinkel notes, it has been incorporated into everything from automobile keys to inventory control systems to passports. If you have an E-ZPass (or some other intelligent highway system) transponder in your car, for example, you are already carrying a wireless tag; E-ZPass uses the serial number to debit your account when your car passes through a tollbooth. Garfinkel notes that these tags now also appear in clothing.

Ranchers in the United States track cattle by implanting RFID tags in the animals' ears. In the future, major cities and municipalities might require RFID tags for pets; in Taiwan, owners of domesticated dogs are now required to have a microchip containing an RFID tag, which identifies the animal's owner and residence, inserted in their pet dog's ear. Policies requiring RFID tags for humans, especially for children and the elderly, may also be established in the near future. In the United States, some nursing homes now provide their patients with RFID bracelets. And chips (containing RFID technology) can be implanted in children so that they can be tracked if abducted; however, Alison Adam (2005) fears that we may come to rely too heavily on these technologies to care for children. Because RFID technology is now included in chips being embedded in humans, which enables them to be tracked, it has raised concerns for many privacy advocates.

In light of these and related privacy concerns, Garfinkel has proposed an "RFID Bill of Rights" to protect individuals and guide businesses that use RFID tags. In this scheme, individuals would have the right to (a) know whether products contain RFID tags, (b) have the tags removed or deactivated when they purchase products, (c) access the tag's stored data, and (d) know when, where, and why the tags are being read.

Like Internet cookies and other online data gathering and surveillance techniques, RFID clearly threatens individual privacy. But unlike surveillance concerns associated with cookies, which track a user's habits while visiting Web sites, RFID technology can be used to track an individual's location in the offline world. We examine some specific privacy and surveillance concerns affecting RFID in connection with "location privacy" and "pervasive surveillance" issues in Chapter 12 in our discussion of ambient intelligence.

5.4.4 Cybertechnology and Government Surveillance

So far, we have examined some surveillance techniques involving cybertechnology that are used mainly in the business and commercial sectors to monitor the activities of consumers and to record data about them. Another mode of surveillance that is also associated with cybertechnology involves governments and government agencies that monitor the activities of citizens, a practice that is sometimes referred to as "domestic spying." As already noted, this practice is not exactly new, but as the technologies used by governments to monitor their citizens' activities become more sophisticated, intrusive, and pervasive, the threats posed to privacy and civil liberties become exacerbated.

Some cybertechnologies, despite their initial objectives and intent, can facilitate government surveillance. Consider, for example, that cell phone companies in the United States are required by the Federal Communications Commission (FCC) to install a GPS locator chip, in compliance with an "enhanced 911 mandate," in all of the cell phones manufactured after December 2005. This technology, which assists 911 operators in emergencies, also enables any cell phone user to be tracked within 100 meters of his or her location. However, privacy advocates worry that this information can also be used by the government to spy on individuals.

Government agencies currently use a variety of technologies that enable them to intercept and read private e-mail messages. In Chapter 6, we will see that this practice, initiated by the George W. Bush administration to monitor e-mail between U.S. residents and people living outside the United States, has been controversial. And in Section 5.7.1, we will see why the U.S. government's decision to subpoena the records of online search requests made by users of search engines such as Google, which are recorded and archived in computer databases, has also been controversial. In Chapter 7, we describe in detail some of the specific technologies (such as Internet pen registers, keystroke monitoring, and biometric technologies) that have been used by government agencies in the United States to conduct surveillance on individuals. There, we will also see why these technologies, which have been used to combat terrorism and crime in cyberspace, have been controversial from the point of view of privacy and civil liberties.

While few would object to the desirable ends that increased security provides, we will see that many oppose the means—i.e., the specific technologies and programs supporting surveillance operations, as well as legislation such as the USA Patriot Act—that the U.S. government has used to achieve its objectives. In Chapter 7, we will see why the Patriot Act, enacted into law in October 2001 and renewed in March 2006, has been controversial from the point of view of civil liberties. Our purpose in this section has been to briefly describe how government surveillance of citizens illustrates one more way that cybertechnology both contributes to and enhances the ability of organizations to gather and record data about individuals.

In concluding this section, we note that plans are well underway for the construction of a government data center in Bluffdale, Utah, under the egis of the National Security Agency (NSA). It is estimated that this $2 billion center should be operational by September 2013. James Bamford (2012) notes that with the sophisticated tools and databases planned for this center, NSA will be able to "intercept, decipher, analyze, and store" vast amounts of the world's communications. He also points out that these communications and data may include "the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking

receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'" NSA's original charter was to conduct foreign surveillance; now, however, the agency's mission appears to have been broadened, as surveillance on U.S. citizens is also now conducted by NSA.

▶ 5.5 EXCHANGING PERSONAL DATA: MERGING AND MATCHING ELECTRONIC RECORDS

In the previous section, we examined ways in which personal data could be gathered using surveillance techniques and then recorded electronically in computer databases. Other tools have been devised to transfer and exchange those records across and between computer databases. Simply collecting and recording personal data, *per se*, might not seem terribly controversial if, for example, the data were never used, transferred, exchanged, combined, or recombined. Some would argue, however, that the mere collection of personal data is problematic from a privacy perspective, assuming that if data are being collected, there must be some motive or purpose for their collection. Of course, the reason, as many now realize, is that transactions involving the sale and exchange of personal data are a growing business.

Much of the personal data gathered electronically by one organization is later exchanged with other organizations; indeed, the very existence of certain institutions depends on the exchange and sale of personal information. Some privacy advocates believe that professional information gathering organizations, such as Equifax, Experion (formerly TRW), and Trans Union (credit reporting bureaus), as well as the Medical Information Bureau (MIB), violate the privacy of individuals because of the techniques they use to facilitate the exchange of personal information across and between databases. These techniques include computer merging and computer matching.

5.5.1 Merging Computerized Records

Few would dispute the claim that organizations, in both the public and the private sectors, have a legitimate need for information about individuals in order to make intelligent decisions concerning those individuals. For example, if you are applying for a credit card, it would be reasonable for the credit company to request information about you. However, few would also disagree with the claim that individuals should have a right to keep some personal information private. A crucial question, then, is: What kind of control can an individual expect to retain over the personal information that he or she has given to an organization? Can, for example, an individual expect that personal information provided to an organization for legitimate use in a specific context will remain within that organization? Or will it instead be exchanged with other organizations who can then combine or merge it with existing information?

Computer merging is the technique of extracting information from two or more unrelated databases that contain information about some individual or group of individuals, and then integrating that information into a composite file. It occurs whenever two or more disparate pieces of information contained in separate databases are combined. Consider the following sequence of events in which you voluntarily give information about yourself to three different organizations. First, you give information about your income and credit history to a lending institution in order to secure a loan.

You next give information about your age and medical history to an insurance company to purchase life insurance. You then give information about your views on certain social issues to a political organization you wish to join. Each of these organizations can be said to have a legitimate need for information to make certain decisions about you—insurance companies have a legitimate need to know about your age and medical history before agreeing to sell you life insurance, and lending institutions have a legitimate need to know about your income and credit history before agreeing to lend you money to purchase a house or a car. And insofar as you voluntarily give these organizations the information requested, no breach of your privacy has occurred.

Now suppose that without your knowledge and consent, information about you that resides in the insurance company's database is transferred and merged with information about you that resides in the lending institution's database or in the political organization's database. Even though you voluntarily gave certain information about yourself to three different organizations, and even though you voluntarily authorized each organization to have the information, it does not follow that you authorized any one organization to have some combination of that information.[11] When organizations merge information about you in a way that you did not specifically authorize, the "contextual integrity" of your information has been violated. (Recall Nissenbaum's criteria for preserving the contextual integrity of personal information, described in Section 5.2.5.)

Next, consider a case of computer merging involving DoubleClick, an online advertising company. In our discussion of cookies technology in the previous section, we described how DoubleClick was able to compile data from multiple Web sites on which it placed DoubleClick ads. If, for example, DoubleClick advertised on 1,000 Web sites, it could retrieve cookie files from any user who visited any of those sites and clicked on its ads. Thus, DoubleClick can compile and cross-reference cookies-related information in ways that individual Web site proprietors cannot. This, in turn, has caused concern among DoubleClick's critics, including privacy advocates.

▶ SCENARIO 5–4: Merging Personal Information in Unrelated Computer Databases

DoubleClick planned to purchase Abacus Direct Corporation, a database company, in late 1999. Abacus's databases contained not only records of consumer's catalogue purchases but also actual names and telephone numbers that had been collected by Abacus primarily from offline transactions. With this acquisition, DoubleClick could merge records in the Abacus database with its own database, which consisted of information gained primarily from Internet cookies files. And with its newly merged data, DoubleClick would have an information mosaic about individuals that included not merely anonymous and indirect information (such as IP addresses and ISP-related information) but also direct personal information. The Web profiles in DoubleClick's original database, gathered via cookies, included data about which Web sites that users (who are identified and tracked via an IP address) visit, how long they visit a particular site, and so on. That information would be able to be compared to and combined with explicit personal information (gathered offline and stored in Abacus's databases), including names, addresses, and phone numbers.[12] ■

The planned merger involving the two companies, which generated considerable controversy at the time, was canceled in January 2000, when DoubleClick was sued by a woman who complained that her right to privacy had been violated. The woman claimed that DoubleClick's business practices were deceptive, because the company had quietly reversed an earlier policy by which it provided businesses with only anonymous data

about Internet users (acquired from cookies files). Because of public pressure, DoubleClick backed off from its proposal to purchase Abacus, but many users were able to see for the first time the privacy threats that can result from merging electronic data. However, DoubleClick continued to function as an online advertising company, and in March 2008, it was acquired by Google. This acquisition has caused concerned for many privacy advocates, because Google integrates information gathered from cookies with its wide array of applications and services, which include Gmail, Google+, Google Chrome, and others. As Michael Zimmer (2008) notes, Google's ability to integrate this information provides the search engine company with a "powerful infrastructure of dataveillance" in which it can monitor and record users' online activities.

