2.4.3 PUBLIC RECORDS: ACCESS VS. PRIVACY

The Web makes it easier for ordinary people to obtain information. That’s one of its major benefits. At the same time, it exposes some information to the whole world that we might prefer to be kept more restricted. Many government databases contain "public records," that is, records that are available to the general public. Examples include bankruptcy records, arrest records, marriage-license applications, divorce proceedings, property-ownership records (including mortgage information), salaries of government employees, and wills. These have long been public, but available on paper in government offices. Lawyers, investigators, real-estate brokers, and others use the records. Some state governments made millions of dollars selling personal information about drivers from motor-vehicle-department records. The murder of an actress by a man who allegedly obtained her address from the motor-vehicle department led to stricter rules about release of driver information. The federal Driver’s Privacy Protection Act of 1994 prohibits unauthorized disclosure of state motor-vehicle-department records, but it has numerous exceptions; for example, it allows disclosure to any government agency and to licensed private investigators.

Now that it is so easy to search and browse through files on the Web, more people access public records for fun, for research, for valid personal purposes—and for purposes that can threaten the peace, safety, and personal secrets of others. In a few cases, courts approved restrictions on the form in which information from government files is provided, allowing access to paper records but not electronic ones. This solution is clearly temporary. Most records are now created and stored on computer systems instead of on paper, and scanners coupled with character-recognition systems make it easy to convert older, printed records to digital form. At some point, the problems generated by a new technology by preventing its use are not likely to succeed.

To illustrate some problems and potential solutions, we consider two cases of specialized information: flight information for private airplanes and the financial statements of judges.

The pilots of the roughly 10,000 company airplanes in the U.S. file a flight plan when they fly. A few businesses have combined this flight information, obtained from government databases, with aircraft registration records, also public government records, to provide a service telling where a particular plane is, where it’s going, when it will arrive, and so on. Who wants this information? Competitors can use it to determine with whom top executives of another company are meeting. Terrorists could use it to track movements of a high-profile target. The information was available before, but not so easily and anonymously.

The Ethics in Government Act requires federal judges (about 1600 of them) to file financial disclosure reports. The public can review these reports to determine whether a particular judge might have a conflict of interest in a particular case. An online news agency sued the government to make the records available online.71 Judges object that information in the records can disclose where family members work or go to school, putting them at risk from defendants who are angry at a judge.

2.5 Protecting Privacy: Education, Technology, and Markets

2.5.1 AWARENESS

Most people have figured out by now you can’t do anything on the Web without leaving a record.

—Holman W. Jenkins Jr., 2000

The first step in protecting privacy from the risks of computer technology is awareness of how the technology works, how it is being used, what the risks are, and what tools are available to reduce exposure and unwanted uses of personal data. No one would have made the statement in the quotation at the beginning of this section a few years earlier; people did not know. (And Jenkins was somewhat optimistic; in 2000, most people probably still did not.) Since the mid 1990s, however, television programs, newspapers, magazines, pro-privacy Web sites, and many organizations have informed the public about risks to privacy from marketing and government databases and the World Wide Web. Articles and books with titles like "The Death of Privacy," can help prevent the death of privacy. The demand for privacy is being met, to some degree, by individual programmers who post free privacy-protecting software on the Web, entrepreneurs who have built new companies to provide technology-based privacy protections, large businesses that are responding to consumer demand, organized efforts of privacy advocates such as the Electronic Privacy Information Center (EPIC), and threats of regulation by government.

As consumers, once we are aware of the problems and potential solutions, we can decide to what extent we wish to use privacy-protecting tools, be more careful about the information we give out, and consider the privacy policies of businesses and Web sites we use or visit. As business managers, we can learn and implement techniques to respond to the privacy demands of customers. As computer professionals, we can design database systems and Web software that make it easier to build in privacy protection and reduce the risks of unauthorized leaks.
The market responds to consumer desire for privacy by producing tools that individuals and organizations can use to protect privacy and by encouraging businesses to adopt policies consumers prefer. We consider several examples in this section.

**PRIVACY-ENHANCING TECHNOLOGIES**

Often problems that arise as side effects of a new technology can be solved with new applications of the technology. Soon after "techies" became aware of the use of cookies by Web sites, they wrote cookie disablers and posted them on the Web. Netscape's and Microsoft's Web browsers have options to alert the user whenever a Web site is about to store a cookie and allow the user to reject it. Magazine articles and online newsletters tell people how to set this option.

Companies like Anonymizer.com and Zero-Knowledge Systems, Inc., provide services with which people can surf the Web anonymously, leaving no record of the sites they visit. Zero-Knowledge is developing digital cash, so that people can make purchases online that are not linked to their names by a credit card. Similar techniques can be used with smart cards for purchasing physical things in the offline world. (Some early attempts to implement digital cash online failed, in part because they were not convenient to use.) Extensions of these techniques have the potential for providing an unprecedented amount of privacy and solving many of the privacy problems we are discussing.

Companies are developing technologies like the Platform for Privacy Preferences (P3P) that "automatically" protect people's privacy when they use the Web. Such systems include software in Web browsers and on Web sites that an individual user specifies his or her privacy requirements. For example, a user can choose not to accept cookies, or not to visit sites unless they allow users to opt out of mailing lists. Web sites include special code that the browser reads, describing their privacy policies. The browser mediates with Web sites. A participating Web site can adapt its actions to meet the user's preferences (e.g., not send a cookie or not collect certain information). The browser can alert the user if he or she attempts to visit a site whose policies do not meet the user's privacy preferences.

A well-designed database for sensitive information includes several features to protect against leaks, intruders, and unauthorized activities. Each person with authorized access to the system should have a unique identifier and a password. Users can be restricted from performing certain operations, such as writing or deleting, on some files. User IDs can be coded so that they give access to only specific parts of a record. For example, a billing clerk in a hospital does not need access to the results of a patient's lab tests. The computer system keeps track of information about each access, including the ID of the person looking at a record and the particular information viewed or modified. This is called an audit trail. It can be used later to trace unauthorized activity. The knowledge that a system contains such provisions will discourage many privacy violations. Storing information in encrypted form reduces some abuses by unauthorized employees and intruders from the outside.

**TRUSTED THIRD PARTIES**

Mailing lists and databases with consumer-purchase histories or Web-activity records are valuable assets that give businesses a competitive advantage. The owners of such lists and databases, as much as the people in them, have an interest in preventing unlimited distribution. Thus, for example, mailing lists are not actually sold; they are "rented." When a list is rented to another organization or business, the renter does not receive a copy (electronic or otherwise): a specialized firm does the mailing. The risk of unauthorized copying is thus restricted to a small number of firms whose reputation for honesty is important to their business. This idea of using trusted third parties to process confidential data can be used in other applications too. In some states, car-rental agencies access a computer service to check the driving record of potential customers. The service examines the motor-vehicle-department records for the rental company's criteria (say, a specific number of traffic tickets or accidents) and reports a simple yes or no. The car rental company does not see the driver's record.

