Chapter 4

Ethical and Social Issues in Information Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to answer the following questions:

1. What ethical, social, and political issues are raised by information systems?
2. What specific principles for conduct can be used to guide ethical decisions?
3. Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?
4. How have information systems affected everyday life?

Interactive Sessions:

The Perils of Texting

Too Much Technology?

CHAPTER OUTLINE

BEHAVIORAL TARGETING AND YOUR PRIVACY: YOU'RE THE TARGET

Ever get the feeling somebody is trailing you on the Web, watching your every click? Wonder why you start seeing display ads and pop-ups just after you've been scouring the Web for a car, a dress, or cosmetic product? Well, you're right: your behavior is being tracked, and you are being targeted on the Web so that you are exposed to certain ads and not others. The Web sites you visit track the search engine queries you enter, pages visited, Web content viewed, ads clicked, videos watched, content shared, and the products you purchase. Google is the largest Web tracker, monitoring thousands of Web sites. As one wag noted, Google knows more about you than your mother does. In March 2009, Google began displaying ads on thousands of Google-related Web sites based on their previous online activities. To parry a growing public resentment of behavioral targeting, Google said it would give users the ability to see and edit the information that it has compiled about their interests for the purposes of behavioral targeting.

Behavioral targeting seeks to increase the efficiency of online ads by using information that Web visitors reveal about themselves online, and if possible, combine this with offline identity and consumption information gathered by companies such as Acxiom. One of the original promises of the Web was that it can deliver a marketing message tailored to each consumer based on this data, and then measure the results in terms of click-throughs and purchases. The technology used to implement online tracking is a combination of cookies, Flash cookies, and Web beacons (also called Web bugs). Web beacons are small programs placed on your computer when you visit any of thousands of Web sites. They report back to servers operated by the beacon owners the domains and Web pages you visited, what ads you clicked on, and other online behaviors. A recent study of 20 million Web pages published by 2 million domains found Google, Yahoo, Amazon, YouTube, Photobucket, and Flickr among the top 10 Web-bugging sites. Google alone accounts for 20% of all Web bugs. The average home landing page at the top 100 Web domains has over 50 tracking cookies and bugs. And you thought you were surfing alone?

Firms are experimenting with more precise targeting methods. Snapple used behavioral targeting methods (with the help of an online ad firm Tacoda) to identify the types of people attracted to Snapple Green Tea. Answer: people who like the arts and literature, travel internationally, and visit health sites. Microsoft offers MSN advertisers access to personal data derived from 270 million worldwide Windows Live users. The goal of Web beacons and bugs is even more granular: these tools can be used to identify your personal interests and behaviors so precisely targeted ads can be shown to you.

The growth in the power, reach, and scope of behavioral targeting has drawn the attention of privacy groups and the Federal Trade Commission (FTC). Currently, Web tracking is unregulated. In November 2007, the FTC opened hearings to consider proposals from privacy advocates to develop a "do not track list," to develop visual online cues to alert people to tracking, and to allow people to opt out. In the Senate, hearings on behavioral targeting were held throughout 2009 and the first half of 2010 with attention shifting to the privacy of personal location information. While Google, Microsoft, and Yahoo pleaded for legislation to protect them

from consumer lawsuits, the FTC refused to consider new legislation to protect the privacy of Internet users. Instead, the FTC proposed industry self-regulation. In 2009, a consortium of advertising firms (the Network Advertising Initiative) responded positively to FTC-proposed principles to regulate online behavioral advertising. In 2010, Congressional committees pressed leading Internet firms to allow users more opportunities to turn off tracking tools, and to make users aware on entry to a page that they are being tracked. In June 2010, the FTC announced it is examining Facebook Inc.'s efforts to protect user privacy.

All of these regulatory efforts emphasize transparency, user control over their information, security, and the temporal stability of privacy promises (unannounced and sudden changes in information privacy may not be allowed).

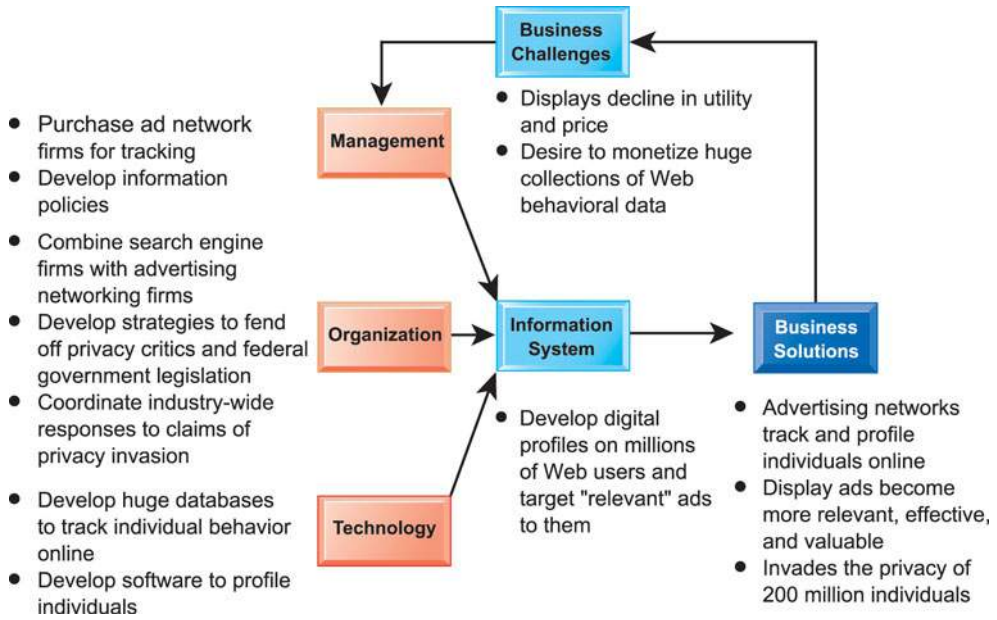
Perhaps the central ethical and moral question is understanding what rights individuals have in their own personally identifiable Internet profiles. Are these "ownership" rights, or merely an "interest" in an underlying asset? How much privacy are we willing to give up in order to receive more relevant ads? Surveys suggest that over 70 percent of Americans do not want to receive targeted ads.

Sources: "Web Bug Report," SecuritySpace, July, 2010; Miguel Helft, "Technology Coalition Seeks Stronger Privacy Laws," *New York Times*, March 30, 2010; "Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice as Effective As Non-targerted Online Ads," Network Advertising Initiative, March 24, 2010; Steve Lohr, "Redrawing the Route to Online Privacy," New York Times, February 28, 2010; "The Collection and Use of Location Information for Commercial Purposes Hearings," U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, February 24, 2010; Tom Krazit, "Groups Call for New Checks on Behavioral Ad Data," CNET News, September 1, 2009; Robert Mitchell, "What Google Knows About You," *Computerworld*, May 11, 2009; Stephanie Clifford, "Many See Privacy on Web as Big Issue, Survey Says," *The New York Times*, March 16, 2009; Miguel Helft, "Google to Offer Ads Based on Interests," *The New York Times*, March 11, 2009; and David Hallerman, "Behavioral Targeting: Marketing Trends," *eMarketer*, June 2008.