5.5.2 Matching Computerized Records

Computer matching is a variation of the technology used to merge computerized records. It involves cross-checking information in two or more unrelated databases to produce matching records, or "hits." In federal and state government applications, this technique has been used by various agencies and departments for the express purpose of creating a new file containing a list of potential law violators, as well as individuals who have actually broken the law or who are suspected of having broken the law.[13]

Consider a scenario in which you complete a series of forms for various federal and state government agencies, such as the Internal Revenue Service (IRS), your state government's motor vehicle registration department, or your local government's property tax assessment department. You supply the specific information requested and, in addition, you include general information requested on each form, such as your social security number and driver's license number, which can be used as identifiers in matching records about you that reside in multiple databases. The information is then electronically stored in the agencies' respective databases, and routine checks (matches) can be made against information (records) contained in those databases. For example, your property tax records can be matched against your federal tax records to see whether you own an expensive house but declared only a small income. Records in an IRS database of divorced or single fathers can be matched against a database containing records of mothers receiving welfare payments to generate a list of potential "deadbeat parents."

In filling out the various governmental forms, you agreed to give some information to each government agency. It is by no means clear, however, that you authorized information given to any one agency to be exchanged with other agencies. You had no say in the way information that you authorized for use in one context was subsequently used in another. Because of this contextual violation of personal information, some have argued that practices involving computerized matching of records containing personal data raise serious threats for personal privacy. The debate over computerized record matching has been hotly contested, and it has been denounced because of its implications for stereotyping and profiling certain classes or groups of individuals. Computerized record matching has also been criticized by civil liberties groups who fear that such a practice might lead to a new form of social control.

Defenders of this practice justify the matching of computer records because it enables us to track down deadbeat parents, welfare cheats, and the like. Although few would object to the ends that could be achieved, we can question whether the practice of computerized matching is compatible with individual privacy. Even if computerized record matching

does help to root out governmental waste and fraud, would that fact alone justify such a practice? Consider this counterexample: Suppose that 24-hour video surveillance and daily drug testing of all government employees also help to root out government waste and fraud—would such means also be justifiable in order to reach the desired end?

Proponents of computer matching might argue that 24-hour video surveillance and daily drug testing of government workers would violate the privacy of workers in ways that matching computerized records does not. However, critics have pointed out that computer matches have been made even when there was no suspicion that a particular individual or group of individuals had violated the law. For example, computer records of entire categories of individuals, such as government employees, have been matched against databases containing records of welfare recipients on the chance that a "hit" will identify one or more welfare cheats. One line of argumentation sometimes used to defend a practice such as computer matching against the charge of violating privacy rights is as follows:

PREMISE 1. Privacy is a legal right.

PREMISE 2. Legal rights are conditional, not absolute.

PREMISE 3. When one violates the law (i.e., commits a crime), one forfeits one's legal rights.

CONCLUSION. Criminals have forfeited their legal right to privacy.

Initially, this line of reasoning seems quite plausible, but does it apply in the case of computerized record matching? First of all, this argument assumes that we have an explicit legal right to privacy. Let us assume, for the sake of argument, that we have such a right and that all legal rights are (or ought to be) conditional only. Even with the addition of these two assumptions, problems remain: for example, those who maintain that a deadbeat parent has, in violating the law, given up his right to privacy seem to either disregard or ignore any right to privacy accorded to individuals who have not broken the law. For it was only by matching the records of mostly innocent individuals whose names were included in multiple government databases that a "hit," identifying one or more alleged criminals, was generated. So even if criminals do forfeit their right to privacy, the process of identifying these criminals via computerized record matching entails that several noncriminals will be required to forfeit that right as well.

Next, consider a computerized matching technique involving biometric identifiers that also has been used by some government agencies.

▶ SCENARIO 5–5: Using Biometric Technology at Super Bowl XXXV

At Super Bowl XXXV in January 2001, a facial recognition technology scanned the faces of individuals entering the stadium. The digitized facial images were then instantly matched against images in a centralized database of suspected criminals and terrorists. Those who attended the sporting advent were not told that their faces had been scanned. The day after the super bowl, many learned what had happened via a newspaper story, which caused considerable controversy at the time. Many privacy advocates and civil liberties proponents criticized the tactics used by the government at this major sports event.[14] ■

Although this incident generated some controversy in early 2001, the attitudes of many Americans who were initially critical of the government's use of biometrics at Super Bowl XXXV changed later that year, following the tragic events of September 11. We will examine this biometric technique in greater detail in Chapter 7, where we discuss cybercrime. However, it is useful at this point to show how this biometric-based matching technique differs from the computerized record-matching practice involving government workers, which we considered earlier in this section.

Initially, one might argue that the biometric-based matching technique used to scan and match faces of individuals at stadiums and airports, as well as other public places, is essentially no different from the computerized record-matching operations previously used to catch welfare cheats and deadbeat parents. But in traditional computerized record matching, all of the databases involved contain records of individuals who were (or should have been) assumed to be innocent. As we saw, records of government workers (presumed to be innocent) were matched against records of welfare recipients (also presumed to be innocent) to ferret out any persons who just happen to be in both groups. In the case of the face recognition program used at Super Bowl XXXV, however, images of persons entering the football stadium were matched against a database of persons already known (or at least suspected) to be criminals and terrorists. So the objectives of the targeted matches at Super Bowl XXXV were much more specific than those involving the "fishing expeditions" used in some earlier computerized record-matching practices. Perhaps this is one reason why the biometric-based matching operations aimed at catching terrorists and dangerous criminals have been less controversial than traditional record-matching practices used by federal and state governments.

▶ 5.6 MINING PERSONAL DATA

A form of data analysis that uses techniques gained from research and development in artificial intelligence (AI), described in Chapter 11, has been used to "mine" personal data. Formally referred to as Knowledge Discovery in Databases, or KDD, the process is now more commonly known as *data mining*. Essentially, data mining involves the indirect gathering of personal information through an analysis of implicit patterns discoverable in data. Data mining activities can generate new and sometimes non-obvious classifications or categories; as a result, individuals whose data are mined can become identified with or linked to certain newly created groups that they might never have imagined to exist. This is further complicated by the fact that current privacy laws offer individuals virtually no protection with respect to how information about them acquired through data mining activities is subsequently used, even though important decisions can be made about those individuals based on the patterns found in the mined personal data. So, data mining technology can be used in ways that raise special concerns for personal privacy.

5.6.1 How Does Data Mining Threaten Personal Privacy?

What is so special about the privacy concerns raised by data mining? For example, how do they differ from privacy issues introduced by more traditional data retrieval techniques, such as computerized merging and matching operations that we examined in

Section 5.5? For one thing, privacy laws as well as informal data protection guidelines have been established for protecting personal data that are

- *explicit* in databases (in the form of specific electronic records),
- *confidential* in nature (e.g., data involving medical, financial, or academic records),
- exchanged between or across databases.

However, virtually no legal or normative protections apply to personal data manipulated in the data mining process, where personal information is typically

- *implicit* in the data,
- *nonconfidential* in nature,
- *not exchanged* between databases.

Unlike personal data that reside in explicit records in databases, information acquired about persons via data mining is often derived from implicit patterns in the data. The patterns can suggest "new" facts, relationships, or associations about a person, placing that person in a "newly discovered" category or group. Also, because most personal data collected and used in data mining applications is considered neither confidential nor intimate in nature, there is a tendency to presume that such data must, by default, be *public* data. And unlike the personal data that are often exchanged between or across two or more databases in traditional database retrieval processes, in the data mining process personal data are often manipulated within a single database, and typically within a large *data warehouse*.

Next consider a scenario involving data mining practices at a bank in determining whether or not to grant loans to its customers. As you consider the privacy issues raised in the following scenario, keep in mind Nissenbaum's distinction between "norms of appropriateness" and "norms of distribution" for determining contextual integrity (described in Section 5.2.5).

▶ **SCENARIO 5–6:** Data Mining at the XYZ Bank

Lee, a junior executive at ABE Marketing Inc., has recently applied for an automobile loan at the XYZ Bank. To secure the loan, Lee agrees to complete the usual forms required by the bank for loan transactions. He indicates that he has been employed at the ABE Marketing Company for more than 3 years and that his current annual salary is $240,000. He also indicates that he has $30,000 in a separate savings account, a portion of which he intends to use as a down payment for a new BMW. On the loan form, Lee also indicates that he is currently repaying a $15,000 personal loan used to finance a family vacation to Europe the previous year.

Next, the bank's computing center runs a data mining program on information in its customer databases and discovers a number of patterns. One reveals that executives earning more than $200,000 but less than $300,000 annually, who purchase luxury cars (such as BMWs), and who take their families on international vacations, are also likely start their own businesses within their first 5 years of employment. A second data mining algorithm reveals that the majority of marketing entrepreneurs declare bankruptcy within 1 year of starting their own businesses. The data mining algorithms can be interpreted to suggest that Lee is a member of a group that neither he nor possibly even the loan officers at the bank had ever known to exist—viz., the group of marketing executives likely to start a business and then declare bankruptcy within a year. With this new category and new information about Lee, the bank determines that Lee, and people that fit into Lee's group, are long-term credit risks.[15] ■

Does the mining of data about Lee by the XYZ Bank raise concerns for privacy? At one level, the transaction between Lee and the bank seems appropriate. To borrow money from XYZ Bank, Lee has authorized the bank to have the information about him, that is, his current employment, salary, savings, outstanding loans, and so forth, that it needs to make an informed decision as to whether or not to grant him the loan. So, if we appeal to Nissenbaum's framework of privacy as contextual integrity, it would seem that there is no breach of privacy in terms of norms of appropriateness. However, Lee gave the bank information about himself for use in one context, viz., to make a decision about whether or not he should be granted a loan to purchase a new automobile. He was assured that the information given to the bank would not be exchanged with a third party without first getting Lee's explicit consent. So, unlike cases involving the computerized merging and matching of records that we considered in Section 5.5, no information about Lee was either exchanged or cross-referenced between databases—i.e., there is no breach of the norms of distribution (in Nissenbaum's model). However, it is unclear whether the bank has agreed not to use the information it now has in its databases about Lee for certain in-house analyses.