**PAYING FOR CONSUMER INFORMATION**

Consumer information is very valuable to marketers. In the 1990s, some privacy advocates argued that consumers should be paid for its use. In many circumstances, we are paid indirectly. For example, when we fill out a contest entry form, we trade data for the opportunity to win prizes. Many stores give discounts to shoppers who use cards that enable tracking of their purchases. A business that sells customer information might be able to charge less for its services than a competitor that does not. Many new businesses offered to trade free computers, free Internet connections, or other services (e.g., personalized product-discount coupons) for permission to send advertising messages to people or to track their Web surfing. These offers are very popular. Free-PC started the trend in 1999 with its offer of 10,000 free PCs in exchange for providing personal information and watching advertising messages. It was swapped with applications from hundreds of thousands of people in the first day. ComScore Networks, Inc., in its first few months of operation, attracted about two million people in the U.S. and other countries with its program to track Internet use. Its incentives included contests and special software that provided faster Web access. By 2000, more than a dozen companies paid people to view ads on the Web. When one such company, AllAdvantage, with millions of members, reduced the number of hours of ad reading it would pay for, many members were disappointed at the reduced earnings opportunity. The success of these businesses shows that many people do not consider the intrusion of online ads to be extremely bothersome, nor their Web surfing to be particularly sensitive. They are willing to trade some privacy for other things. People who value their privacy more highly do not sign up.
Some people view such programs as more options for consumers in general and, particularly, options for low-income people to obtain Internet service or product discounts. Some privacy advocates vehemently oppose these programs. For example, Lauren Wein-stein, founder of Privacy Forum, argues that less affluent people, to whom the attraction of free services may be strong, will be "coerced" into giving up their privacy.73

ARE BUSINESSES GETTING THE MESSAGE?

In 1998, the Federal Trade Commission examined 674 commercial Web sites and found that 92% of them collected personal information but only 14% informed people of what they did with the information. A year later, Georgetown University examined 364 of the most popular sites, those that get about 99% of Web traffic, and found that two-thirds of the sites post their policy about information use and more than three-quarters of those offer a choice about how a person's data are used.76

It has become common for credit card companies, Web sites, Internet service providers, cable companies, health companies, magazines, retail chains, and so on to have explicit policy statements about how they use the information collected from their subscribers and customers. The statements vary in clarity, completeness, and prominence. The policies vary in content and have improved over time. In the early 1990s, America Online’s policy stated that "AOL, Inc. may use or disclose information regarding Member for any purpose" (with a few exceptions, and with an opt-out option).77 By 2000, however, AOL had an 8-page privacy policy stating, among other things, that it did not use or disclose any information about where a member goes in AOL or on the Web and did not give out telephone numbers or information that links screen names with real names.78

Web-site operators pay thousands, sometimes millions, of dollars to companies that do privacy audits. Privacy auditors check for leaks of information, review the company’s privacy policy and its compliance with its policy, evaluate warnings on its Web site to alert visitors when sensitive data are requested and how they will be used, and so forth. Hundreds of large businesses established a new position called chief privacy officer; this person guides company privacy policy. DoubleClick, after its colossal blunder in trying to combine its database of consumer activity online with a database of offline personal information, hired a chief privacy officer and hired PricewaterhouseCoopers to do regular privacy audits. Just as the Automobile Association of America rates hotels, the Better Business Bureau and new organizations like TRUSTe offer their seal of approval to be posted on Web sites of companies that comply with their privacy standards.79

Large companies use their economic influence to improve consumer privacy on the Web. IBM and Microsoft decided to remove their Internet advertising from Web sites that do not post clear privacy policies. Walt Disney Company and Infosys Corporation did the same and, in addition, stopped accepting advertising on their Web sites from sites that don't post privacy policies. The Direct Marketing Association adopted a policy

---

1TRUSTe was criticized for sometimes weak standards, but it was a beginning.

26 Protecting Privacy: Law and Regulation

In Section 2.2, especially in Section 2.2.2, we considered some aspects of law and constitutional principles related to protection of privacy from government. The privacy right protected by the Fourth Amendment is the negative right against intrusion and interference by government. The main application for the discussion in this section is legal remedies for privacy problems related to personal data collected or used by other people, businesses, and organizations.

We separate legal remedies from technical, management, and market solutions because they are fundamentally different. The tools and policies described in Section 2.5 are voluntary and varied. Different people or businesses can choose from among them. Law, on the other hand, is enforced by fines, imprisonment, or other penalties. Thus we should examine uses of law more carefully. Privacy is a condition or state we can be in, like good health or financial security. To what extent should we have a legal right to it? Is it a negative right or a positive right (in the sense of Section 1.2.2)? How far should law go, and what should be left to the voluntary interplay of markets, educational efforts of public interest groups, consumer choices and responsibilities, and so forth?

2.6.1 PHILOSOPHICAL VIEWS

Until the late 19th century, legal decisions supporting privacy in social and business activities were based on property rights and contracts. An independent right to privacy was not recognized. In 1890, a crucial article called "The Right of Privacy," by Samuel Warren and Louis Brandeis,80 (later a Supreme Court Justice), argued that privacy was distinct from other rights and needed more protection. Judith Jarvis Thomson, an MIT philosopher, argued in a 1975 essay that the old view was more accurate, that in all cases requiring its member companies to inform consumers when personal information will be shared with other marketers and to give people an opt-out option.

More than a dozen credit-information companies, the three major credit bureaus among them, agreed to limit availability of sensitive consumer information, including unlisted telephone numbers, driving histories, medical records, and all information about children. In 2000, a group of major online advertising companies, led by DoubleClick, agreed to give consumers "robust notice and choice" about how marketers use their information collected online. The companies also agreed to ban the use of sensitive information, including medical information and sexual orientation, for marketing. They agreed to give consumers access to the information collected about them and to give consumers an opportunity to opt out before information collected online is combined with offline information.

There continue, of course, to be many businesses without strong privacy policies and many abuses, such as various forms of invisible information collection. The examples described here represent a strong trend, not a privacy utopia.
where a violation of privacy is a violation of someone's rights, another right has been violated.\textsuperscript{81} We present some of the claims and arguments of these papers.

One purpose of this section is to show the kinds of analyses that are done by philosophers, legal scholars, and economists in trying to elucidate underlying principles. Another is to emphasize the importance of principles, of working out a theoretical framework in which to make decisions about particular issues and cases.

**WARREN AND BRANDEIS: THE INVIOLATE PERSONALITY**

The main target of criticism in the Warren and Brandeis article is newspapers, especially the gossip columns. They vehemently criticize the press for "overshooting . . . obvious bounds of propriety and decency." The kinds of information of most concern to them are personal appearance, statements, acts, and interpersonal relationships (marital, family, and others).\textsuperscript{82} Warren and Brandeis take the position that people have the right to prohibit publication of facts about themselves and photographs of themselves. Warren and Brandeis argue that, for example, if someone writes a letter in which he says he had a fierce argument with his wife, that fact is protected and the recipient of the letter cannot publish it. This claim is not based on any property right or other rights besides privacy; rather, it is part of the right to be left alone. Warren and Brandeis base their defense of privacy rights on, in their often-quoted phrase, the principle of "an inviolate personality."