The growing use of behavioral targeting techniques described in the chapter-opening case shows that technology can be a double-edged sword. It can be the source of many benefits (by showing you ads relevant to your interests) but it can also create new opportunities for invading your privacy, and enabling the reckless use of that information in a variety of decisions about you.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. Online advertising titans like Google, Microsoft, and Yahoo are all looking for ways to monetize their huge collections of online behavioral data. While search engine marketing is arguably the most effective form of advertising in history, banner display ad marketing is highly inefficient because it displays ads to everyone regardless of their interests. Hence the search engine marketers cannot charge much for display ad space. However, by tracking the online movements of 200 million U.S. Internet users, they can develop a very clear picture of who you are, and use that information to show you ads that might be of interest to you. This would make the marketing process more efficient, and more profitable for all the parties involved.

But this solution also creates an ethical dilemma, pitting the monetary interests of the online advertisers and search engines against the interests of individuals to maintain a sense of control over their personal information and their privacy. Two closely held values are in conflict here. As a manager, you will need to be sensitive to both the negative and positive impacts of information systems for your firm, employees, and customers. You will need to learn how to resolve ethical dilemmas involving information systems.



4.1 Understanding Ethical and Social Issues Related to Systems

In the past 10 years, we have witnessed, arguably, one of the most ethically challenging periods for U.S. and global business. Table 4-1 provides a small sample of recent cases demonstrating failed ethical judgment by senior and middle managers. These lapses in management ethical and business judgment occurred across a broad spectrum of industries.

In today's new legal environment, managers who violate the law and are convicted will most likely spend time in prison. U.S. federal sentencing guidelines adopted in 1987 mandate that federal judges impose stiff sentences on business

TABLE 4-1 RECENT EXAMPLES OF FAILED ETHICAL JUDGMENT BY SENIOR MANAGERS

Lehman Brothers (2008–2010)	One of the oldest American investment banks collapses in 2008. Lehman used information systems and accounting sleight of hand to conceal its bad investments. Lehman also engaged in deceptive tactics to shift investments off its books.
WG Trading Co. (2010)	Paul Greenwood, hedge fund manager and general partner at WG Trading, pled guilty to defrauding investors of $554 million over 13 years; Greenwood has forfeited $331 million to the government and faces up to 85 years in prison.
Minerals Management Service (U.S. Department of the Interior) (2010)	Managers accused of accepting gifts and other favors from oil companies, letting oil company rig employees write up inspection reports, and failing to enforce existing regulations on offshore Gulf drilling rigs. Employees systematically falsified information record systems.
Pfizer, Eli Lilly, and AstraZeneca (2009)	Major pharmaceutical firms paid billions of dollars to settle U.S. federal charges that executives fixed clinical trials for antipsychotic and pain killer drugs, marketed them inappropriately to children, and claimed unsubstantiated benefits while covering up negative outcomes. Firms falsified information in reports and systems.
Galleon Group (2009)	Founder of the Galleon Group criminally charged with trading on insider information, paying $250 million to Wall Street banks, and in return received market information that other investors did not get.
Siemens (2009)	The world's largest engineering firm paid over $4 billion to German and U.S. authorities for a decades-long, world-wide bribery scheme approved by corporate executives to influence potential customers and governments. Payments concealed from normal reporting accounting systems.

executives based on the monetary value of the crime, the presence of a conspiracy to prevent discovery of the crime, the use of structured financial transactions to hide the crime, and failure to cooperate with prosecutors (U.S. Sentencing Commission, 2004).

Although in the past business firms would often pay for the legal defense of their employees enmeshed in civil charges and criminal investigations, now firms are encouraged to cooperate with prosecutors to reduce charges against the entire firm for obstructing investigations. These developments mean that, more than ever, as a manager or an employee, you will have to decide for yourself what constitutes proper legal and ethical conduct.

Although these major instances of failed ethical and legal judgment were not masterminded by information systems departments, information systems were instrumental in many of these frauds. In many cases, the perpetrators of these crimes artfully used financial reporting information systems to bury their decisions from public scrutiny in the vain hope they would never be caught. We deal with the issue of control in information systems in Chapter 8. In this chapter, we talk about the ethical dimensions of these and other actions based on the use of information systems.

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, the telephone, and the radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

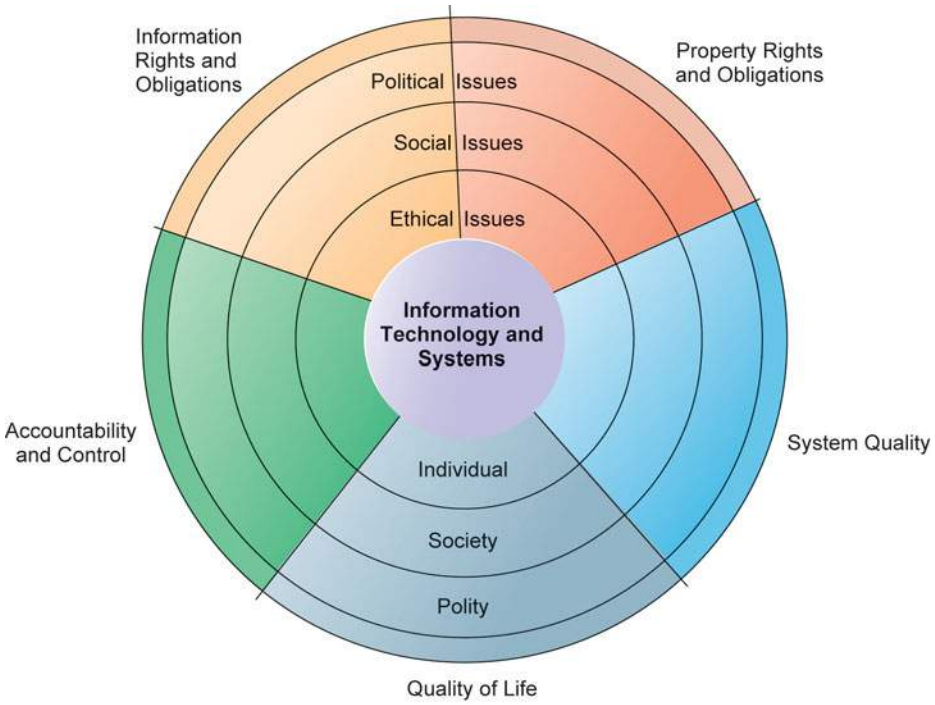
Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property.

Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, "What is the ethical and socially responsible course of action?"