Although Lee voluntarily gave the bank information about his annual salary, about previous personal loans, and about the type of automobile he intended to purchase, he gave each piece of information for a specific purpose and use, in order that the bank could make a meaningful determination about Lee's request for an automobile loan. It is, however, by no means clear that Lee authorized the bank to use disparate pieces of that information for more general data mining analyses that would reveal patterns involving Lee that neither he nor the bank could have anticipated at the outset. Using Lee's information for this purpose would now raise questions about "appropriateness" in the *context* involving Lee and the XYZ Bank.

The mining of data in Lee's case is controversial from a privacy perspective for several reasons. For one thing, the information that Lee is someone likely to start his own business, which would probably lead to his declaring personal bankruptcy, was not explicit in any of the data (records) about Lee; rather it was implicit in patterns of data about people similar to Lee in certain respects but vastly different from him in other respects. For another thing, Lee's case illustrates how data mining can generate new categories and groups such that the people whom the data mining analysis identifies with those groups would very likely have no idea that they would be included as members. And we have seen that, in the case of Lee, certain decisions can be made about members of these newly generated groups simply by virtue of those individuals being identified as members. For example, it is doubtful that Lee would have known that he was a member of a group of professional individuals likely to start a business, and that he was a member of a group whose businesses were likely to end in bankruptcy. The "discovery" of such groups is, of course, a result of the use of data mining tools.

Even though no information about Lee was exchanged with databases outside XYZ, the bank did use information about Lee internally in a way that he had not explicitly authorized. And it is in this sense—unauthorized internal use by data users—that data mining raises serious concerns for personal privacy. Note also that even if Lee had been granted the loan for the automobile, the bank's data mining practices would still have raised serious privacy concerns with respect to the contextual integrity of his personal information. Lee was merely one of many bank customers who had voluntarily given certain personal information about themselves to the bank for use in one context—in this

example, a loan request—and subsequently had that information used in ways that they did not specifically authorize.

Consumer Profiling

Of course, the scenario involving Lee is merely hypothetical. But some relatively recent evidence now suggests that banks and consumer credit organizations are using data mining techniques to determine an individual's "credit worthiness" in ways that are not so different from the example involving Lee. In these cases, a consumer's credit rating could actually be determined via profiling schemes that can suggest "guilt by association." For example, a consumer could have the spending limit on her credit card reduced, or have that card revoked altogether, because of where she shops or where she lives. Following the economic turndown in the United States that began in 2008, many private homes have been lost to foreclosure. So people living in neighborhoods where there was a high rate of foreclosures, or people holding mortgages with certain banks or lending institutions that have experienced high rates of home foreclosures, may now be considered credit risks by virtue of their association with either a certain neighborhood or bank, even though they have been responsible in paying their mortgages and other loans on time. Similarly, if individuals shop at a certain kind of retail store, say Wal-Mart, information about their purchases at such a store can associate them with other individuals who shop there, and who may have a higher-than-average default rate on their credit cards.

Mike Stuckey (2008) describes an incident where a 37-year-old computer consultant had two of his American Express cards canceled and the limit on a third card reduced. The consumer was told that the credit card company's decision was based in part on criteria having to do with *where* he shopped and with *whom* held his mortgage. American Express informed this customer that included in the criteria it uses to decide to reduce the spending limit on someone's credit card are the company's

> "credit experience with customers who have made purchases at establishments where you have recently used your card."
>
> "analysis of the credit risk associated with customers who have residential loans from the creditor(s) indicated in your credit report."

While there had been suspicion for some time that credit card companies engage in the kind of profiling scheme used by American Express, consumer advocates and credit analysts believe that this may be the first time that a major credit company admitted to using such criteria. In its defense, however, American Express claimed that it needs to analyze its exposure to risk as it reviews its cardholder's credit profiles in light of the economic turndown in the United States that severely affected the credit industry (Stuckey 2008).

We have seen how data mining can be used to threaten consumer privacy. But can it also be used to protect consumers against fraudulent activities? Perhaps not surprisingly, data mining, like other technologies, can be viewed as a "double-edged sword" with respect to consumers' interests, as the following story suggests. One day, to my surprise, I received a telephone call from my credit card company informing me that a purchase, which the company apparently viewed as suspicious, had been charged earlier that day to my credit card account. When asked about the purchase, I informed the company's representative that it had not been made by me, and I also thanked the person for notifying me so promptly about this transaction. The company representative then

immediately canceled my existing credit card and issued me a new card with a new account number.

Why did the company suspect that the purchase made that day with my credit card was questionable? It would seem that the data mining algorithms used by the credit card company to determine the patterns of my purchases—which kinds of purchases and credit card transactions I typically make, with whom and where I make them, and when—revealed the anomaly of the questionable purchase made that day with my credit card. So in this instance, data mining appeared to have been used in a way that protected the interests of a consumer.

5.6.2 Web Mining

Initially, the mining of personal data depended on large (offline) commercial databases called data warehouses, which stored the data, consisting primarily of transactional information. Data mining techniques are now also used by commercial Web sites to analyze data about Internet users, which can then be sold to third parties. This process is sometimes referred to as "Web mining," which has been defined as the application of data mining techniques to discover patterns from the Web.[16] The kinds of patterns discovered from Web mining can be useful to marketers in promotional campaigns. The following scenario, involving Facebook, illustrates one way in which mining can be done on the Web.

▶ **SCENARIO 5–7:** The Facebook Beacon Controversy

Facebook (originally called "The Facebook") is a popular social networking service founded by Mark Zuckerberg in 2004, when he was a student at Harvard University. As in the case of other SNSs (examined in detail in Chapter 11), Facebook enables its members to share information about themselves with "friends" and to make additional friends through its range of services. In November 2007, Facebook announced a marketing initiative called Facebook Beacon, which would let Facebook friends share information about what they do online, including the purchases they make. Although this feature, made possible by external Web sites that sent data about individuals to Facebook, enabled users to share their online activities with their friends, it also allowed targeted advertisements by the Web sites sending the data. Essentially, Beacon allowed affiliate Web sites (including Blockbuster, Fandago, and many others) to send stories about a user's online activities to Facebook, which were then displayed to that user's "friends" in the form of news feeds and Social Ads.

However, the Beacon initiative proved to be very controversial; for one reason, it disclosed what purchases users made at certain Web sites. Also, when Facebook introduced Beacon, it stated that it would not share any personally identifiable information in the Social Ads, and it claimed that users would only see those ads to the extent that they were willing to share that information with others. But Facebook was soon criticized for collecting more user information for advertisers than it had originally admitted. In December 2007, Zuckerberg publicly apologized for the way that the Beacon project had been set up, admitting that it was established as an "opt-out" system instead of an "opt-in" system. So, by default, if a Facebook user did not explicitly decline to share something, Beacon would share the advertising information with that person's friends via the user's profile.[17] ■

Many Facebook users complained when they discovered what was happening with the information about their online purchases and activities. But were the practices used in

the Beacon program incompatible with Facebook's privacy policy at that time? Facebook's original privacy agreement stated

> We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers, and other users of Facebook, to supplement your profile.

A controversial clause in its privacy policy was Facebook's right to sell a user's data to private companies, which stated

> We may share your information with third parties, including responsible companies with which we have a relationship.

However, Facebook officials claimed that they had never provided, nor had they intended to provide, users' information to third-party companies. But Facebook nonetheless decided to change its privacy policy in response to the controversy generated by Beacon.[18]

The Beacon controversy also generated other privacy concerns for Facebook users, independent of Web mining. One concern had to do with Facebook's policy for users wishing to delete their accounts. Some users worried about what would happen to the personal information that Facebook had collected about them while their accounts were active. Did Facebook own that information? Could it be used in future Web mining or sold to third parties, or both? Facebook's initial policy stated that users could only "deactivate" their accounts. Once deactivated, the user's profile would no longer be visible on Facebook. However, that information would remain on Facebook's servers. Again, many users were not satisfied, because they wished to delete their accounts permanently. For example, some users wished to permanently remove information that may have been embarrassing or highly sensitive, including photos of them drinking at parties or in their dormitory rooms. In response to pressure from users, Facebook has since changed its policy for deleting accounts. The new policy enables users to contact Facebook to request that their accounts be permanently deleted.

In Table 5.2, we summarize some of the differences in mining, matching, and merging techniques used to process personal information.

The Facebook Beacon controversy illustrates how easily personal data can be mined on the Web. Because the amount of data on the Internet is so vast, one might assume that it is impossible to mine those data in ways that could be useful. However, current data mining tools employ sophisticated and advanced AI technology that enable the users of

TABLE 5.2 Mining, Matching, and Merging Techniques for Manipulating Personal Data

*Data **Merging***	A data exchange process in which personal data from two or more sources is combined to create a "mosaic" of individuals that would not be discernable from the individual pieces of data alone.
*Data **Matching***	A technique in which two or more unrelated pieces of personal information are cross-referenced and compared to generate a match, or "hit, " that suggests a person's connection with two or more groups.
*Data **Mining***	A technique for "unearthing" implicit patterns in large single databases, or "data warehouses," revealing statistical data that associates individuals with nonobvious groups; user profiles can be constructed from these patterns.

those tools to "comb" through massive amounts of data that would not have been possible to analyze with traditional information retrieval techniques. Also, sophisticated search engines have programs (called "spiders") that "crawl" through the Web in order to uncover general patterns in information across multiple Web sites. Sue Halpern (2011) points out that approximately 500 companies now mine the "raw material of the Web" and then sell it to data mining companies. And Eli Pariser (2011) notes that one of these companies, Acxiom, has managed to accumulate 1500 pieces of data, on average, for each person in its database; this personal data ranges from people's credit scores to the kinds of medications they use.