Privacy violations can be addressed by laws against other wrongs, such as slander, libel, defamation, copyright infringement, violation of property rights, and breach of contract, but Warren and Brandeis argue that there remain many privacy violations that those other laws do not cover. For example, publication of personal or business information could constitute a violation of a contract (explicit or implied), but not if someone has no contract or relationship of trust with the person who is asked to publish. Libel, slander, and defamation laws protect us when someone spreads false or damaging rumors about us, but they do not apply to true personal information whose exposure makes us uncomfortable. According to Warren and Brandeis, privacy is distinct and needs its own protection. They allow exceptions for publication of information of general interest (news), use in limited situations when the information concerns another person's interests, and oral publication. (They were writing before radio and television, so oral publication meant a quite limited audience.)

**JUDITH JARVIS THOMSON: IS THERE A RIGHT TO PRIVACY?**

Judith Jarvis Thomson argues the opposite point of view. She gets to her point after examining a few scenarios.

Suppose you own a copy of a magazine. Your property rights include the right to refuse to allow others to read, destroy, or even see your magazine. If someone does anything to your magazine that you did not allow, that person is violating your property rights. For example, if someone uses binoculars to see your magazine from a neighboring building, that person is violating your right to exclude others from seeing it. It does not matter whether the magazine is an ordinary news magazine (not a privacy issue), or a pornographic magazine, or any other magazine you do not want others to know you read (a privacy issue). The right violated is your property right.

You may waive your property rights, intentionally or inadvertently. If you absent-mindedly leave the magazine on a park bench, someone could take it. If you leave it on the coffee table when you have guests at your home, someone could see it. If you read the magazine on a bus, and someone sees you and tells other people that you read dirty magazines, your rights are not violated. The person might be doing something improper, unfriendly, or cruel, but not something that violates a right.

Our rights to our person and our bodies include the right to decide to whom to show various parts of our bodies. By walking around in public, most of us waive our rights to prevent others from seeing our faces. (Some Muslim women cover their faces, exercising their right to keep others from viewing them.) If someone uses binoculars to spy on us at home in the shower, they are violating our rights to our person. Similarly, according to Thomson, our right to our person includes the right to decide who may listen to us. Someone who eavesdrops on our intimate conversations at home violates our right to our person. If we speak in public, we waive the right, and people may listen.

If someone beats you on to get some information, the beater is violating your right to be free from physical harm done by others. If the information is the time of day, privacy is not at issue. If the information is more personal, then your privacy is compromised, but the right violated is your right to be free from attack. On the other hand, if a person peacefully asks whom you live with or what your political views are, then no rights are violated. If you choose to answer and do not make a confidentiality agreement, the person is not violating your rights by repeating the information to someone else, though it could be inconvenient to do so. However, if the person agreed not to repeat the information, then but then, it does not matter whether or not the information was sensitive; the confidentiality agreement has been violated.

In these examples, whether or not privacy is compromised depends on the kind of information. In each case, there is no violation of privacy without violation of some other right, such as the right to control our property or our person, the right to be free from violent attack, or the right to form contracts (and expect them to be enforced). Thomson concludes, "I suggest it is a useful heuristic device in the case of any purported violation of the right to privacy to ask whether or not the act is a violation of any other right, and if not whether the act really violates a right at all."\textsuperscript{83}

**CRITICISMS OF WARREN AND BRANDEIS AND OF THOMSON**

Critics of the Warren and Brandeis position argue that their arguments do not provide a workable principle or definition from which to conclude that a privacy-right violation occurs. Their notion of privacy is too broad; it conflicts with freedom of the press; it appears to make any unauthorized mention of a person a violation of the person's right. Some critics present theories and examples, in addition to Thomson's, to show that existing legal wrongs encompass privacy violations; for example, trespass and appropriation of a person's likeness.\textsuperscript{84}
Critics of Thomson present examples in which a right to privacy (not just a desire for privacy), but no other right, is violated. Thomson's notion of the right to our person can be seen as vague or too broad. Her examples might (or might not) be a convincing argument for the thesis that considering other rights can resolve privacy rights questions, but no finite number of examples can prove such a thesis. Neither article directly refutes the other. Their emphases are different. Warren and Brandeis focus on how information is used (publication); Thomson focuses on how it is obtained. This distinction sometimes underlies differences in arguments by those who advocate strong legal regulations on use of personal data and those who advocate more reliance on technical and market solutions.

APPLYING THE THEORIES

How do the theoretical arguments apply to the privacy issues related to the vast amount of personal data in computerized databases and the practice of tracking our activities on the Web?

Throughout Warren and Brandeis, the objectionable action is publication of personal information—its widespread, public distribution. Many court decisions since the appearance of their article have taken this point of view. If information in consumer databases were published (in print or electronically, say on the Web), that would violate the Warren and Brandeis notion of privacy. A plaintiff might well win a case if his or her consumer profile were published or if he or she were on a published list of people who bought condoms or did not pay their debts. But publication is not the main concern in the current context of consumer databases and Web tracking. Warren and Brandeis and various court decisions allow disclosure of personal information to people who have an interest in it. By implication, they do not preclude, for example, disclosure of a person's driving record to a car rental company from which he or she wants to rent a car or disclosure of information about whether someone smokes cigarettes to a life insurance company from whom the person is trying to buy insurance. They do not preclude use of consumer information to generate targeted mailing lists if the lists are not published. (If disclosure of the information violates a trust or confidence or contract, then it is not permissible.)

An important aspect of both the Warren and Brandeis paper and the Thomson paper is that of consent. There is no privacy violation if information is obtained or published with the person's consent.

TRANSACTIONS

No matter which of the views presented so far in this section you find convincing or weak, we have another puzzle to consider: how to apply philosophical and legal notions of privacy to transactions, which automatically involve more than one person. The following scenario will illustrate the problem.

One day in the small farm community of Friendlyville, Joe buys five pounds of potatoes from Maria, and Maria sells five pounds of potatoes to Joe. (Describe the transaction in this repetitive manner to emphasize that there are two people involved and two sides to the transaction.)

Either Maria or Joe might prefer the transaction to remain secret. Joe might be embarrassed that his own potato crop failed. Or Joe might be unpopular in Friendlyville, and Maria fears the townspeople will be angry at her for selling to him. Either way, we are not likely to consider it a violation of the other's rights if Maria or Joe talks about the purchase or sale of the potatoes to other people in town. But suppose Joe asks for confidentiality as part of the transaction. Maria has three options. (1) She can say OK. (2) She can say no; she might want to tell people she sold potatoes to Joe. (3) She can agree to keep the sale confidential if Joe pays a higher price. In the latter two cases, Joe can decide whether to buy the potatoes. On the other hand, if Maria asks for confidentiality as part of the transaction, Joe has three options. (1) He can say OK. (2) He can say no; he might want to tell people he bought potatoes from Maria. (3) He can agree to keep the purchase confidential if Maria charges a lower price. In the latter two cases, Maria can decide whether to sell the potatoes.