A MODEL FOR THINKING ABOUT ETHICAL, SOCIAL, AND POLITICAL ISSUES

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure 4-1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. What happens? Ripples, of course.

FIGURE 4-1 **THE RELATIONSHIP BETWEEN ETHICAL, SOCIAL, AND POLITICAL ISSUES IN AN INFORMATION SOCIETY**



The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Imagine instead that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. Suddenly, individual actors are confronted with new situations often not covered by the old rules. Social institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, social responsibility, politically correct attitudes, or approved rules. Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime, you may have to act. You may be forced to act in a legal gray area.

We can use this model to illustrate the dynamics that connect ethical, social, and political issues. This model is also useful for identifying the main moral dimensions of the information society, which cut across various levels of action—individual, social, and political.

FIVE MORAL DIMENSIONS OF THE INFORMATION AGE

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

Information rights and obligations. What **information rights** do individuals and organizations possess with respect to themselves? What can they protect?

Property rights and obligations. How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?

Accountability and control. Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?

System quality. What standards of data and system quality should we demand to protect individual rights and the safety of society?

Quality of life. What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

We explore these moral dimensions in detail in Section 4.3.

KEY TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

Ethical issues long preceded information technology. Nevertheless, information technology has heightened ethical concerns, taxed existing social arrangements, and made some laws obsolete or severely crippled. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 4-2.

The doubling of computing power every 18 months has made it possible for most organizations to use information systems for their core production processes. As a result, our dependence on systems and our vulnerability to system errors and poor data quality have increased. Social rules and laws have not yet adjusted to this dependence. Standards for ensuring the accuracy and reliability of information systems (see Chapter 8) are not universally accepted or enforced.

Advances in data storage techniques and rapidly declining storage costs have been responsible for the multiplying databases on individuals—employees, customers, and potential customers—maintained by private and public organizations. These advances in data storage have made the routine violation of individual privacy both cheap and effective. Massive data storage systems are inexpensive enough for regional and even local retailing firms to use in identifying customers.

Advances in data analysis techniques for large pools of data are another technological trend that heightens ethical concerns because companies and government agencies are able to find out highly detailed personal information

TABLE 4-2 TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

TREND	IMPACT
Computing power doubles every 18 months	More organizations depend on computer systems for critical operations.
Data storage costs rapidly declining	Organizations can easily maintain detailed databases on individuals.
Data analysis advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individual behavior.
Networking advances	Copying data from one location to another and accessing personal data from remote locations are much easier.

Credit card purchases can make personal information available to market researchers, telemarketers, and direct-mail companies. Advances in information technology facilitate the invasion of privacy.

about individuals. With contemporary data management tools (see Chapter 5), companies can assemble and combine the myriad pieces of information about you stored on computers much more easily than in the past.

Think of all the ways you generate computer information about yourself—credit card purchases, telephone calls, magazine subscriptions, video rentals, mail-order purchases, banking records, local, state, and federal government records (including court and police records), and visits to Web sites. Put together and mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, and your political interests.

Companies with products to sell purchase relevant information from these sources to help them more finely target their marketing campaigns. Chapters 3 and 6 describe how companies can analyze large pools of data from multiple sources to rapidly identify buying patterns of customers and suggest individual responses. The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called **profiling**.

For example, several thousand of the most popular Web sites allow DoubleClick (owned by Google), an Internet advertising broker, to track the activities of their visitors in exchange for revenue from advertisements based on visitor information DoubleClick gathers. DoubleClick uses this information to create a profile of each online visitor, adding more detail to the profile as the visitor accesses an associated DoubleClick site. Over time, DoubleClick can create a detailed dossier of a person's spending and computing habits on the Web that is sold to companies to help them target their Web ads more precisely.

ChoicePoint gathers data from police, criminal, and motor vehicle records; credit and employment histories; current and previous addresses; professional licenses; and insurance claims to assemble and maintain electronic dossiers on almost every adult in the United States. The company sells this personal

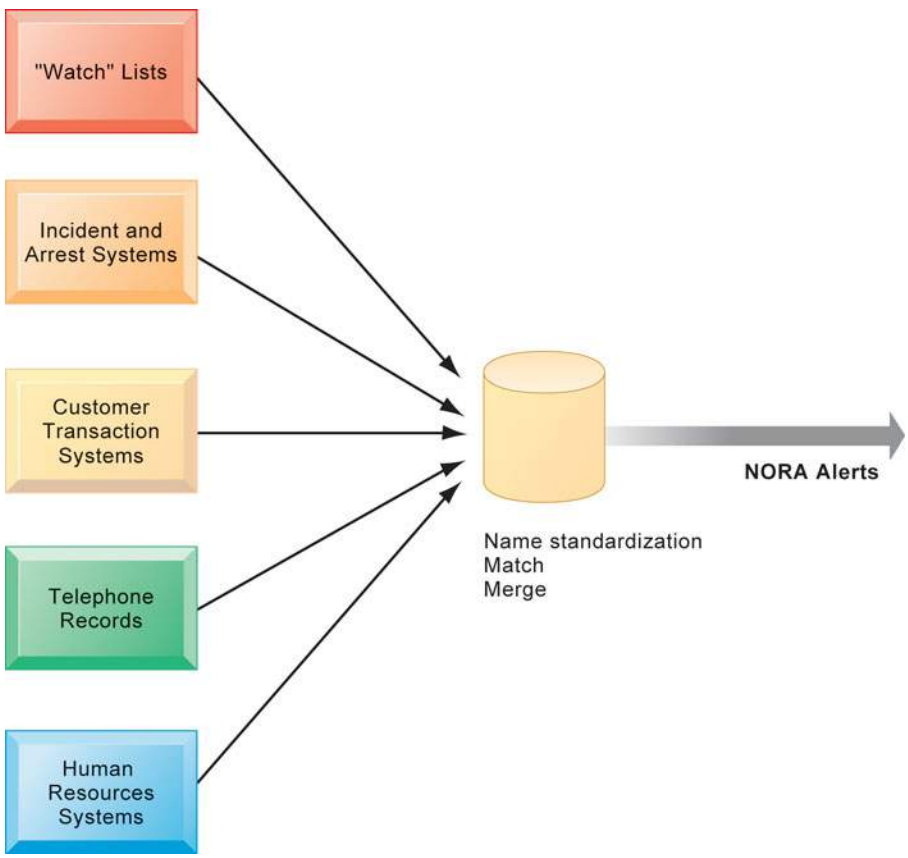
information to businesses and government agencies. Demand for personal data is so enormous that data broker businesses such as ChoicePoint are flourishing.

A new data analysis technology called **nonobvious relationship awareness (NORA)** has given both the government and the private sector even more powerful profiling capabilities. NORA can take information about people from many disparate sources, such as employment applications, telephone records, customer listings, and "wanted" lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists (see Figure 4-2).

NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool for homeland security but does have privacy implications because it can provide such a detailed picture of the activities and associations of a single individual.