Pariser also notes that Google and other major search engine companies use "prediction engines" to construct and refine theories about us and the kinds of results we desire from our search queries. (We examine Google's 2012 Privacy Policy, which has been criticized by privacy advocates, in Section 5.9.1.) In Section 5.7.1, we examine some specific ways in which the use of Internet search engines raise privacy concerns, even though the kind of personal information about us that is acquired by search engine companies might not initially seem to warrant explicit privacy protection. To see why such protection might indeed be needed in these cases, however, we first examine some questions underlying a concern that Helen Nissenbaum (2004b) calls the "problem of privacy in public."

▶ 5.7 PROTECTING PERSONAL PRIVACY IN PUBLIC SPACE

So far, we have examined how cybertechnology can be used to gather, exchange, and mine personal information. With the exception of data mining, which manipulates personal, but nonconfidential information, the kind of personal information gathered and exchanged was often confidential and intimate in nature. For example, we saw how financial and medical records could be exchanged between two or more databases using computerized merging and matching. This confidential and very personal information is referred to as nonpublic personal information (NPI). Privacy analysts are now concerned about a different kind of personal information—public personal information (PPI), which is neither confidential nor intimate and which is also being gathered, exchanged, and mined using cybertechnology.

PPI includes information about you, such as where you work or attend school or what kind of car you drive. Even though it is information about you as a particular person, PPI has not enjoyed the privacy protection that has been granted to NPI.

Until recently, most concerns about personal information that was gathered and exchanged electronically were limited to NPI, and because of the attention it has received, privacy laws and policies were established to protect NPI. But now privacy advocates are extending their concern to PPI; they are arguing that PPI deserves greater legal and normative protection than it currently has. As noted above, Nissenbaum refers to this challenge as the problem of protecting privacy in public.

Why should the collection and exchange of PPI raise privacy concerns? Suppose that I discover some information about you: you are a junior at Technical University, you frequently attend your university's football games, and you are actively involved in your university's computer science club. In one sense, the information that I have discovered about you is personal, because it is about *you* (as a person), but it is also public, because it

pertains to things that you do in the public sphere. Should you be worried that this information about you is so easily available?

In the past, the public availability of such seemingly harmless and uncontroversial information about you was no cause for concern. Imagine that 80 years ago a citizen petitioned his or her congressperson to draft legislation protecting the privacy of each citizen's movements in public places. It would have been difficult then to make a strong case for such legislation; no one would have seen any need to protect that kind of personal information. But now some are arguing that we need to protect privacy in public, that our earlier assumptions are no longer tenable. Nissenbaum (2004b) believes that many in the commercial sector proceed from an assumption that she believes is "erroneous"—viz., "There is a realm of public information about persons to which no privacy norms apply."[19] Keep this assumption in mind as you consider the following scenario.

▶ SCENARIO 5–8: Shopping at SuperMart

One day, you decide to shop for groceries at SuperMart. If I happen to see you enter or leave SuperMart, or if we are both shopping in this store at the same time, I now have information that you shop (or, at least, have once shopped) at SuperMart. (This information could be considered "public" because it was acquired in a public forum and because it is neither intimate nor confidential in nature.) If I also happen to pass by you in one of the aisles at SuperMart, I can observe the contents of your shopping basket; I may notice that you are purchasing several bottles of wine but relatively little food. Again, I have acquired this information about you by observing your activity in a public forum. ■

Because the information I have acquired about you in the above scenario can be considered public information, it would not warrant any legal privacy protection. And even though this information is about *you as a person*, it is not the kind of personal information to which we, as a society, would typically grant normative privacy protection. What, exactly, is the privacy problem regarding the kind of personal information about your public activities in shopping at SuperMart? Why should you be concerned about information that is gathered about what you do at SuperMart or, for that matter, in any public place? Let us continue the shopping metaphor, but this time we consider shopping that takes place in an online forum.

▶ SCENARIO 5–9: Shopping at Nile.com

Imagine that you visit an online bookstore called *Nile.com* to locate a particular book that you are considering purchasing. Because you are visiting this bookstore via a computer or electronic device located in your own home, you cannot be observed by people in physical space nor can you be seen by other customers on the *Nile.com* Web site. However, from the moment you log on to *Nile.com*, information about you is being intentionally gathered and carefully recorded—i.e., information about the exact time that you entered Nile, as well as the exact time that you leave. As you make contact with the Nile Web site, Nile requests a cookie file from your computer to determine whether you have previously visited this site. If you have visited this site before and have clicked on items that interested you, Nile can find a record of these items. The information stored in that cookie file can also be used by Nile to alert you to newly released books that it believes might interest you, based on an analysis of the data Nile collected from your previous visits to its site. ■

The information that Nile now has about you does not seem categorically different from the information that SuperMart might also have about you (assuming that you used that store's "courtesy card" or discount card in making your purchases). However, there are significant differences in the ways that information about you can be gathered, recorded, and then used as a result of your shopping at each store.

When you shopped in physical space at SuperMart, only your actual purchases could be recorded and stored in SuperMart's databases. Items that might have only caught your attention and items that you might also have picked up or even placed in your cart at one point while shopping but did not eventually purchase at the checkout register are not recorded by SuperMart's data collection system. However, as you shop, or even browse, at Nile, there is a record of virtually every move you make—every book that you search, review, etc., as well as the one(s) you purchase. Yet, just like the information gathered about your shopping habits in physical space at SuperMart, this personal information that Nile has gathered about your browsing and shopping habits online is considered and treated as public information.

Now we can see why some people worry about having their movements online tracked and recorded. The information Nile gathered about you is, in effect, *Nile's* information, even though it pertains to *you* as a person; Nile now owns that information about you, as well as the information it has about its other customers, and is, in principle at least, free to do with that information whatever it chooses. On the one hand, the information seems fairly innocuous—after all, who really cares which books you happen to browse or purchase? On the other hand, however, this information can be combined with other information about your online transactions at additional Web sites to create a consumer profile of you, which can then be sold to a third party.

One argument that online entrepreneurs might advance to defend these business practices is that if a user puts information about him- or herself into the public domain of the Internet, then that information is no longer private. Of course, one response to this line of reasoning could be to question whether users clearly understand the ways that data they submit might subsequently be used.

In the Nile.com scenario, Nile used information about you in ways that you neither authorized nor intended—an example of the kind of practice that Nissenbaum (2004a, 2010) describes as violating "contextual integrity" (see Section 5.2.5). Also, we can question whether businesses, such as Nile, should be able to "own" the information about us that they collect and then do with that information whatever they please for as long as they want? Joseph Fulda (2004) questions whether the old legal rule that states, "Anything put by a person in the public domain can be viewed as public information," should still apply. He admits that such a rule may have served us well, but only before data were "mined" to produce profiles and other kinds of patterns about individuals.[20]

5.7.1 Search Engines and the Disclosure of Personal Information

Internet search engines are valuable for directing us to available online resources for academic research, commerce, recreation, and so forth; so it might be surprising to find that search engine technology, too, can be controversial from the perspective of personal privacy. How can search engine technology conflict with personal privacy? At least two different kinds of concerns affecting privacy arise because of practices involving search engines: (1) search engine companies such as Google record and archive each search

request made by users and (2) search engines enable users to acquire a wealth of personal information about individuals, with relative ease. We begin with a brief examination of (1).

Google and the Controversy Surrounding Records of Users' Searches

Google creates a record of every search made on its site, which it then archives. The topic searched for, as well as the date and time the specific search request is made by a user, are included in the record. These data can be linked to the IP address and the ISP of the user requesting the search. So individual searches made by a particular user could theoretically be analyzed in ways that suggest patterns of that individual's online behavior, and, perhaps more controversially, these records could later be subpoenaed in court cases. Yet, until relatively recently, many (if not most) Google users were unaware of the company's policy regarding the recording and archiving of users' search requests.

On the one hand, this information might seem relatively innocuous—after all, who would be interested in knowing about the kinds of searches we conduct on the Internet, and who would want to use this information against us? On the other hand, however, consider the case of a student, Mary, who is writing a research paper on Internet pornography. Records of Mary's search requests could reveal several queries that she made about pornographic Web sites, which in turn might suggest that Mary was interested in viewing pornography. In early 2006, Google users discovered that any worries they may have had about the lack of privacy protection concerning their Internet searches were justified, in light of the events described in the following scenario.

▶ **SCENARIO 5–10:** Tracking Your Search Requests on Google

In 2005, the George W. Bush administration informed Google that it must turn over a list of all users' queries entered into its search engine during a 1-week period (the exact dates were not specified by Google). But Google refused to comply with the subpoena on the grounds that the privacy rights of its users would be violated. Both Yahoo Inc. and Microsoft Corp. MSN, companies that operated the second- and third-most-used search engines, respectively, also had their search records subpoenaed by the Bush administration. Yahoo, unlike Google, complied with the subpoena. It was not clear whether Microsoft also turned over its records to the government, since it declined to say one way or another.[21] ■

The Bush administration's decision to seek information about the search requests of ordinary users has since drawn significant criticism from many privacy advocates. Critics argued that although the Bush administration claimed that it had the authority to seek electronic information in order to fight the "war on terror" and to prevent another September 11-like attack, the records at issue in this particular case had to do with the number of users requesting information about, or inadvertently being sent to, pornographic Web sites. Some critics further argued that the Bush administration was interested in gathering data to support its stance on the Child Internet Pornography Act (CIPA), which had been challenged in a U.S. District Court (see Chapter 9). So, many critics were quick to point out that the Bush administration's rationale for obtaining records of search requests made by ordinary citizens seemed politically and ideologically motivated, and may have had nothing to do with protecting national security.