Privacy includes control of information on oneself, but the point here is that there is no clear reason for either party to the transaction to have more right than the other to control information about the transaction. If a confidentiality agreement is made, then the parties are obliged to respect it.

If control of the information about the transaction is to be assigned to one of the parties, we need a firm philosophical foundation for choosing which party gets it. Warren and Brandeis are not of much help. They say we should have control of publication of facts about ourselves. Even if we consider discussion of the transaction in the town square to be publication, we still have the question: Is the transaction a fact about Maria or a fact about Joe? There does not appear to be a convincing reason to favor one over the other, yet this problem is critical to legal policy decisions about consumer information in computer databases.

Philosophers and economists often use simple two-person transactions or relationships, like the Maria/Joe scenario, to try to clarify the principles involved in an issue. Do the observations and conclusions about Maria and Joe generalize to large, complex societies and a global economy, where one party to a transaction is often a business? All transactions are really between people, even if indirectly. So if a property right or a privacy right in the information about a transaction is to be assigned to one of the parties, we need an argument showing how the transaction in a modern economy is different from the one in Friendlyville. In the next section, we will discuss two viewpoints on the regulation of information about consumer transactions: the free-market view and the consumer-protection view. The free-market view treats both parties equally, whereas the consumer-protection view includes arguments for treating the parties differently.
Chapter 2: Privacy and Personal Information

1. Truth in Information Gathering. Organizations collecting personal data (including government agencies and businesses) should clearly inform the person providing the information if it will not be kept confidential (from other businesses, individuals, and government agencies) and how it will be used. They should be liable for violations.

2. Freedom in Information Contracting. People should be free to enter agreements (or not enter agreements) to disclose personal information in exchange for a fee or for services according to their own judgment.

3. Freedom of Speech and Commerce. People (as well as businesses and organizations) should not be prevented by law from disclosing facts independently and uninterruptedly discovered (e.g., without theft, trespass, or violation of contractual obligations).

Figure 2.3 Freedom of Information Use Guidelines

2.6.2 Contrasting Viewpoints

When asked "If someone sues you and loses, should they have to pay your legal expenses?" more than 80% of people surveyed said "yes." When asked the same question from the opposite perspective: "If you sue someone and lose, should you have to pay their legal expenses?" about 40% said "yes."

The political, philosophical, and economic views of many scholars and advocates who write about privacy differ. As a result, their interpretations of various privacy problems and their approaches to solutions often differ, particularly when they are considering regulation of personal information collected and used by businesses.4 We will contrast two perspectives; I call them the free-market view and the consumer-protection view.

The Free-Market View

People who prefer market and contractual solutions for privacy problems tend to emphasize the diversity of individual tastes and values, the flexibility of technological and market solutions, the response of markets to consumer preferences, and the flaws of detailed or restrictive legislation and regulatory solutions.

Figure 2.3 shows a set of guidelines that express a free-market viewpoint for use of personal information.86 It incorporates informed consent, freedom of contract, and free flow of information acquired without violating rights or agreements. The market viewpoint respects the right and ability of consumers to make choices for themselves that are based on their own values. Market supporters expect consumers to take the responsibility that goes with freedom, for example, to read contracts or to understand that desirable services have costs.

4 These trends to be more agreement when considering privacy threats and intrusions by government.

Protecting Privacy: Law and Regulation

Market supporters prefer to avoid restrictive legislation and detailed regulation for several reasons. They argue that the political system is a worse system than the free market for determining what consumers want in the real world of trade-offs and costs. It is impossible for legislators to know in advance how much money, convenience, or other benefits people will want to trade for more or less privacy. Businesses respond over time to the preferences of millions of consumers expressed through their purchases. Different companies can offer different levels of privacy, satisfying different consumers. In response to the desire for privacy expressed by many people, the market provides a variety of privacy-protection tools.

Market supporters argue that laws requiring specific policies or prohibiting certain kinds of contracts violate the freedom of choice of both consumers and businesses. Private firms are owned by individuals or groups of individuals who have invested their own resources in the business. They should be free to offer the selection of products, services, and terms that they choose. Consumers should have the freedom to sell personal data if they choose.

We cannot always expect to get exactly the mix of attributes we want in any product, service, or job; it could be that no seller or employer chooses to offer that combination. Just as we might not get cheeseless pizza in every pizza restaurant or find a car with the exact set of features we want, we might not be able to get both privacy and special discounts. We might not be able to get certain Web sites—or magazines—without advertising, or a specific job without agreeing to provide certain personal information to the employer. These compromises are not unusual or unreasonable when interacting with other people.

There is an extraordinary range in the amount of privacy different people want. Some tell details of their personal lives on television shows. Some set up personal Web pages describing their lives and families to the world. Some gladly sign up for free services in exchange for allowing their activity to be tracked. Others use cash to avoid leaving a record of their purchases, encrypt all their e-mail and use anonymizers when surfing the Web, never give personal information on warranty cards, and are appalled and angry when information is collected about them. The free-market viewpoint sees privacy as a "good," both in the sense that it is desirable and that it is something we can obtain varying amounts of by buying or trading in the economy, like food, entertainment, and safety. Just as some people choose to trade some safety for excitement (bungee jumping, motorcycle riding), money (buying a cheaper, but less safe product), or convenience, some choose different levels of privacy. As with safety, law can provide minimum standards, but should allow the market to provide a wide range of options to meet the range of personal preferences.

The Consumer-Protection View

Advocates of strong privacy regulation emphasize all the unsettling business uses of personal information we have mentioned throughout this chapter. They argue for more stringent consent requirements, strong limitations on secondary uses, legal restrictions on consumer profiling, and prohibitions on certain types of contracts or agreements to
disclose data. They urge, for example, that companies be required by law to have opt-in policies because the opt-out option may not be obvious or easy enough for consumers who would prefer it. As we mentioned earlier, many privacy advocates are very critical of contracts to trade free computers and Web services for either personal information, or consent to the monitoring of Web activity.

The focus of this viewpoint is to protect consumers against abuses by businesses and against their own lack of knowledge, judgment, or interest. Advocates of the consumer-protection viewpoint argue that people do not understand the risks of agreeing to disclose personal data and that business privacy policies are vague, in small print, or hard to find. (Thus, many privacy advocates support bans on generalized consent forms or waivers.) Consumer advocate and privacy "absolutist" Mary Gardner Jones does not accept the idea of consumers consenting to dissemination of personal data. She said, "You can't expect an ordinary consumer who is very busy trying to earn a living to sit down and understand what [consents] means. They don't understand the implications of what use of their data can mean to them." She said the idea that some consumers like having their names on mailing lists is a myth created by the industry.87 The view that informed consent is not sufficient protection was expressed by a former director of the ACLU's Privacy and Technology Project who urged a Senate committee studying confidentiality of health records to "re-examine the traditional reliance on individual consent as the linchpin of privacy law."88

Consumer and privacy protection groups argue for banning various kinds of contracts and transactions. For example, they supported the laws that stopped merchants from asking for a telephone number when a customer uses a credit card. Some advocate bans on all sales of personal medical data even if the person consents.