Finally, advances in networking, including the Internet, promise to greatly reduce the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely using small desktop machines, permitting an invasion of privacy on a scale and with a precision heretofore unimaginable.

FIGURE 4-2 NONOBVIOUS RELATIONSHIP AWARENESS (NORA)



NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

4.2 Ethics in an Information Society

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. **Responsibility** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make. **Accountability** is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, and who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. **Liability** extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a related feature of law-governed societies and is a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them. First, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behaviors. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

ETHICAL ANALYSIS

When confronted with a situation that seems to present ethical issues, how should you analyze it? The following five-step process should help:

1. *Identify and describe clearly the facts.* Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.
2. *Define the conflict or dilemma and identify the higher-order values involved.* Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-ending case study illustrates two competing values: the need to improve health care record keeping and the need to protect individual privacy.

3. *Identify the stakeholders.* Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.
4. *Identify the options that you can reasonably take.* You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.
5. *Identify the potential consequences of your options.* Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

CANDIDATE ETHICAL PRINCIPLES

Once your analysis is complete, what ethical principles or rules should you use to make a decision? What higher-order values should inform your judgment? Although you are the only one who can decide which among many ethical principles you will follow, and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history:

1. Do unto others as you would have them do unto you (the **Golden Rule**). Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.
2. If an action is not right for everyone to take, it is not right for anyone **(Immanuel Kant's Categorical Imperative)**. Ask yourself, "If everyone did this, could the organization, or society, survive?"
3. If an action cannot be taken repeatedly, it is not right to take at all **(Descartes' rule of change)**. This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if it is repeated, it would bring unacceptable changes in the long run. In the vernacular, it might be stated as "once started down a slippery path, you may not be able to stop."
4. Take the action that achieves the higher or greater value **(Utilitarian Principle)**. This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
5. Take the action that produces the least harm or the least potential cost **(Risk Aversion Principle)**. Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid these high-failure-cost actions, paying greater attention to high-failure-cost potential of moderate to high probability.
6. Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the **ethical "no free lunch" rule.**) If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work.

Actions that do not easily pass these rules deserve close attention and a great deal of caution. The appearance of unethical behavior may do as much harm to you and your company as actual unethical behavior.

PROFESSIONAL CODES OF CONDUCT

When groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect. Professional codes of conduct are promulgated by associations of professionals, such as the American Medical Association (AMA), the American Bar Association (ABA), the Association of Information Technology Professionals (AITP), and the Association for Computing Machinery (ACM). These professional groups take responsibility for the partial regulation of their professions by determining entrance qualifications and competence. Codes of ethics are promises by professions to regulate themselves in the general interest of society. For example, avoiding harm to others, honoring property rights (including intellectual property), and respecting privacy are among the General Moral Imperatives of the ACM's Code of Ethics and Professional Conduct.

SOME REAL-WORLD ETHICAL DILEMMAS

Information systems have created new ethical dilemmas in which one set of interests is pitted against another. For example, many of the large telephone companies in the United States are using information technology to reduce the sizes of their workforces. Voice recognition software reduces the need for human operators by enabling computers to recognize a customer's responses to a series of computerized questions. Many companies monitor what their employees are doing on the Internet to prevent them from wasting company resources on non-business activities.

In each instance, you can find competing values at work, with groups lined up on either side of a debate. A company may argue, for example, that it has a right to use information systems to increase productivity and reduce the size of its workforce to lower costs and stay in business. Employees displaced by information systems may argue that employers have some responsibility for their welfare. Business owners might feel obligated to monitor employee e-mail and Internet use to minimize drains on productivity. Employees might believe they should be able to use the Internet for short personal tasks in place of the telephone. A close analysis of the facts can sometimes produce compromised solutions that give each side "half a loaf." Try to apply some of the principles of ethical analysis described to each of these cases. What is the right thing to do?

4.3 The Moral Dimensions of Information Systems

In this section, we take a closer look at the five moral dimensions of information systems first described in Figure 4-1. In each dimension, we identify the ethical, social, and political levels of analysis and use real-world examples to illustrate the values involved, the stakeholders, and the options chosen.

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN THE INTERNET AGE

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are

subject to electronic and other forms of high-tech surveillance (Ball, 2001). Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

The claim to privacy is protected in the U.S., Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. In the United States, the claim to privacy is protected primarily by the First Amendment guarantees of freedom of speech and association, the Fourth Amendment protections against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process.

Table 4-3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information. At present, most U.S. federal privacy laws apply only to the federal government and regulate very few areas of the private sector.

Most American and European privacy law is based on a regime called **Fair Information Practices (FIP)** first set forth in a report written in 1973 by a federal government advisory committee (U.S. Department of Health, Education, and Welfare, 1973). FIP is a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual. The individual has an interest in engaging in a transaction, and the record keeper—usually a business or government agency-requires information about the individual to support the transaction. Once information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, the FTC restated and extended the original FIP to provide guidelines for protecting online privacy. Table 4-4 describes the FTC's Fair Information Practice principles.

The FTC's FIP principles are being used as guidelines to drive changes in privacy legislation. In July 1998, the U.S. Congress passed the Children's Online Privacy Protection Act (COPPA), requiring Web sites to obtain parental permission before collecting information on children under the age of 13. (This law is

TABLE 4-3 FEDERAL PRIVACY LAWS IN THE UNITED STATES

GENERAL FEDERAL PRIVACY LAWS	PRIVACY LAWS AFFECTING PRIVATE INSTITUTIONS
Freedom of Information Act of 1966 as Amended (5 USC 552)	Fair Credit Reporting Act of 1970
Privacy Act of 1974 as Amended (5 USC 552a)	Family Educational Rights and Privacy Act of 1974
Electronic Communications Privacy Act of 1986	Right to Financial Privacy Act of 1978
Computer Matching and Privacy Protection Act of 1988	Privacy Protection Act of 1980
Computer Security Act of 1987	Cable Communications Policy Act of 1984
Federal Managers Financial Integrity Act of 1982	Electronic Communications Privacy Act of 1986
Driver's Privacy Protection Act of 1994	Video Privacy Protection Act of 1988
E-Government Act of 2002	The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	Children's Online Privacy Protection Act (COPPA) of 1998
	Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999

TABLE 4-4 FEDERAL TRADE COMMISSION FAIR INFORMATION PRACTICE PRINCIPLES

1.	Notice/awareness (core principle). Web sites must disclose their information practices before collecting data. Includes identification of collector; uses of data; other recipients of data; nature of collection (active/inactive); voluntary or required status; consequences of refusal; and steps taken to protect confidentiality, integrity, and quality of the data.
2.	Choice/consent (core principle). There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
3.	Access/participation. Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
4.	Security. Data collectors must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
5.	Enforcement. There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulations.

in danger of being overturned.) The FTC has recommended additional legislation to protect online consumer privacy in advertising networks that collect records of consumer Web activity to develop detailed profiles, which are then used by other companies to target online ads. Other proposed Internet privacy legislation focuses on protecting the online use of personal identification numbers, such as social security numbers; protecting personal information collected on the Internet that deals with individuals not covered by COPPA; and limiting the use of data mining for homeland security.