Using Search Engines to Acquire Information about People

It is not only the fact that an individual's search requests are recorded and archived by major companies such as Google that make Internet search engines controversial from the perspective of personal privacy. Search engine-related privacy issues also arise because that technology can be used for questionable purposes such as stalking. In fact, one search facility—Gawker-Stalker (www.gawker.com/stalker)—has been designed specifically for the purpose of stalking famous people, including celebrities. For example, suppose that Matt Damon is spotted ordering a drink at an up-scale café in Boston. The individual who spots Damon can send a "tip" via e-mail to Gawker-Stalker, informing the site's users of Damon's whereabouts. The Gawker site then provides its users, via precise GPS software, with information about exactly where, and at what time, Damon was sighted. Users interested in stalking Damon can then follow his movements electronically, via the Gawker site, or they can locate and follow him in physical space, if they are in the same geographical vicinity as Damon.

But it is not just celebrities who are vulnerable to information about them being acquired by others via search engines. Consider the amount and kind of personal information about ordinary individuals that is now available to search engines. In some cases, that information may have been placed on the Internet inadvertently, without the knowledge and consent of those affected. Yet information about those persons can be located by an Internet user who simply enters their names in a search engine program's entry box. The fact that one can search the Internet for information about someone might not seem terribly controversial. After all, people regularly place information about themselves on Web sites (or perhaps they authorize someone else to do it for them) and on social networking services such as Facebook and LinkedIn. And it might seem reasonable to assume that any online personal information that is currently available to the public should be viewed simply as public information. But should such information about persons be unprotected by privacy norms merely because it is now more easily accessible for viewing by the public?

We have seen how the use of search engines can threaten the privacy of individuals in two distinct ways: (1) by recording and archiving records of a user's search queries that reveal the topic of the search and the time the request was made by the user and (2) by providing users of search engines with personal information about individuals who may have no idea of the wealth of personal information about them that is available online (and have no control over how it is accessed and by whom it is accessed). The latter concern is further complicated by the fact that individuals who are the subject of online searches enjoy no legal protection because of the presumed "public" nature of the personal information about them that is available via online searches.

So far, we have seen how our personal information can be collected and then manipulated by search engines in ways that are controversial. We next consider some controversies that involve access to personal information that resides in public records available online.

5.7.2 Accessing Online Public Records

Another kind of personal information that can also be considered public in nature is information about us stored in records located in municipal buildings, which are accessible to the general public. Public records have generally been available to anyone

willing to go to those municipal buildings and request hardcopy versions of them. Some municipalities charge a small fee to retrieve and copy the requested records. Many of these public records can now also be accessed online. Has this changed anything?

Consider that information merchants were always able to physically or manually collect all of the public records they could acquire. But traditional "information entrepreneurs" without computer technology would have had to hire legions of clerks to collect the (publicly available) data, sort the data according to some scheme, and then compile and print the data for sale. The process would have been physically impractical and hardly profitable, given the labor it involved; it would probably never have occurred to anyone even to attempt it prior to the advent of sophisticated information technology.

We could ask why public records were made public in the first place. Were they made public so that information merchants could profit from them, or were they instituted to serve broader societal and governmental ends? In order for governmental agencies at all levels to operate efficiently, records containing personal information are needed. For example, municipal governments need real estate information for tax assessment purposes, state governments need information about motor vehicle owners and operators, and federal governments need social security and income tax information. Records have to be easily accessible to and transferable and exchangeable between governmental agencies at various levels. Since they contain information that is neither confidential nor intimate, they are, with good reason, public records. It has been assumed that the availability of public records causes no harm to individuals, and that communities are better served because of the access and flow of those records for what seems to be legitimate purposes. But information gathering companies now access those public records, manipulate them to discover patterns useful to businesses, and then sell that information to third parties.

Many information merchants seem to assume that offices responsible for maintaining public records now have a legal obligation to make *all* public records available online. Their presumption is that the government has no right to restrict or limit, in any way, information that has been deemed appropriate for inclusion in public records. Is this a reasonable presumption? Consider two incidents, one involving public records at the city level and the other at the state level, which have caused controversy.

▶ **SCENARIO 5–11:** Accessing Online Public Records in Pleasantville

The city of Pleasantville has recently made all of its public records, including real estate records, available online; with a networked computer or electronic device, one can simply enter the address of any house in Pleasantville and retrieve the current tax assessment for the house, the price paid by the most recent owner, and a description of the physical layout of the house, including the location of doors and windows. Many of Pleasantville's citizens were outraged when they learned that this information was available online, even though the same information had previously been available as public records, stored in physical file cabinets at City Hall.[22] ■

Why should the residents of Pleasantville be so concerned? For one thing, some might worry that prospective burglars could plan break-ins by accessing the detailed physical layouts of their homes, which were readily available online. Consider that public records in the form of motor vehicle information have also been made available online, and, as in the Pleasantville scenario involving access to records about one's home, this practice has also outraged many citizens.

▶ **SCENARIO 5–12:** Accessing a State's Motor Vehicle Records Online

In the late 1990s, information from the state of Oregon's Department of Motor Vehicle became accessible online. An independent computer consultant used the means available to any private citizen to purchase data from that state's department, which was already available offline to anyone willing to pay a small fee. Once he purchased the information and converted it to electronic format, the consultant set up a Web site where any Internet user could, for a small fee, enter an Oregon license plate number and obtain the name and address of the owner of the registered vehicle. Many of Oregon's residents were outraged when they heard about this practice; eventually, the state's governor intervened and persuaded the consultant to close down the Web site.[23] ■

We ask again, What was the purpose of making such records public in the first place? There is no reason to believe that it was to facilitate commerce in the private sector. Of course, selling information, as the State of Oregon did, is now an important source of revenue for many state governments. But we also need to consider the privacy (and other ethical) implications of states selling information about their residents to online merchants, especially in an era where technology makes it so easy to erode personal privacy. Can technology also provide us with tools to protect our privacy?

▶ 5.8 PRIVACY-ENHANCING TECHNOLOGIES

We have seen how cybertechnology has exacerbated privacy concerns. Ironically, perhaps, cybertechnology also provides tools that can help users to protect their privacy. For example, *privacy-enhancing technologies* or *PETs* have been developed to help users protect (a) their personal identity while navigating the Internet and (b) the privacy of their online communications (such as e-mail). An example of (b) is encryption tools that encode and decode e-mail messages. Our main focus in this section is on whether PETs actually accomplish (a).

Some PETs enable users to navigate the Internet either anonymously or pseudonymously; one of the best-known anonymity tools is available from *Anonymizer.com*. It is important to note that although Anonymizer users enjoy anonymity while visiting Web sites, they are not anonymous to *Anonymizer.com* or to their own ISPs. A user's activities on a Web site can be recorded in server log files and can thus be traced back to a specific ISP and IP address. To enjoy complete anonymity on the Internet, online users need tools that do not require them to place their trust in a single "third party" (such as Anonymizer).

Another useful tool is TrackMeNot (http://cs.nyu.edu/trackmenot/), which was designed to work with the Firefox Web browser to protect users against surveillance and data profiling by search engine companies. Rather than using encryption or concealment tools to accomplish its objectives, TrackMeNot instead uses "noise and obfuscation." In this way, a user's Web searches become "lost in a cloud of false leads." By issuing randomized search queries to popular search engines such as Google and Bing, TrackMeNot "hides users' actual search trails in a cloud of 'ghost' queries." This technique makes it difficult for search engine companies to aggregate the data it collects into accurate user profiles.

Although PETs such as Anonymizer and TrackMeNot assist users in navigating the Web with relative anonymity, they are not useful for e-commerce transactions in which

users must reveal their actual identities. Many e-commerce sites now provide users with a stated privacy policy that is backed by certified "trustmarks" or trust seals (discussed in more detail in Section 5.9.1). These trust agreements between users and e-commerce sites can also be viewed as PETs in that they are intended to protect a user's privacy during a consumer transaction. But are they adequate to the task? To answer this question, we next analyze PETs in relation to two specific challenges: consumer education and informed consent.[24]

5.8.1 Educating Users about PETs

How are users supposed to find out about PETs? Consider that Web sites are not required to inform users about the existence of PETs or to make those tools available to them. Furthermore, online consumers must not only discover that PETs are available, but they must also learn how to use these tools. So at present, responsibility for learning about PETs and how to use them is incumbent upon consumers. Is it reasonable and is it fair to expect users to be responsible for these tasks?

Recall our earlier discussion of cookies. Although many Web browsers allow users to reject cookies, the default is that cookies will be accepted unless the user explicitly rejects them. But why shouldn't the default setting be changed such that Web sites would have to get a user's permission to send a cookie file to that user's computer system? The Web site could also inform, and possibly educate, the user about the existence of cookies, and then ask whether he or she is willing to accept them. Why not presume that users do not want cookie information recorded and stored on their computer systems, and then set the default conditions on Web browsers accordingly? And why not further presume that users do not want their personal data used in ways they did not explicitly authorize when they initially disclosed it in a commercial transaction? Following Judith DeCew (2006), we could "presume in favor of privacy" and then develop ways that would allow individuals to determine for themselves how and when that presumption should be overridden. (This is part of a process that DeCew refers to as "dynamic negotiation.") Independent of questions about where the presumption should reside, however, the widespread application and use of PETs will require a massive educational effort.

5.8.2 PETs and the Principle of Informed Consent

Even if the consumer-education-related issues involving PETs can be resolved, other questions need to be asked. For example, do PETs adequately support users in making *informed* decisions about the disclosure of their personal data in commercial transactions? Traditionally, the principle of informed consent has been the model, or standard, in contexts involving the disclosure of one's personal data. However, users who willingly consent to provide information about themselves for one purpose (e.g., in one transaction) may have no idea how that information can also be used in secondary applications.