These advocates would argue that the Joe/Maria scenario in Friendlyville, described in Section 2.6.1, is not relevant in a complex society. The imbalance of power between the individual and a large corporation is one reason. Another is that, in Friendlyville, the information about the transaction circulates to only a small group of people, whom Joe and Maria know. If someone draws inaccurate or unfair conclusions, Joe or Maria can talk to the person and present his or her explanations. In a larger society, information circulates among many strangers, and we often do not know who has it and what decisions about us are being based on it.

A consumer cannot realistically negotiate contract terms with a business; at any specific time, the consumer can only accept or reject what the business offers. And the consumer is often not in a position to reject it. If we want a loan for a house or car, we have to accept whatever terms lenders currently offer. If we need a job, we are likely to agree to disclose personal information against our true preference because of the economic necessity of working.

The business-policy improvements that have occurred resulted from government action or the threat of it, not from business response to consumer preferences. Self-regulation by business does not work. Businesses sometimes don't follow their stated policies. Consumer pressure is sometimes effective, but some companies ignore it. In

stead, all businesses must be required to adopt pro-privacy policies. Privacy-enhancing technologies are far from perfect, hence not good enough to protect privacy.

The consumer-protection viewpoint sees privacy as a right rather than something to be bargained about. For example, a Web site jointly sponsored by the Electronic Privacy Information Center and Privacy International frames the slogans "Privacy is a right, not a preference" and "Notice is not enough."89 The latter indicates that they see privacy as a positive right, or claim-right (in the terminology of Section 1.2.2). As a negative right, privacy allows us to use anonymizing technologies and to refrain from interacting with those who request information we do not wish to supply. As a positive right, it means we can stop others from communicating about us. A spokesperson for the Committee for Democracy and Technology expressed that view in a statement to Congress, saying that we must incorporate into law the principle that people should be able to "determine for themselves when, how and to what extent information about them is shared."90

2.6.3 CONTRACTS AND REGULATIONS

A BASIC LEGAL FRAMEWORK

A good basic legal framework that defines and enforces legal rights and responsibilities is essential to a complex, robust society and economy. One of its tasks is enforcement of agreements and contracts. Contracts—including freedom to form them and enforcement of their terms by the legal system—are a mechanism for implementing flexible and diverse economic transactions that take place over time and between people who do not know each other well or at all.

We can apply the idea of contract enforcement to the published privacy policies of businesses, organizations, and Web sites. The Toymart case is an example. Toymart, a Web-based seller of educational toys, collected extensive information on about 250,000 visitors to its Web site, including family profiles, shopping preferences, and names and ages of children. Toymart had promised not to release this personal information. When the company filed for bankruptcy in 2000, it had a large amount of debt and virtually no assets—except its customer database, which was valued highly. Toymart's creditors wanted the database sold to raise funds to repay them. Toymart offered the database for sale, causing a storm of protest. Consistent with the interpretation that Toymart's policy was a contract with the people in the database, the bankruptcy-court settlement reached in 2001 included destruction of the customer database.

A second task of a legal system is to set defaults for situations that are not explicitly covered in contracts. Suppose a Web site posts no policy about what it does with the information it collects. What should the site be legally permitted to do with the information? Many sites and offline businesses act as though the default is that they can do anything they choose. A privacy-protecting default would be that the information could be used only for the direct and obvious purpose for which it was supplied. The legal system can (and should) set special confidentiality defaults for sensitive information, such as medical
and financial information, that tradition and most people consider private. If a business or organization wants to use information for purposes beyond the default, it would have to specify those uses in its policies, agreements, or contracts or request consent for its uses. Many business interactions do not have written contracts, so the default provisions established by law are very influential (hence controversial).

REQUIRING SPECIFIC CONSENT POLICIES

When we go beyond the basic framework, there is more controversy. We consider consent policies as an example of privacy-protecting regulation. The principle of informed consent can be incorporated into law in a variety of ways differing in their levels of control. Here are four levels:

1. Businesses and organizations must clearly state their policy for use of personal information. If a person proceeds and makes a purchase, explores the Web site, provides information, and so on, consent to the policy is assumed.
2. Businesses and organizations must provide an opt-out option.
3. Businesses and organizations must use an opt-in policy.
4. Businesses and organizations must obtain consumer consent for each individual secondary use, disclosure, or transfer of their personal information.

What level should the law enforce? The first is the least intrusive, but provides the least privacy protection. The strictest level of regulation above provides the most privacy protection. Privacy advocates who think blanket consent agreements are too broad recommend this regulation; consumers do not realize all the ways others may use the information. This option has an attribute economists call "high transaction cost." It could be so expensive and difficult to implement that it would eliminate most secondary uses of information, including those many consumers find desirable. Market supporters oppose it for this reason and because it violates freedom to offer and form contracts with broader consent provisions.

REGULATION

Technical tools for privacy protection (like those described in Section 2.5.2), market mechanisms, and self-regulation by businesses are not perfect. Some privacy advocates consider this a strong argument for regulatory laws. Regulation is not perfect either. We must evaluate regulatory solutions by considering effectiveness, costs and benefits, side effects, and ease of use (clarity), just as we do throughout this book for computer technology itself and for other kinds of potential solutions to problems caused by technology. Whole books can be written on the pros and cons of regulation. We briefly point out some of its weaknesses in the next four paragraphs.

The actual laws that get passed often depend more on the current focus of media attention and special-interest pressure than on well thought-out principles and true cost/benefit trade-offs.51

It is extremely difficult to write reasonable regulations for complex situations. General statements of principle are not precise enough in a context where people may be fined or jailed. When laws are not written carefully, they often have unintended effects or interpretations.52 They could apply where they do not make sense or where people simply do not want them.

Regulations often have high costs, both direct dollar costs to businesses (and, ultimately, consumers) and hidden or unexpected costs, such as loss of services or increased inconvenience. Consider the response to the Children's Online Privacy Protection Act (COPPA) which required that Web sites get parental permission before collecting personal information from children under 13 (Section 2.3.2). Some sites deleted online profiles of all children under 13, some canceled their free e-mail and home pages for kids, and some banned children under 13 entirely. (The New York Times does not allow children under 13 to register to use its Web site.) An attorney who helps sites meet COPPA’s requirements estimated the cost of compliance at $60,000–100,000 per year, a lot for a small business, not a burden for large ones like AOL and Disney.53 Regulations often provide a relative benefit to large businesses and organizations over smaller ones because they have the legal department to deal with the rules and the revenue to absorb the added costs. Even laws like COPPA, one of the less controversial privacy regulatory laws, must be examined carefully to determine whether they are effective and whether the increased cost or loss of some services is a reasonable price for the increased protection.

Laws that include very specific regulations prevent other options from being tried.