In February 2009, the FTC began the process of extending its fair information practices doctrine to behavioral targeting. The FTC held hearings to discuss its program for voluntary industry principles for regulating behavioral targeting. The online advertising trade group Network Advertising Initiative (discussed later in this section), published its own self-regulatory principles that largely agreed with the FTC. Nevertheless, the government, privacy groups, and the online ad industry are still at loggerheads over two issues. Privacy advocates want both an opt-in policy at all sites and a national Do Not Track list. The industry opposes these moves and continues to insist on an opt-out capability being the only way to avoid tracking (Federal Trade Commission, 2009). Nevertheless, there is an emerging consensus among all parties that greater transparency and user control (especially making opt-out of tracking the default option) is required to deal with behavioral tracking.

Privacy protections have also been added to recent laws deregulating financial services and safeguarding the maintenance and transmission of health information about individuals. The Gramm-Leach-Bliley Act of 1999, which repeals earlier restrictions on affiliations among banks, securities firms, and insurance companies, includes some privacy protection for consumers of financial services. All financial institutions are required to disclose their policies and practices for protecting the privacy of nonpublic personal information and to allow customers to opt out of information-sharing arrangements with nonaffiliated third parties.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, which took effect on April 14, 2003, includes privacy protection for medical records. The law gives patients access to their personal medical records maintained by health care providers, hospitals, and health insurers, and the right to authorize how protected information about themselves can be used or disclosed. Doctors, hospitals, and other health care providers must limit the disclosure of personal information about patients to the minimum amount necessary to achieve a given purpose.

The European Directive on Data Protection

In Europe, privacy protection is much more stringent than in the United States. Unlike the United States, European countries do not allow businesses to use personally identifiable information without consumers' prior consent. On October 25, 1998, the European Commission's Directive on Data Protection went into effect, broadening privacy protection in the European Union (EU) nations. The directive requires companies to inform people when they collect information about them and disclose how it will be stored and used. Customers must provide their informed consent before any company can legally use data about them, and they have the right to access that information, correct it, and request that no further data be collected. **Informed consent** can be defined as consent given with knowledge of all the facts needed to make a rational decision. EU member nations must translate these principles into their own laws and cannot transfer personal data to countries, such as the United States, that do not have similar privacy protection regulations.

Working with the European Commission, the U.S. Department of Commerce developed a safe harbor framework for U.S. firms. A **safe harbor** is a private, self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement. U.S. businesses would be allowed to use personal data from EU countries if they develop privacy protection policies that meet EU standards. Enforcement would occur in the United States using self-policing, regulation, and government enforcement of fair trade statutes.

Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

It is possible to record many online activities, including what searches have been conducted, which Web sites and Web pages have been visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. Much of this monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. It is conducted not just by individual Web sites but by advertising networks such as Microsoft Advertising, Yahoo, and DoubleClick that are capable of tracking all browsing behavior at thousands of Web sites. Tools to monitor visits to the World Wide Web have become popular because they help businesses determine who is visiting their Web sites and how to better target their offerings. (Some firms also monitor the Internet usage of their employees to see how they are using company network resources.) The commercial demand for this personal information is virtually insatiable.

Web sites can learn the identities of their visitors if the visitors voluntarily register at the site to purchase a product or service or to obtain a free service, such as information. Web sites can also capture information about visitors without their knowledge using cookie technology.

Cookies are small text files deposited on a computer hard drive when a user visits Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize

its contents for each visitor's interests. For example, if you purchase a book on Amazon.com and return later from the same browser, the site will welcome you by name and recommend other books of interest based on your past purchases. DoubleClick, described earlier in this chapter, uses cookies to build its dossiers with details of online purchases and to examine the behavior of Web site visitors. Figure 4-3 illustrates how cookies work.

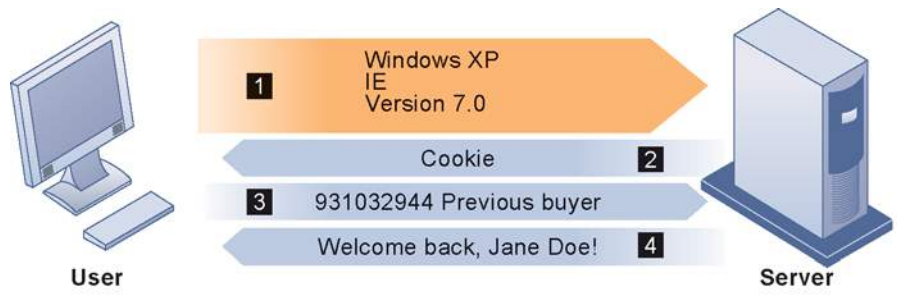
Web sites using cookie technology cannot directly obtain visitors' names and addresses. However, if a person has registered at a site, that information can be combined with cookie data to identify the visitor. Web site owners can also combine the data they have gathered from cookies and other Web site monitoring tools with personal data from other sources, such as offline data collected from surveys or paper catalog purchases, to develop very detailed profiles of their visitors.

There are now even more subtle and surreptitious tools for surveillance of Internet users. Marketers use Web beacons as another tool to monitor online behavior. **Web beacons**, also called *Web bugs,* are tiny objects invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail. The Web beacon captures and transmits information such as the IP address of the user's computer, the time a Web page was viewed and for how long, the type of Web browser that retrieved the beacon, and previously set cookie values. Web beacons are placed on popular Web sites by "third party" firms who pay the Web sites a fee for access to their audience. Typical popular Web sites contain 25–35 Web beacons.

Other **spyware** can secretly install itself on an Internet user's computer by piggybacking on larger applications. Once installed, the spyware calls out to Web sites to send banner ads and other unsolicited material to the user, and it can also report the user's movements on the Internet to other computers. More information is available about intrusive software in Chapter 8.

About 75 percent of global Internet users use Google search and other services, making Google the world's largest collector of online user data. Whatever Google does with its data has an enormous impact on online privacy. Most experts

FIGURE 4-3 HOW COOKIES IDENTIFY WEB VISITORS



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

believe that Google possesses the largest collection of personal information in the world—more data on more people than any government agency. Table 4-5 lists the major Google services that collect user data and how Google uses these data.

For a number of years, Google has been using behavioral targeting to help it display more relevant ads based on users' search activities. One of its programs enables advertisers to target ads based on the search histories of Google users, along with any other information the user submits to Google that Google can obtain, such as age, demographics, region, and other Web activities (such as blogging). An additional program allows Google to help advertisers select keywords and design ads for various market segments based on search histories, such as helping a clothing Web site create and test ads targeted at teenage females.