Some in the commercial sector argue that because no one is forcing users to reveal personal data, the disclosure of such data is done on a completely voluntary basis. Assume that a user has willingly consented to disclose personal data in an e-commerce transaction. Has the user also consented to having that information used for additional, "secondary" purposes? Recall our discussion in Section 5.6 about data mining, where we

saw that specific information given by a consumer for use in one context could be subsequently "mined."

We can also ask whether businesses that collect personal data could possibly know in advance exactly how those data will be used in secondary and future applications? When data mining technology is involved, for example, it would seem that businesses could *not* adequately inform users about exactly how their personal data might be used in secondary applications. What kind of *informed* choice, then, could users make in these cases? (In Chapter 12, we examine how the principle of informed consent has become nontransparent or "opaque" in genomic research that employs data mining technology.)

Some in the e-commerce sector have responded to critics by pointing out that in most cases, users are provided with the means to either "opt-in" or "opt-out" of having their personal data collected, as well as having those data made available for secondary use. But the default is such that if no option is specified by the user when he or she discloses personal data for use in one context, then those disclosed personal data are also available for secondary use. Hence, the policy is "presumed consent," not informed consent. Is that presumption fair to online consumers?

Because PETs provide users with some ways of protecting their identity and also provide them some choice in controlling the flow of their personal information, they would seem to be an empowering rather than a disabling technology. But PETs alone are insufficient for resolving many privacy concerns affecting e-commerce.

▶ 5.9 PRIVACY LEGISLATION AND INDUSTRY SELF-REGULATION

We saw in the previous section that even though PETs offer users a means to protect their identity in certain kinds of activities, they are not the "magic bullet" many of their staunchest supporters have suggested. Recognizing the limitations of PETs, some privacy advocates believe that stronger privacy laws will protect consumers, whereas others in the commercial sector, for example, believe that additional privacy legislation is neither necessary nor desirable. Instead, they suggest strong industry controls regulated by standards.

Generally, privacy advocates have been skeptical of voluntary controls, including industry standards for "self-regulation initiatives." Instead, they argue for stricter privacy legislation and data protection principles to protect the interests of users. We begin this section with a look at certain self-regulatory schemes for privacy protection that is provided to consumers by industry standards.

5.9.1 Industry Self-Regulation Initiatives Regarding Privacy

Some industry representatives who advocate for the use of "voluntary controls" might concede that tools such as PETs, in themselves, are not adequate to protect the privacy of consumers in e-commerce transactions. However, they also believe that alternatives to additional privacy legislation are possible. These advocates point to the establishment of industry standards that have already been accepted and implemented. Some of these standards are similar to PETs in the sense that they are intended to protect a user's privacy, but unlike PETs in that they are not themselves tools.

An industry-backed (self-regulatory) initiative called TRUSTe was designed to help ensure that Web sites adhere to the privacy policies they advertise. TRUSTe uses a branded system of "trustmarks" (graphic symbols), which represent a Web site's privacy policy regarding personal information. Trustmarks provide consumers with the assurance that a Web site's privacy practices accurately reflect its stated policies. Through this PET-like feature, users can file a complaint to TRUSTe if the Web site bearing its trust seal does not abide by the stated policies. Any Web site that bears the TRUSTe mark and wishes to retain that seal must satisfy several conditions: The Web site must clearly explain in advance its general information-collecting practices, including which personally identifiable data will be collected, what the information will be used for, and with whom the information will be shared. Web sites that bear a trust seal but do not conform to these conditions can have their seal revoked. And Web sites displaying trust seals, such as TRUSTe, are subject to periodic and unannounced audits of their sites.

Critics have pointed out some of the difficulties in implementing TRUSTe. For example, the amount of information users are required to provide can easily discourage them from carefully reading and understanding the agreement. Also, the various warnings displayed may appear unfriendly and thus might discourage users; "friendlier" trustmarks, on the contrary, might result in users being supplied with less direct information that is important for protecting their privacy. But advocates of tools such as TRUSTe argue that, with these tools, users will be better able to make informed choices regarding electronic purchasing and other types of online transactions.

Critics worry that such programs do not go far enough. Consider, for example, the case of *Toysmart.com*, an e-commerce site that operated in Massachusetts. Consumers who purchased items from Toysmart were assured, via an online trust seal, that their personal data would be protected. The vendor's policy stated that personal information disclosed to Toysmart would be used internally but would not be sold to or exchanged with external vendors. So, users who dealt with Toysmart expected that their personal data would remain in that company's databases and not be further disclosed or sold to a third party. In the spring of 2000, however, Toysmart was forced to file for bankruptcy.[25]

In the bankruptcy process, Toysmart solicited bids for its assets, which included its databases containing the names of customers. Were the parties interested in purchasing that information under any obligation to adhere to the privacy policy that Toysmart had established with its clients? If not, whoever either took over Toysmart or purchased its databases, would, in principle, be free to do whatever they wished with the personal information in them, despite the fact that such information was given to Toysmart by clients under the belief that information about them would be protected indefinitely.

The Toysmart incident illustrates a situation in which users had exercised control over their personal information in one context—that is, in electing whether to disclose information about themselves to Toysmart in online transactions—based on specific conditions stated in Toysmart's privacy policy. However, it also turned out that these individuals were not guaranteed that the personal information they disclosed to Toysmart would be protected in the future. Thus, it would seem that controls beyond those provided by trustmarks and e-commerce vendors are needed.

Another concern has to do with various privacy policies established by search engine companies. Unlike e-commerce sites, which users can easily avoid if they wish, virtually every Internet user depends on search engines to navigate the Web. In Section 5.7.1, we

saw how major search engine companies such as Google record and keep a log of users' searches. This practice, as we also saw, has generated privacy concerns. In early 2012, Google announced a new comprehensive privacy policy, as described in the following scenario.

▶ **SCENARIO 5–13:** Controversies Involving Google's Privacy Policy

Google Inc., perhaps the most well-known search engine company in the world, also owns and/or operates several subsidiary services and Web-based applications. These include, Gmail, Google Maps, Google+, Google Calendar, Google Chrome, Picasa, Adsense/Adwords, and so forth. In the past, each had its own privacy policy. In 2012, however, Google replaced the individual policies with one comprehensive privacy policy across all of its services. When it implemented this change, Google also announced that the company would share user account data across all its services. Critics note that a user's search engine history could be shared with YouTube, or vice versa, and that a user's Google+ account data might be shared with Adwords to generate more targeted advertising.[26] ■

Google's new privacy policy, while explicit and transparent, has nonetheless been controversial for several reasons. For one thing, it is not clear how Google will use all of the personal information that it can now access so easily. For another, no one outside Google fully understands how the search engine company uses that information to manipulate (i.e., tailor or personalize) the search results a user receives for his or her search queries. Additionally, it is not clear whether one's personal information collected from the various Google services will be used only internally, or will also be available to advertisers and information merchants outside the company (e.g., those Web sites that include embedded Google ads to generate revenue).

Others worry whether users can trust Google—a company that officially embraces the motto: "do not be evil"—to abide by its new privacy policy. Some note, for example, that many people who used Apple's Safari Web browser on their computers and iPhones were under the impression that Google was not able to track their browsing activities. In early 2012, however, it was discovered Google had used software code that tricked the Safari browser, thus enabling Google to track the activities of those using that browser. Google disabled the controversial software code shortly after the incident was reported in *The Wall Street Journal*, and Safari users were informed by Google that they could rely on Safari's privacy settings to prevent tracking by Google in the future (Anguin and Valentino-DeVries 2012). But some critics remain skeptical.

Because of concerns involving distrust of Google and other commercial Web sites to regulate themselves, privacy advocates believe that explicit privacy laws are needed to protect users. We next briefly examine some existing privacy legislation.

5.9.2 Privacy Laws and Data Protection Principles

Many nations have enacted strong privacy legislation. The United States, however, has not taken the lead on legislation initiatives; some would argue that the United States is woefully behind the European nations in this regard. In fact, in the United States there is currently very little privacy protection in legal statutes. In 1974, Congress passed the Privacy Act, which has been criticized both for containing far too many loopholes and for lacking adequate provisions for enforcement. It applies only to records in federal

agencies and thus is not applicable in the private sector. Subsequent privacy legislation in the United States has resulted mostly in a "patchwork" of individual state and federal laws that are neither systematic nor coherent. In 2003, the Health Insurance Portability and Accountability Act (HIPAA), which provides protection for "individually identifiable" medical records from "inappropriate use and disclosure," was enacted into law. (HIPAA is examined in Chapter 12 in connection with our discussion of bioinformatics.) But the kind of privacy protection provided by HIPAA does not apply to an individual's nonmedical/health records such as consumer data.

Generally, U.S. lawmakers have resisted requests from privacy advocates for stronger consumer privacy laws, siding instead with business interests in the private sector who believe that such legislation would undermine economic efficiency and thus adversely impact the overall economy. Critics point out, however, that many of those businesses who have subsidiary companies or separate business operations in countries with strong privacy laws and regulations, such as nations in Western Europe, have found little difficulty in complying with the privacy laws of the host countries; profits for those American-owned companies have not suffered because of their compliance. In any event, there has been increased pressure on the U.S. government, especially from Canada and the European Union (EU), to enact stricter privacy laws, and pressure on American businesses to adopt stricter privacy polices and practices because of global e-commerce pressures.