OWNERSHIP OF PERSONAL DATA

Some economists, legal scholars, and privacy advocates propose giving people property rights in information about themselves. The concept of property rights can be very useful even when applied to intangible property (intellectual property, for example), but there are problems in using this concept for personal information. First, as we have seen, activities and transactions often involve at least two people, each of whom would have reasonable but conflicting claims to own the information about the transaction. Some personal information does not appear to be about a transaction, but there still may be problems in assigning ownership. For example, your birthday is recorded in some databases. Do you own your birthday? Or does your mother own it? After all, she was a more active participant in the event!

The second problem with assigning ownership of personal information arises from the notion of owning facts. (Copyright, the main topic of Chapter 6, protects intangible property such as computer programs and music, but facts cannot be copyrighted.) Ownership of facts would severely impair the flow of information in society. Information is stored on computers, but it is also stored in our minds. Can we own facts about ourselves without violating the freedom of thought and freedom of speech of others?

Some of the information of most concern to privacy advocates is information that can lead to denial of a job or some kind of service or contract (e.g., a loan). Federal
Judge Richard Posner offered a different perspective when he considered how to allocate property rights to information. He argued that a person should not have a property right to "discreditable" personal information (e.g., one's criminal history or credit history) or other information whose concealment aids people in misrepresentation, fraud, or manipulation.44 Although it may be unreasonable to assign ownership in individual facts, another issue is whether we can own our "profiles," that is, a collection of data describing our activities, purchases, interests, and so on. We cannot own the fact that our eyes are blue, but we do have the legal right to control some uses of our photographic image. In almost all states, a person's photograph cannot be used for commercial purposes without the person's consent. Should our consumer profiles be treated the same way? How can we distinguish between a few facts about a person and a "profile"?

**CONFLICTS WITH FREEDOM OF SPEECH**

Law professors Eugene Volokh and Tom W. Bell argue that laws that prohibit communicating information about people's transactions violate freedom of speech. (Contractual agreements not to transfer data do not violate free speech.) Courts have made some exceptions to the First Amendment, for example, for libel and for some advertising, but not for transfer of commercially valuable information. Volokh argues that it would be unwise to create such an exception for facts about people's transactions and activities. Advocates of strict laws regulating transfer of such information argue that it does not have the social value and significance of political speech and hence should not have First Amendment protection. Volokh points out that a similar argument is used by supporters of laws to censor speech with sexual content. It is risky to chip away at the First Amendment by designating more categories of speech not worthy of protection.45

Some groups advocate restrictions on sharing of information that might facilitate negative decisions about people, for example, landlords sharing a database with information about tenant payment histories. Should landlords have as much right to communicate to each other about bad tenants as tenants have to communicate about bad landlords? One of the main arguments that led the Supreme Court to rule Internet censorship laws unconstitutional was that people could use filtering software to avoid pornography and other undesirable material. (We discuss these laws and arguments in Chapter 5.) Bell points out that the same reasoning applies to laws that would restrict freedom of speech by businesses about Internet users.46 Web surfers can use a variety of tools such as cookie disablers and anonymizers. Many of the same organizations that successfully fought censorship laws, partly on the grounds that self-help technologies were available, support laws that restrict business speech, partly on the grounds that privacy enhancing technologies are not perfect. Bell sees these positions as inconsistent; he says both kinds of laws restrict speech that some people argue can be harmful, but that both kinds of laws are unnecessary and have similar constitutional problems.

**PROTECTING PRIVACY: LAW AND REGULATION**

**PRIVACY REGULATIONS IN THE EUROPEAN UNION**

The European Union (EU) passed a comprehensive privacy directive covering processing of personal data.47 It defines "processing" to include collection, use, storage, retrieval, transmission, destruction, and other actions. The 30-page directive sets forth general principles that the 15 EU member nations were required to implement in their own laws. The principles, similar to the privacy principles in Figure 2.2, include the following:

1. Personal data may be collected only for specified, explicit purposes and must not be processed for incompatible purposes.
2. Data must be accurate and up to date. Data must not be kept longer than necessary.
3. Processing of data is permitted only if the person consented unambiguously, or if the processing is necessary to fulfill contractual or legal obligations, or if the processing is needed for tasks in the public interest or by official authorities to accomplish their tasks (or a few other reasons).
4. Special categories of data, including ethnic and racial origin, political and religious beliefs, health and sex life, and union membership, must not be processed without the subject's explicit consent. Member nations may outlaw processing of such data even if the subject does consent.
5. People must be notified of the collection and use of data about them. They must have access to the data stored about them and a way to correct incorrect data.
6. Processing of data about criminal convictions is severely restricted.

While the European Union has much stricter regulations than the U.S. on collection and use of personal information by the private sector, some civil libertarians believe that the European Directive does not provide enough protection from use of personal data by government agencies.

The EU Data Privacy Directive prohibits transfer of personal data to countries outside the European Union that do not have an adequate system of privacy protection. This part of the Directive caused significant problems for companies that do business both in and outside of Europe and might normally process customer and employee data outside the EU. In 2001, the EU determined that Australia, for example, did not have adequate privacy protection. Australia allows businesses to create their own privacy codes consistent with the government's National Privacy Principles. The Australian government argued that it had adequate protection. The U.S. has privacy laws covering specific areas such as medical information, video rentals, driver license records, and so on, but does not have comprehensive privacy laws covering all personal data. Business and government officials worked to develop standards other than national laws that could be accepted as meeting the requirement for adequate privacy protection. Possibilities include business privacy policies (enforceable by law in some cases) and certifications by independent organizations such as TRUSTe and the Better Business Bureau's BBBOnline Privacy Seal Program. In
2000, the EU agreed to the "Safe Harbor" plan, under which companies outside the EU that agree to abide by a set of privacy requirements similar to the principles in the Data Protection Directive may receive personal data from the EU.98 Many privacy advocates describe U.S. privacy policy as "behind Europe" because the U.S. does not have comprehensive federal legislation regulating personal data collection and use. Others point out that the U.S. and Europe have different cultures and traditions. European countries tend to put more emphasis on regulation and centralization, especially concerning commerce, whereas the U.S. tradition puts more emphasis on contracts, consumer pressure, and the flexibility and freedom of the market.

When the EU Directive was passed, in 1995, member nations were required to implement its principles in their own laws within three years. In 2000, the European Commission determined that many countries had not yet complied. In 2001, a study done by Consumers International found that 60% of European Web sites did not comply with the Privacy Directive requirement that Web sites provide an opt-out option, while almost 60% of the most popular sites in the U.S. offered an opt-out option. The study also found that about a third of EU sites that collected data on users posted their privacy policies, and 62% of U.S. sites did. The study, while critical of privacy policies on both U.S. and EU sites, concluded that "despite tight EU legislation ... U.S.-based sites tend to set the standard for decent privacy policies."100 Consumer and privacy advocates argued that in the EU, even though enforcement was weak, people have legal recourse, whereas in the U.S. they often do not.

**EXERCISES**

**Review Exercises**

2.1 What does the term personal information mean?

2.2 What does the term invisible information gathering mean? Give an example.

2.3 What does the term secondary use mean? Give an example.

2.4 Give an example of computer technology being used to collect personal information that existed before computer technology, but wasn't collected at all before.