Google has also been scanning the contents of messages received by users of its free Web-based e-mail service called Gmail. Ads that users see when they read their e-mail are related to the subjects of these messages. Profiles are developed on individual users based on the content in their e-mail. Google now displays targeted ads on YouTube and on Google mobile applications, and its DoubleClick ad network serves up targeted banner ads.

In the past, Google refrained from capitalizing too much on the data it collected, considered the best source of data about user interests on the Internet. But with the emergence of rivals such as Facebook who are aggressively tracking and selling online user data, Google has decided to do more to profit from its user data.

The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other marketing purposes without obtaining the informed consent of the individual whose information is being used. U.S. e-commerce sites are largely content to publish statements on their Web sites informing visitors about how their information will be used. Some have added opt-out selection boxes to these information policy statements. An **opt-out** model of informed consent permits the collection of personal information until the consumer specifically requests that the

TABLE 4-5 HOW GOOGLE USES THE DATA IT COLLECTS

GOOGLE FEATURE	DATA COLLECTED	USE
Google Search	Google search topics Users' Internet addresses	Targeting text ads placed in search results
Gmail	Contents of e-mail messages	Targeting text ads placed next to the e-mail messages
DoubleClick	Data about Web sites visited on Google's ad network	Targeting banner ads
YouTube	Data about videos uploaded and downloaded; some profile data	Targeting ads for Google display-ad network
Mobile Maps with My Location	User's actual or approximate location	Targeting mobile ads based on user's ZIP code
Google Toolbar	Web-browsing data and search history	No ad use at present
Google Buzz	Users' Google profile data and connections	No ad use at present
Google Chrome	Sample of address-bar entries when Google is the default search engine	No ad use at present
Google Checkout	User's name, address, transaction details	No ad use at present
Google Analytics	Traffic data from Web sites using Google's Analytics service	No ad use at present

data not be collected. Privacy advocates would like to see wider use of an **opt-in** model of informed consent in which a business is prohibited from collecting any personal information unless the consumer specifically takes action to approve information collection and use.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. In 1998, the online industry formed the Online Privacy Alliance to encourage self-regulation to develop a set of privacy guidelines for its members. The group promotes the use of online seals, such as that of TRUSTe, certifying Web sites adhering to certain privacy principles. Members of the advertising network industry, including Google's DoubleClick, have created an additional industry association called the Network Advertising Initiative (NAI) to develop its own privacy policies to help consumers opt out of advertising network programs and provide consumers redress from abuses.

Individual firms like AOL, Yahoo!, and Google have recently adopted policies on their own in an effort to address public concern about tracking people online. AOL established an opt-out policy that allows users of its site to not be tracked. Yahoo follows NAI guidelines and also allows opt-out for tracking and Web beacons (Web bugs). Google has reduced retention time for tracking data.

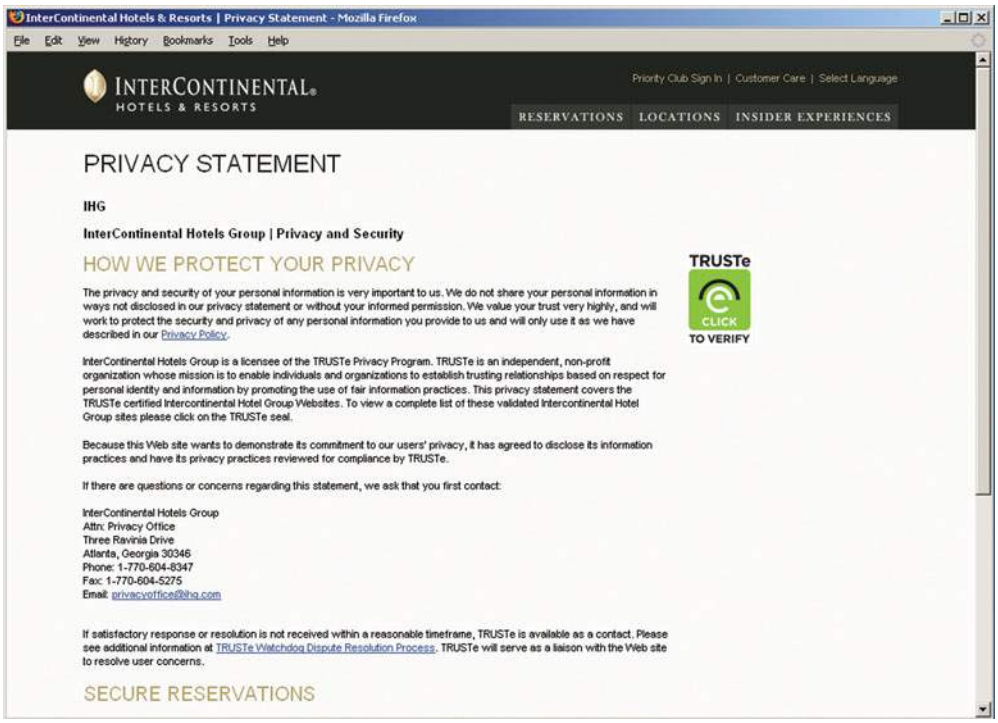
In general, most Internet businesses do little to protect the privacy of their customers, and consumers do not do as much as they should to protect themselves. Many companies with Web sites do not have privacy policies. Of the companies that do post privacy polices on their Web sites, about half do not monitor their sites to ensure they adhere to these policies. The vast majority of online customers claim they are concerned about online privacy, but less than half read the privacy statements on Web sites (Laudon and Traver, 2010).

In one of the more insightful studies of consumer attitudes towards Internet privacy, a group of Berkeley students conducted surveys of online users, and of complaints filed with the Federal Trade Commission involving privacy issues. Here are some of their results. User concerns: people feel they have no control over the information collected about them, and they don't know who to complain to. Web site practices: Web sites collect all this information, but do not let users have access; the policies are unclear; they share data with "affiliates" but never identify who the affiliates are and how many there are. (MySpace, owned by NewsCorp, has over 1,500 affiliates with whom it shares online information.) Web bug trackers: they are ubiquitous and we are not informed they are on the pages we visit. The results of this study and others suggest that consumers are not saying "Take my privacy, I don't care, send me the service for free." They are saying "We want access to the information, we want some controls on what can be collected, what is done with the information, the ability to opt out of the entire tracking enterprise, and some clarity on what the policies really are, and we don't want those policies changed without our participation and permission." (The full report is available at knowprivacy.org.)

Technical Solutions

In addition to legislation, new technologies are available to protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware.

There are now tools to help users determine the kind of personal data that can be extracted by Web sites. The Platform for Privacy Preferences, known as P3P, enables automatic communication of privacy policies between an e-commerce site and its visitors. **P3P** provides a standard for communicating a Web site's



Web sites are posting their privacy policies for visitors to review. The TRUSTe seal designates Web sites that have agreed to adhere to TRUSTe's established privacy principles of disclosure, choice, access, and security.

privacy policy to Internet users and for comparing that policy to the user's preferences or to other standards, such as the FTC's FIP guidelines or the European Directive on Data Protection. Users can use P3P to select the level of privacy they wish to maintain when interacting with the Web site.