EU nations have, through the implementation of strict data protection principles, been far more aggressive than the United States in addressing privacy concerns of individuals. In the early 1990s, the European community began to consider synthesizing the data protection laws of the individual European nations.[27] The European Community has since instituted a series of directives, including the EU Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995, which is referred to as the EU Directive on Data Protection, designed to protect the personal data of its citizens by prohibiting the "transborder flow" of such data to countries that lack adequate protection of personal data.[28]

Dag Elgesem (2004) has pointed out that a central focus of the EU Directive, unlike earlier privacy legislation in Europe that focused simply on the recording and the storage of personal information, is on the *processing* and *flow* of personal data. Several principles make up the European Directive; among them are the principles of Data Quality, Legitimate Purposes, Sensitive Data, and The Right to Be Informed. Whereas the Data Quality Principle is concerned with protecting the data subject's reasonable expectations concerning the processing of data about that subject, the Legitimate Purposes Principle lists the purposes for which the processing of personal data about the data subject are considered legitimate. What helps to ensure that each of these principles is enforced on behalf of individuals, or "data subjects," is the presence of privacy protection commissions and boards in the various European nations. As in the case of Canada, which has also set up privacy oversight agencies with a Privacy Commissioner in each of its provinces, many European countries have their own data protection agencies.

So far, we have considered various kinds of proposals aimed at addressing privacy concerns. Some have called for stricter privacy laws on the part of governments and for the formation of privacy oversight commissions to enforce those laws. Others call for more serious self-regulatory measures by those in the commercial sector. And some proposals have suggested the need for technological solutions that empower online users

by providing them with privacy-enhancing tools. Can these various proposals, or at least relevant aspects of them, be successfully combined or integrated into one comprehensive proposal?

While there has been no uniform consensus on a comprehensive privacy policy, especially one that could be implemented across international borders, there does seem to be considerable agreement on at least one point: any comprehensive privacy policy should be as transparent as possible. In examining James Moor's theory of privacy in Section 5.2.4, we saw that personal privacy could be protected in "situations" or zones that were declared "normatively private." We also saw that Moor requires that the rules for setting up normatively private situations be "public" and open to debate. This point is made explicit in his *Publicity Principle*, which states that the rules and conditions governing private situations should be "clear and known to persons affected by them" (Moor 2000). Thus, a critical element in Moor's model for an adequate privacy policy is openness, or transparency, so that all parties in the "situation," or context, are kept abreast of what the rules are at any given point in time. In this sense, Moor's publicity principle would seem to provide a key foundational element in any comprehensive privacy policy that incorporates legislation, self-regulation, and privacy-enhancing tools.

▶ 5.10 CHAPTER SUMMARY

We began by examining some ways that cybertechnology has exacerbated privacy concerns introduced by earlier technologies. We then briefly examined the concept of privacy and some theories that have attempted to explain and justify privacy. We saw that "informational privacy" could be distinguished from "accessibility privacy" and "decisional privacy," and that Moor's privacy theory was able to integrate key components of three traditional theories into one comprehensive theory of privacy. We also saw that privacy is an important value, essential for human ends such as friendship and autonomy.

We saw how NPI is threatened by data gathering and data exchanging techniques, including computerized matching and merging of records. And we also saw how PPI is threatened by data mining technology. We examined some privacy threats posed by the use of RFID technology, Internet cookies, and search engine technology. We also considered whether technology itself, in the form of privacy-enhancing technologies or PETs, could be used to preserve personal privacy or whether stronger privacy legislation and better industry self-regulation are needed.

We also noted at the outset that not all computer-related privacy concerns could be examined in Chapter 5. For example, specific kinds of privacy concerns pertaining to computerized monitoring in the workplace are discussed in Chapter 10, and privacy issues affecting computerized medical and healthcare information are examined in Chapter 12. Also examined in Chapter 12 are surveillance concerns affecting "location privacy" made possible by pervasive computing and GPS technologies. Although some privacy concerns affecting personal information about individuals collected by governmental organizations were also briefly considered in this chapter, additional privacy issues in this area are examined in Chapter 6 in the context of our discussion of computer security. Our main focus in Chapter 5 has been with privacy and cybertechnology concerns affecting the collection, exchange, and mining of personal data acquired from a typical individual's day-to-day activities, both on- and offline.

▶ REVIEW QUESTIONS

1. Identify and briefly describe four ways in which the privacy threats posed by cybertechnology differ from those posed by earlier technologies.
2. What is personal privacy, and why is privacy difficult to define?
3. Describe some important characteristics that differentiate "accessibility privacy," "decisional privacy," and "informational privacy."
4. How does James Moor's theory of privacy combine key elements of these three views of privacy? What does Moor mean by a "situation," and how does he distinguish between "natural privacy" and "normative privacy"?
5. Why is privacy valued? Is privacy an intrinsic value or is it an instrumental value? Explain.
6. Is privacy a social value, or is it simply an individual good?
7. What does Roger Clarke mean by "dataveillance"? Why do dataveillance techniques threaten personal privacy?
8. What are Internet cookies, and why are they considered controversial from the perspective of personal privacy?
9. What is RFID technology, and why is it a threat to privacy?
10. Explain computerized merging. Why is it controversial from the perspective of personal privacy?
11. Describe the technique known as computerized matching? What problems does it raise for personal privacy?
12. What is data mining, and why is it considered controversial?
13. What is the difference between PPI and NPI?
14. What is meant by "privacy in public"? Describe the problem of protecting personal privacy in public space.
15. Why are certain aspects and uses of Internet search engines controversial from a privacy perspective?
16. Why does online access to public records pose problems for personal privacy?
17. What are privacy-enhancing technologies (PETs)? How is their effectiveness challenged by concerns related to (user) education and informed consent?
18. Describe some of the voluntary controls and self-regulation initiatives that have been proposed by representatives from industry and e-commerce. Are they adequate solutions?
19. What are some of the criticisms of U.S. privacy laws such as HIPAA and the Privacy Act of 1974?
20. Describe some principles included in the EU Directive on Data Protection. What do you believe to be some of the strengths and weaknesses of those principles when compared to privacy laws in America?

▶ DISCUSSION QUESTIONS

21. Review Helen Nissenbaum's framework of privacy in terms of "contextual integrity." What are the differences between what she calls "norms of appropriateness" and "norms of distribution"? Give an example of how either or both norms can be breached in a specific context.
22. Through the use of currently available online tools and search facilities, ordinary users can easily acquire personal information about others. In fact, anyone who has Internet access can, via a search engine such as Google, find information about us that we ourselves might have had no idea is publicly available there. Does this use of search engines threaten the privacy of ordinary people? Explain.
23. In debates regarding access and control of personal information, it is sometimes argued that an appropriate balance needs to be struck between individuals and organizations: individuals claim that they should be able to control who has access to their information, and organizations, including government and business groups, claim to need that information in order to make appropriate decisions. How can a reasonable resolution be reached that would satisfy both parties?
24. Reexamine the arguments made by the U.S. government and by Google regarding the government's requests for information about users' search requests made during the summer of 2005. Are the government's reasons for why it should have access to that information reasonable? Does Google have an obligation to protect the personal information of its users, with respect to disclosing information about their searches? Could this obligation be overridden by certain kinds of national defense interests? If, for example, the government claimed to need the information to

prevent a potential terrorist attack, would that have changed your analysis of the situation? Or does the government have the right, and possibly an obligation to the majority of its citizens, to monitor the searches if doing so could positively affect the outcome of child pornography legislation?

▶ ESSAY/PRESENTATION QUESTIONS

25. Initially, privacy concerns involving computer technology arose because citizens feared that a strong centralized government could easily collect and store data about them. In the 1960s, for example, there was talk of constructing a national computerized database in the United States, and many were concerned that George Orwell's prediction of Big Brother in his classic book *1984* had finally arrived. The centralized database, however, never materialized. Prior to September 11, 2001, some privacy advocates suggested that we have fewer reasons to be concerned about the federal government's role in privacy intrusions (Big Brother) than we do about privacy threats from the commercial sector (Big Bucks and Big Browser). Is that assessment still accurate? Defend your answer.

26. Apply Helen Nissenbaum's framework of "privacy as contextual integrity" (examined in Section 5.2.5) to personal blogs that contain online personal diaries, such as the "Washingtonienne" (involving Jessica Cutler) scenario that we briefly described in Chapter 1. (At this point, you may want to revisit Scenario 1–3 in Chapter 1.) An important question that we were unable to analyze in our earlier analysis of that case was whether Cutler's privacy had been violated. Using Nissenbaum's framework, however, we can further refine our initial question by asking whether the incident violated the integrity of the norms of appropriateness or the norms of distribution, or both, in that context. Consider that, when Cutler set up her blog, she did not bother to protect it with a password. Is that point relevant in your assessment? Because the information included in her blog could, in principle, be read by anyone on the Internet, could Cutler plausibly claim that her privacy had been violated when her online diary was discovered and then posted in *Wonkette*, the Washington DC online gossip column? Also consider the six men implicated in her blog? Was it appropriate for her to include that information in her online diary? Did the distribution of information about them via Cutler's diary violate their privacy? Explain.

Scenarios for Analysis

1. In the days and weeks immediately following the tragic events of September 11, 2001, some political leaders in the United States argued that extraordinary times call for extraordinary measures; in times of war, basic civil liberties and freedoms, such as privacy, need to be severely restricted for the sake of national security and safety. Initially, the majority of American citizens strongly supported the Patriot Act, which passed by an overwhelming margin in both houses of Congress and was enacted into law on October 21, 2001. However, between 2001 and 2005 support for this act diminished considerably. Many privacy advocates believe that it goes too far and thus erodes basic civil liberties. Some critics also fear that certain provisions included in the act could easily be abused. Examine some of the details of the Patriot Act (which can be viewed on the Web at www.govtrack.us/congress/bills/107/hr3162/text), and determine whether its measures are as extreme as its critics suggest. Are those measures also consistent with the value of privacy, which many Americans claim to embrace? Do privacy interests need to be reassessed, and possibly recalibrated, in light of ongoing threats from terrorists? To what extent does the following expression, attributed to Benjamin Franklin, affect your answer to this question: "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

2. At the beginning of Chapter 5, we suggested that concerns about the loss of privacy may have a generational dimension or element—i.e., younger people may be less concerned

about privacy loss involving cybertechnology than older people. To further explore this possibility, conduct a series of informal interviews with individuals that represent three generations: Millennials, Gen X/Y, and Baby Boomers. Ask members of each group how much they value their privacy and how much of it they are willing to trade off for the convenience of cybertechnology. Compare the results of the answers you get from the three groups. Are their respective views about the importance of privacy as far apart as some might expect? Explain.