2.5 Give one example in which release of someone's personal information threatened the person's safety.

2.6 Describe two tools people can use to protect their privacy on the Web.

2.7 Explain the difference between opt in and opt out policies for distribution of a customer's name and address (and other personal information) to other businesses.

---

98 For example, German laws prohibit or severely restrict discounts, rebates, and sales; more hours are limited by law; and businesses could not advertise unconditional return policies or that they give a contribution to charity for each sale. Some of these laws, in force for 90 years, are now being repealed because of globalization and competition from the Internet. They were defended on the grounds that discounts and guarantees confuse or trick consumers.

99 General Exercises

2.8 List two government databases that probably have information about you. For each one, tell what service or benefit, if any, you get in exchange for providing information about yourself.

2.9 List two private databases that probably have information about you. For each one, tell what service or benefit, if any, you get in exchange for providing information about yourself.

2.10 A company that supplies filtering software to schools (to block access by children to Web sites with violence or pornography) sold statistical data about the sites visited by school children. The data did not identify the children or individual schools. Was this a privacy violation? Why or why not?

2.11 Many telephone directories on the Web do not provide a reverse directory feature. That is, they do not allow a user to type in a telephone number and find out to whom it belongs.

- a) Give some arguments for and against this policy. Do you think it is a good policy?

- b) Printed reverse directories existed in book form before the Internet. How might making them available on the Web change their use and impact?

2.12 A confidential file containing the names of about 4000 AIDS patients was sent from a county health department to a newspaper, presumably by a disgruntled employee.

- a) Would this have been more or less likely to have happened if the names were in paper files, not electronic files? Why?

- b) What are some ways this leakage of sensitive data could have been prevented?

2.13 A city government wants to track down people who run small businesses and do not pay the city's $125 business-license fee. The city hired a private detective to obtain IRS tax records of city residents and determine who has reported small-business income to the IRS but not paid for a license.

- a) What arguments might the city government give in support of this action? What arguments might privacy advocates give against it?

- b) Do you think this application of computer matching should be permitted or prohibited? Give your reasons.

2.14 Suppose a small political party strongly opposes an existing law, for example, the income tax or the law against smoking marijuana. Consider the possibility of allowing government agencies like the IRS and the FBI to use the voter registration database (which includes a personal party affiliation in some states) to initiate investigations of party members to see whether they comply with the existing laws. Give arguments in favor of this give arguments in opposition. Which side do you think is stronger? Why?

2.15 The National Insurance Crime Bureau maintained a big database of suspicious insurance claims to be checked for fraud. Federal, state, and local law enforcement agencies had direct, almost unlimited access to the database. When the NICB announced plans in 1997 to expand the database to include all insurance claims, privacy advocates objected. What are some advantages of the expanded database? What are some privacy concerns?

2.16 The Federal Aviation Administration has proposed that airlines be required to collect the Social Security number of each passenger. Discuss some possible reasons for this and some possible risks. Evaluate them. Is the proposal a good idea?

2.17 Give an example of a database whose access by law-enforcement agents without a court order seems inconsistent with the spirit of the Fourth Amendment to the U.S. Constitution. (Use an example not discussed in Section 2.2.2.)

2.18 Describe some uses of satellite surveillance that you think are acceptable extensions of traditional law enforcement activities and capabilities. Describe some uses where the technology makes a fundamental change that is not acceptable. Explain your reasoning.
2.19 Police used to search manually through mug shot (photos of people who have been arrested) to find one that matched a witness’ description of a person who committed a crime. Modern computer techniques allow police to search large databases of digitized photos. What are some benefits and some risks of expanding the search to include all driver’s-license photos?

2.20 A member of the Tampa, Florida, City Council described the camera and face-recognition system installed in a Tampa neighborhood (Section 2.2.3) as a "public safety tool, no different from having a cop walking around with a mug shot." Is he right? What are some similarities and differences, relevant to privacy, between the camera system and a cop walking around?

2.21 An individual sets up a 24-hour-a-day webcam, on an island on the Atlantic coast, aimed at a ferry dock used by local people and tourists. People could visit his Web site to check on weather conditions, to determine if ferry service were likely to be canceled. But some people complained that the webcam violated their privacy. Suppose you are asked to help settle the dispute. What solution would you suggest? What arguments would you give?

2.22 Computer chips are implanted into pets and farm animals so they can be identified if they get lost. Some people suggest using the same technology for children. Discuss the privacy implications of such proposals. What are the risks? Do the benefits outweigh the risks? If there were a bill in Congress to require ID chips in children, would you support it? Why?

2.23 Consumers Union, publisher of Consumer Reports, uses a huge mailing-list broker to find potential customers, but Consumer Reports does not give information on its subscribers to the list broker. First take the position that their behavior is inconsistent and hypocritical. Give arguments for this position. Next take the position that the policy is reasonable. Give arguments for this position. Which side you think is more persuasive? Which principles or points are most important?

2.24 When formulating a policy on whether certain government records should be open to the public, we must anticipate a broad range of uses. Consider motor-vehicle records. Formulate a policy about access to the database by the news media. (News media could include both a newspaper trying to get home addresses from vehicle license-plate numbers for cars parked at an abortion clinic and a newspaper trying to get home addresses from vehicle license-plate numbers for cars parked at a Ku Klux Klan rally).

2.25 Give arguments in favor of and opposed to a law to require that credit bureaus send a copy of each person’s credit report to the person once a year (without charge).

2.26 A business maintains a database containing the names of shoppers. It distributes the list to stores that subscribe.

a) Should such a service be illegal as a violation of privacy? (Give reasons.)

b) Describe the likely position of each of Warren and Brandeis, Judith Thomson (Section 2.6.1), Richard Posner (Section 2.6.3), and Eugen V. Volokh (Section 2.6.3), with their reasons, on this question.

c) Would your answer to part (a) differ if the question were about a database of tenant history available to landlords? How and why?

2.27 "Caller ID" is the feature that displays the telephone number of the caller on the telephone of the recipient of a telephone call.

a) What aspect of privacy (in the sense of Section 2.1.1) does Caller ID protect for the recipient of the call? What aspect of privacy does Caller ID violate for the caller?

b) What are some good reasons why a nonbusiness, noncriminal caller might not want his or her number displayed?

c) What are some positive and negative business uses of caller ID?

d) In your state, what options are available for using or blocking Caller ID? Do you consider them reasonable?

2.28 Suppose students who live in a dormitory on a college campus are given cards with a magnetic strip that opens the front door of the dorm. Students are not told that each card contains the individual student identifier and that a record of each use of the card is kept. What are possible good purposes of such record keeping? What are some problems with it? Is it right? Is it okay if students are told? Give arguments and examples to support your answers.

2.29 A company called, say, Digitizer provides a service for many other companies by converting their paper documents to digital files on CDs. The documents include employee information, medical records, business records, and many others. Digitizer hires relatively unskilled employees to organize the documents and get them ready to scan.

a) What are some potential risks here? Describe at least two actual examples with some similarity to this situation.

b) Describe some actions Digitizer can take or policies it can adopt to reduce the risks.