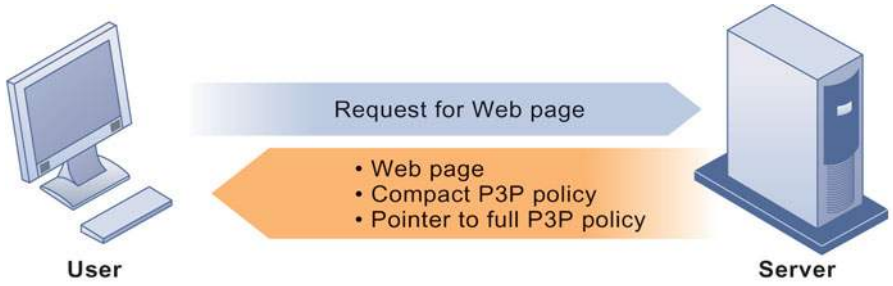
The P3P standard allows Web sites to publish privacy policies in a form that computers can understand. Once it is codified according to P3P rules, the privacy policy becomes part of the software for individual Web pages (see Figure 4-4). Users of Microsoft Internet Explorer Web browsing software can access and read the P3P site's privacy policy and a list of all cookies coming from the site. Internet Explorer enables users to adjust their computers to screen out all cookies or let in selected cookies based on specific levels of privacy. For example, the "Medium" level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy.

However, P3P only works with Web sites of members of the World Wide Web Consortium who have translated their Web site privacy policies into P3P format. The technology will display cookies from Web sites that are not part of the consortium, but users will not be able to obtain sender information or privacy statements. Many users may also need to be educated about interpreting company privacy statements and P3P levels of privacy. Critics point out that only a small percentage of the most popular Web sites use P3P, most users do not understand their browser's privacy settings, and there is no enforcement of P3P standards—companies can claim anything about their privacy policies.

PROPERTY RIGHTS: INTELLECTUAL PROPERTY

Contemporary information systems have severely challenged existing laws and social practices that protect private intellectual property. **Intellectual property** is considered to be intangible property created by individuals or

FIGURE 4-4 THE P3P STANDARD



1. The user with P3P Web browsing software requests a Web page.
2. The Web server returns the Web page along with a compact version of the Web site's policy and a pointer to the full P3P policy. If the Web site is not P3P compliant, no P3P data are returned.
3. The user's Web browsing software compares the response from the Web site with the user's privacy preferences. If the Web site does not have a P3P policy or the policy does not match the privacy levels established by the user, it warns the user or rejects the cookies from the Web site. Otherwise, the Web page loads normally.

P3P enables Web sites to translate their privacy policies into a standard format that can be read by the user's Web browser software. The browser software evaluates the Web site's privacy policy to determine whether it is compatible with the user's privacy preferences.

corporations. Information technology has made it difficult to protect intellectual property because computerized information can be so easily copied or distributed on networks. Intellectual property is subject to a variety of protections under three different legal traditions: trade secrets, copyright, and patent law.

Trade Secrets

Any intellectual work product—a formula, device, pattern, or compilation of data—used for a business purpose can be classified as a **trade secret**, provided it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly.

Software that contains novel or unique elements, procedures, or compilations can be included as a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make this claim, the creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

The limitation of trade secret protection is that, although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software is widely distributed.

Copyright

Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death. For corporate-owned works, copyright protection lasts for 95 years after their initial creation. Congress has extended copyright protection to books, periodicals, lectures, dramas, musical compositions, maps, drawings, artwork of any kind, and

motion pictures. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

In the mid-1960s, the Copyright Office began registering software programs, and in 1980, Congress passed the Computer Software Copyright Act, which clearly provides protection for software program code and for copies of the original sold in commerce, and sets forth the rights of the purchaser to use the software while the creator retains legal title.

Copyright protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that the underlying ideas behind a work are not protected, only their manifestation in a work. A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright.

"Look and feel" copyright infringement lawsuits are precisely about the distinction between an idea and its expression. For instance, in the early 1990s, Apple Computer sued Microsoft Corporation and Hewlett-Packard for infringement of the expression of Apple's Macintosh interface, claiming that the defendants copied the expression of overlapping windows. The defendants countered that the idea of overlapping windows can be expressed only in a single way and, therefore, was not protectable under the merger doctrine of copyright law. When ideas and their expression merge, the expression cannot be copyrighted.

In general, courts appear to be following the reasoning of a 1989 case—*Brown Bag Software vs. Symantec Corp.*—in which the court dissected the elements of software alleged to be infringing. The court found that similar concept, function, general functional features (e.g., drop-down menus), and colors are not protectable by copyright law (*Brown Bag Software vs. Symantec Corp.*, 1992).

Patents

A **patent** grants the owner an exclusive monopoly on the ideas behind an invention for 20 years. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or methods receive the full financial and other rewards of their labor and yet make widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under license from the patent's owner. The granting of a patent is determined by the United States Patent and Trademark Office and relies on court rulings.

The key concepts in patent law are originality, novelty, and invention. The Patent Office did not accept applications for software patents routinely until a 1981 Supreme Court decision that held that computer programs could be a part of a patentable process. Since that time, hundreds of patents have been granted and thousands await consideration.

The strength of patent protection is that it grants a monopoly on the underlying concepts and ideas of software. The difficulty is passing stringent criteria of nonobviousness (e.g., the work must reflect some special understanding and contribution), originality, and novelty, as well as years of waiting to receive protection.

Challenges to Intellectual Property Rights

Contemporary information technologies, especially software, pose severe challenges to existing intellectual property regimes and, therefore, create

significant ethical, social, and political issues. Digital media differ from books, periodicals, and other media in terms of ease of replication; ease of transmission; ease of alteration; difficulty in classifying a software work as a program, book, or even music; compactness—making theft easy; and difficulties in establishing uniqueness.

The proliferation of electronic networks, including the Internet, has made it even more difficult to protect intellectual property. Before widespread use of networks, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed. The Seventh Annual Global Software Piracy Study conducted by the International Data Corporation and the Business Software Alliance reported that the rate of global software piracy climbed to 43 percent in 2009, representing $51 billion in global losses from software piracy. Worldwide, for every $100 worth of legitimate software sold that year, an additional $75 worth was obtained illegally (Business Software Alliance, 2010).

The Internet was designed to transmit information freely around the world, including copyrighted information. With the World Wide Web in particular, you can easily copy and distribute virtually anything to thousands and even millions of people around the world, even if they are using different types of computer systems. Information can be illicitly copied from one place and distributed through other systems and networks even though these parties do not willingly participate in the infringement.