▶ ENDNOTES

1. See the interview with Arthur Miller in the video "The World at Your Fingertips" in the BBC/PBS Series, *The Machine That Changed the World*, 1990.
2. See Warren and Brandeis (1890) for more detail.
3. For a discussion of the right to privacy in the Quinlan case, see "Court at the End of Life—The Right to Privacy: Karen Ann Quinlan" at http://www.libraryindex.com/pages/582/Court-End-Life-RIGHT-PRIVACY-KAREN-ANN-QUINLAN.html.
4. Moor (2000), p. 207. [Italics added]
5. Nissenbaum (2004a), p. 137.
6. *Ibid*, p. 135. For analyses of how Nissenbaum's contextual-integrity model of privacy can be applied to the blogosphere and to "the Cloud," see Grodzinsky and Tavani (2010, 2011), respectively.
7. See Westin (1967) for more detail on this point.
8. DeCew (2006), p. 121. Moor (2006, p. 114) also describes privacy as a kind of "shield" that protects us.
9. See Clarke's account of dataveillance, available at http://www.rogerclarke.com/DV/.
10. Nissenbaum (2004a), p. 135.
11. Mason (2007, p. 42) makes a similar point when he notes that "I may authorize one institution to collect 'A' about me, and another institution to collect 'B' about me: but I might not want anyone to possess 'A and B' about me at the same time."
12. See, for example, Scott Chapman and Gurpreet S. Dhillon (2002). "Privacy and the Internet: The Case of DoubleClick, Inc." In G. Dhillon, ed. *Social Information in the Information Age: issues and Controversies*. Hershey PA: Idea Group, pp. 75–88.
13. My discussion of computerized matching here draws from Tavani (1996).
14. For more information about this incident, see Brey (2004).
15. This scenario is adapted from Tavani (1999).
16. See "Web Mining." *Wikipedia*. Available at http://en.wikipedia.org/wiki/Web_mining.
17. See http://en.wikipedia.org/wiki/Facebook.
18. *Ibid*.
19. Nissenbaum (2004b), p. 455.
20. Fulda (2004), p. 472.
21. See, for example, Nissenbaum (2010).
22. This scenario is based in part on an actual controversy involving online public records in Merrimack, NH.
23. See Scanlan (2001) for a more detailed account of the issues involved in this scenario.
24. My analysis of PETs in this section draws from Tavani (2000) and Tavani and Moor (2001).
25. For more information about this scenario, see Nicholas Morehead (2000). "Toysmart: Bankruptcy Litmus Test." *Wired* 7, no. 12. Available at http://www.wired.com/techbiz/media/news/2000/07/37517.
26. See Werner (2012) for a more detailed analysis of this controversy.
27. See http://www.oecd.org/document/18/0, 3343, en_2649_34255_1815186_1_1_1_1, 00.html.
28. See http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

▶ REFERENCES

Adam, Alison. 2005. "Chips in Our Children: Can We Inscribe Privacy in a Machine?" *Ethics and Information Technology* 7, no. 4: 233–42.

Anguin, Julia, and Jennifer Valentino-DeVries. 2012. "Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy." *Wall Street Journal*, February 17. Available at http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDEwNjExNDYyWj.html.

Bamford, James. 2012. "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)." *Wired*, March 15. Available at http://m.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

Brey, Philip. 2004. "Ethical Aspects of Facial Recognition Systems in Public Places." In R. A. Spinello and H. T. Tavani, eds. *Readings in Cyberethics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 585–600.

DeCew, Judith W. 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca NY: Cornell University Press.

DeCew, Judith W. 2006. "Privacy and Policy for Genetic Research." In H. T. Tavani, ed. *Ethics, Computing, and Genomics*. Sudbury MA: Jones and Bartlett, pp. 121–35.

Elgesem, Dag. 2004. "The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 418–35.

Fried, Charles. 1990. "Privacy: A Rational Context." In M. D. Ermann, M. B. Williams, and C. Gutierrez, eds. *Computers, Ethics, and Society*. New York: Oxford University Press, pp. 51–67.

Froomkin, Michael. 2000. "The Death of Privacy?" *Stanford Law Review* 52. Available at www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

Fulda, Joseph S. 2004. "Data Mining and Privacy." In R. A. Spinello and H. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 471–75.

Garfinkel, Simson. 2000. *Database Nation: The Death of Privacy in the 21st Century*. Cambridge MA: O'Reilly and Associates.

Garfinkel, Simson. 2002. "RFID Bill of Rights." *Technology Review*, October. Available at http://www.technologyreview.com/article/401660/an-rfid-bill-of-rights/.

Grodzinsky, Frances S., and Herman T. Tavani. 2010. "Applying the 'Contextual Integrity' Model of Privacy to Personal Blogs in the Blogosphere," *International Journal of Internet Research Ethics* 3, no. 1: 38–47.

Grodzinsky, Francis, S., and Herman T. Tavani. 2011. "Privacy in 'the Cloud': Applying Nissenbaum's Theory of Contextual Integrity." *Computers and Society* 41, no. 1: 38–47.

Halpern, Sue. 2011. "Mind Control and the Internet." *New York Review of Books*, June 23. Available at http://www.nybooks.com/articles/archives/2011/jun/23/mind-control-and-internet/.

Lockton Vance, and Richard S. Rosenberg. 2005. "RFID: The Next Serious Threat to Privacy." *Ethics and Information Technology* 7, no. 4: 221–31.

Mason, Richard O. 2007. "Four Ethical Issues of the Information Age." In J. Weckert, ed. *Computer Ethics*. Aldershot UK: Ashgate, pp. 31–40. Reprinted from *MIS Quarterly* 10: 5–12.

Moor, James H. 2000. "Towards a Theory of Privacy for the Information Age." In R. M. Baird, R. Ramsower, and S. E. Rosenbaum, eds. *Cyberethics: Moral, Social, and Legal Issues in the Computer Age*. Amherst NY: Prometheus Books, pp. 200–12.

Moor, James H. 2004. "Reason, Relativity, and Responsibility in Computer Ethics." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 40–54.

Moor, James H. 2006. "Using Genetic Information While Protecting the Privacy of the Soul." In H. T. Tavani, ed. *Ethics, Computing, and Genomics*. Sudbury MA: Jones and Bartlett, pp. 109–19.

Nissenbaum, Helen. 2004a. "Privacy as Contextual Integrity." *Washington Law Review* 79, no. 1: 119–57.

Nissenbaum, Helen. 2004b. "Toward an Approach to Privacy in Public: Challenges of Information Technology." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics*. 2nd ed. Sudbury MA: Jones and Bartlett, pp. 450–61. Reprinted from *Ethics and Behavior* 7, no. 3 (1997): 207–19.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.

Pariser, Eli. 2011. *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill NC: The University of North Carolina Press.

Scanlan, Michael. 2001. "Informational Privacy and Moral Values." *Ethics and Information Technology* 3, no. 1: 3–12.

Spinello, Richard A. 2010. "Informational Privacy." In G. Brenkert and T. Beauchamp, eds. *Oxford Handbook of Business Ethics*. Oxford, UK: Oxford University Press, pp. 366–87.

Stuckey, Mike. 2008. "Amex Rates Credit Risk by Where You Live, Shop." *MSNBC.Com*. Available at http://www.msnbc.msn.com/id/27055285/ (accessed May 18, 2009).

Tavani, Herman T. 1996. "Computer Matching and Personal Privacy: Can They Be Compatible?" In C. Huff, ed. *Proceedings of the Symposium on Computers and the Quality of Life*. New York: ACM Press, pp. 97–101.

Tavani, Herman T. 1999. "Informational Privacy, Data Mining and the Internet." *Ethics and Information Technology* 1, no. 2: 137–45.

Tavani, Herman T. 2000. "Privacy-Enhancing Technologies as a Panacea for Online Privacy Concerns: Some Ethical Considerations." *Journal of Information Ethics* 9, no. 2: 26–36.

Tavani Herman T., and James H. Moor. 2001. "Privacy Protection, Control over Information, and Privacy-Enhancing Technologies." *Computers and Society* 31, no. 1: 6–11.

Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4, no. 5: 193–220.

Werner, Jeff. 2012. "Should You Be Worried about Google's New Privacy Policy?" *NWFDailyNews.com*, March 25. Available at http://www.nwfdailynews.com/articles/google-48355-new-policy.html.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Atheneum Press.

Zimmer, Michael. 2008. "The Gaze of the Perfect Search Engine: Google as an Institution of Dataveillance." In A. Spink and M. Zimmer, eds. *Web Search: Multidisciplinary Perspectives*. Berlin: Springer-Verlag, pp. 77–99.

▶ FURTHER READINGS

Alfino, Mark. "Misplacing Privacy." *Journal of Information Ethics* 10, no. 1 (2001): 5–8.

Cavoukian, Ann."Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet." Available at http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf, 2008.

Shoemaker, David W. "Self Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity." *Ethics and Information Technology* 12, no. 1 (2010): 3–15.

Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

Spinello, Richard A. "Privacy and Social Networking." *International Review of Information Ethics* 16 (2011): 42–46.

Zimmer, Michael. "Surveillance, Privacy, and the Ethics of Vehicle Safety Communication Technologies." *Ethics and Information Technology* 7, no. 4 (2005): 201–10.