2.30 Suppose you want to borrow $200,000 to buy a house. List all the kinds of information you think a mortgage lender might ask for and a likely reason for each. Which, if any, of the items do you think is not needed? Why?

2.31 One writer defines privacy as "freedom from the inappropriate judgement of others." Is this a good definition of privacy? Why or why not?

b) Suppose we use this definition. Should people have a positive right (claim-right) for this kind of privacy? Why or why not? Should people have a negative right (liberty) for this kind of privacy? Why or why not? (See Section 1.2.2 for explanations of negative and positive rights.)

2.32 a) Consider a company that specializes in information services or manages databases with personal information (e.g., a popular Web site, a large retailing chain, a credit-card company). The vice president for privacy policy in the company recommends that the staff prepare a privacy-impact study for any new information service or database the company develops and that the study be used in deciding whether to proceed with the new service and how to design it. Give factors or arguments the president of the company should consider for and against this policy. Should the policy be adopted? Why?

b) A privacy-advocacy group recommends that privacy impact studies be required by law, as are environmental-impact studies, to assess the implications of new information systems on consumer privacy. The study would have to be prepared by a licensed privacy analyst and submitted to a government agency for approval before a company could use or market the new system. Give arguments for and against such a law. Should the law be passed? Why?

2.33 Give an explanation, with examples and/or analogies, to describe what it would mean for privacy to be a negative right (liberty). Do the same for considering privacy a positive right (claim-right). (See Section 1.2.2 for explanations of negative and positive rights.) Which kind of right, if either, seems more appropriate for privacy? Why?

2.34 Many privacy activists propose that the United States establish an office or position at the federal government level to oversee and regulate privacy issues. (Several European countries have such an office.) Give arguments for and against this proposal.
Assignments

These exercises require some research or activity.

2.35 Find out what policy your university has about releasing the names, addresses, and telephone numbers of students either individually or as a list. Is there an online student directory? Are there any other policies that students should be aware of?

2.36 Get a warranty form or an application from a local supermarket, discount store, or video rental store for a check-cashing card or store club membership card. Does it say anything about how information about the applicant will be used? If so, summarize the statement.

2.37 Find a Web site at which people can buy something online with a credit card. Look for the privacy policy that tells how the site uses the customer information it collects. Write a brief summary of the privacy policy. Include the URL, the business name, and the type of product. Also, tell how many sites you looked at before finding one with a privacy policy.

2.38 The Telephone Consumer Protection Act of 1991 regulates telemarketing. Find this law and summarize its main provisions.

2.39 Find a recent application of smart cards. Discuss its privacy implications and protections.

Class Discussion Exercises

These exercises are for class discussion, perhaps with short presentations prepared in advance by small groups of students.

2.40 Are businesses that provide free Internet services or PCs in exchange for tracking Web activity offering a fair option for consumers, or are they unfairly taking advantage of low-income Web users who must give up some privacy for these services?

2.41 A health-information Web site has many articles on health and medical issues, a chat room where people can discuss health issues with other users, and provisions for people to send questions by e-mail to be answered by doctors. You have been hired to do a privacy audit. In other words, you are to examine the site, find privacy risks (or good privacy protection practices), and make recommendations for changes as needed. Describe at least three things you would look for, explain their significance, and tell what your recommendations would be if you do or don't find them.

2.42 Your town is considering setting up a camera and face-recognition system in the downtown area and in a neighborhood with a high crime rate. You are hired as a consultant to help design policies for the use of the system. Consider a variety of aspects, for example, who will have access to the system, what databases of photos will be used for matching, how long video will be stored, and other factors you consider important. Describe some of your most important recommendations to the city with your reasons for them.

2.43 A company planned to sell a laser device a person can wear around his or her neck that makes photographs taken of the person come out streaked and useless. It was marketed to celebrities who are hounded by photographers. Suppose the device works well against CCTV cameras and many people begin to use it routinely in public places. Law-enforcement agencies will almost certainly try to ban it. Give arguments for and against such a ban.

2.44 Consider the kinds of search and surveillance tools described in Section 2.2.3. Choose several of them and discuss whether they would ( singly or in combination) likely have prevented the terrorist attack on September 11, 2001. What other computer-related technology might prevent such attacks in the future?

NOTES

3. "Privacy as a Aspect of Human Dignity," in Ferdinand David Schopenhauer, ed., Philosophical Dimensions of Pri-
4. vacy: An Anthology, Cambridge University Press, 1984, pp. 156-203, quote on p. 188.
11. Steven Levy, "Is It Softwear or Spyware?" Newsweek, Nov. 29, 2001, p. 51, Associated Press, "People Soft-
14. cial Security Administration, the IRS, and the Secret Service.
19. um.
22. Rothkoff, Privacy for Sale, p. 142.
25. Letter from Vince Benda, director of Census Bu-
26. reau under President Nixon and Carter, and comments from Carl Clark, Justice Department coordinator of af-

Margo Anderson, The American Census: A Social His-
30. These observations were made in John Shamrock, "Computer Matching Is a Serious Threat to Individual-
32. Computer and Privacy: How the Government Ow-
35. son of Federal Agency Practice with FTC Fair Informat-
44. Meridith is United States 390 U.S. 39 (1968), quoted in Steven A. Berson, "Smart Card Privacy Issues: An Overview," BID-T091, July 1994, Smart Card For-
45. um.
46. Ron Kerber, "When Is a Satisfire Photo An Unassum-
also Volokh's article and the article by Solvig Singleton listed at the end of the chapter.


B O O K S  A N D  A R T I C L E S


- James Rachels, "Why Privacy is Important," in Philosophy and Public Affairs, 4-4, Princeton University Press, 1975. (Appears in several anthologies including Schoeman, Philosophical Dimensions of Privacy, listed below, and Johnson and Nussbaum, Companions, Ethics and Social Values, listed at the end of Chapter 1.)


- Robert Ellis Smith, publisher, Privacy Journal. A monthly newsletter covering news on many aspects of privacy.


O R G A N I Z A T I O N S  A N D  W E B S I T E S

- Cato Institute, www.cato.org/tech
- Electronic Frontier Foundation, www.eff.org
- Electronic Frontiers Australia, wwwefa.org.au
- Electronic Privacy Information Center, www.epic.org. See also www.privacy.org, jointly sponsored by EPIC and Privacy International
- Junkbusters, www.junkbusters.com
- The Library of Congress site for U.S. laws and bills currently going through Congress: thomas.loc.gov
- PrivaCilla, www.privacilla.org. A site on privacy policy from a free-market, pro-technology perspective
- Privacy & American Business (Center for Social and Legal Research): www.pandub.org

- Privacy Commission of Australia: www.privacy.gov.au
- Privacy Commissioner of Canada: www.privcom.gc.ca
- Privacy Forum: www.ventrex.com/privacy
- Privacy Rights Clearinghouse: www.privacyrights.org
- TRUSTe: www.truste.org