Individuals have been illegally copying and distributing digitized MP3 music files on the Internet for a number of years. File-sharing services such as Napster, and later Grokster, Kazaa, and Morpheus, sprung up to help users locate and swap digital music files, including those protected by copyright. Illegal file sharing became so widespread that it threatened the viability of the music recording industry. The recording industry won some legal battles for shutting these services down, but has not been able to halt illegal file sharing entirely. As more and more homes adopt high-speed Internet access, illegal file sharing of videos will pose similar threats to the motion picture industry.

Mechanisms are being developed to sell and distribute books, articles, and other intellectual property legally on the Internet, and the **Digital Millennium Copyright Act (DMCA)** of 1998 is providing some copyright protection. The DMCA implemented a World Intellectual Property Organization Treaty that makes it illegal to circumvent technology-based protections of copyrighted materials. Internet service providers (ISPs) are required to take down sites of copyright infringers that they are hosting once they are notified of the problem.

Microsoft and other major software and information content firms are represented by the Software and Information Industry Association (SIIA), which lobbies for new laws and enforcement of existing laws to protect intellectual property around the world. The SIIA runs an antipiracy hotline for individuals to report piracy activities, offers educational programs to help organizations combat software piracy, and has published guidelines for employee use of software.

ACCOUNTABILITY, LIABILITY, AND CONTROL

Along with privacy and property laws, new information technologies are challenging existing liability laws and social practices for holding individuals and institutions accountable. If a person is injured by a machine controlled, in part, by software, who should be held accountable and, therefore, held liable? Should a public bulletin board or an electronic service, such as America Online,

permit the transmission of pornographic or offensive material (as broadcasters), or should they be held harmless against any liability for what users transmit (as is true of common carriers, such as the telephone system)? What about the Internet? If you outsource your information processing, can you hold the external vendor liable for injuries done to your customers? Some real-world examples may shed light on these questions.

Computer-Related Liability Problems

During the last week of September 2009, thousands of customers of TD Bank, one of the largest banks in North America, scrambled to find their payroll checks, social security checks, and savings and checking account balances. The bank's 6.5 million customers were temporarily out of funds because of a computer glitch. The problems were caused by a failed effort to integrate systems of TD Bank and Commerce Bank. A spokesperson for TD Bank, said that "while the overall integration of the systems went well, there have been some speed-bumps in the final stages, as you might expect with a project of this size and complexity." (Vijayan, 2009). Who is liable for any economic harm caused to individuals or businesses that could not access their full account balances in this period?

This case reveals the difficulties faced by information systems executives who ultimately are responsible for any harm done by systems developed by their staffs. In general, insofar as computer software is part of a machine, and the machine injures someone physically or economically, the producer of the software and the operator can be held liable for damages. Insofar as the software acts like a book, storing and displaying information, courts have been reluctant to hold authors, publishers, and booksellers liable for contents (the exception being instances of fraud or defamation), and hence courts have been wary of holding software authors liable for booklike software.

In general, it is very difficult (if not impossible) to hold software producers liable for their software products that are considered to be like books, regardless of the physical or economic harm that results. Historically, print publishers, books, and periodicals have not been held liable because of fears that liability claims would interfere with First Amendment rights guaranteeing freedom of expression.

What about software as a service? ATM machines are a service provided to bank customers. Should this service fail, customers will be inconvenienced and perhaps harmed economically if they cannot access their funds in a timely manner. Should liability protections be extended to software publishers and operators of defective financial, accounting, simulation, or marketing systems?

Software is very different from books. Software users may develop expectations of infallibility about software; software is less easily inspected than a book, and it is more difficult to compare with other software products for quality; software claims actually to perform a task rather than describe a task, as a book does; and people come to depend on services essentially based on software. Given the centrality of software to everyday life, the chances are excellent that liability law will extend its reach to include software even when the software merely provides an information service.

Telephone systems have not been held liable for the messages transmitted because they are regulated common carriers. In return for their right to provide telephone service, they must provide access to all, at reasonable rates, and achieve acceptable reliability. But broadcasters and cable television stations are subject to a wide variety of federal and local constraints on content and facilities. Organizations can be held liable for offensive content on their Web sites, and online services, such as America Online, might be held liable for postings by their

users. Although U.S. courts have increasingly exonerated Web sites and ISPs for posting material by third parties, the threat of legal action still has a chilling effect on small companies or individuals who cannot afford to take their cases to trial.

SYSTEM QUALITY: DATA QUALITY AND SYSTEM ERRORS

The debate over liability and accountability for unintentional consequences of system use raises a related but independent moral dimension: What is an acceptable, technologically feasible level of system quality? At what point should system managers say, "Stop testing, we've done all we can to perfect this software. Ship it!" Individuals and organizations may be held responsible for avoidable and foreseeable consequences, which they have a duty to perceive and correct. And the gray area is that some system errors are foreseeable and correctable only at very great expense, an expense so great that pursuing this level of perfection is not feasible economically—no one could afford the product.

For example, although software companies try to debug their products before releasing them to the marketplace, they knowingly ship buggy products because the time and cost of fixing all minor errors would prevent these products from ever being released. What if the product was not offered on the marketplace, would social welfare as a whole not advance and perhaps even decline? Carrying this further, just what is the responsibility of a producer of computer services—should it withdraw the product that can never be perfect, warn the user, or forget about the risk (let the buyer beware)?

Three principal sources of poor system performance are (1) software bugs and errors, (2) hardware or facility failures caused by natural or other causes, and (3) poor input data quality. A Chapter 8 Learning Track discusses why zero defects in software code of any complexity cannot be achieved and why the seriousness of remaining bugs cannot be estimated. Hence, there is a technological barrier to perfect software, and users must be aware of the potential for catastrophic failure. The software industry has not yet arrived at testing standards for producing software of acceptable but not perfect performance.

Although software bugs and facility catastrophes are likely to be widely reported in the press, by far the most common source of business system failure is data quality. Few companies routinely measure the quality of their data, but individual organizations report data error rates ranging from 0.5 to 30 percent.

QUALITY OF LIFE: EQUITY, ACCESS, AND BOUNDARIES

The negative social costs of introducing information technologies and systems are beginning to mount along with the power of the technology. Many of these negative social consequences are not violations of individual rights or property crimes. Nevertheless, these negative consequences can be extremely harmful to individuals, societies, and political institutions. Computers and information technologies potentially can destroy valuable elements of our culture and society even while they bring us benefits. If there is a balance of good and bad consequences of using information systems, who do we hold responsible for the bad consequences? Next, we briefly examine some of the negative social consequences of systems, considering individual, social, and political responses.

Balancing Power: Center Versus Periphery

An early fear of the computer age was that huge, centralized mainframe computers would centralize power at corporate headquarters and in the nation's capital, resulting in a Big Brother society, as was suggested in George Orwell's novel *1984*. The shift toward highly decentralized computing, coupled with an ideology of empowerment of thousands of workers, and the decentralization of decision making to lower organizational levels, have reduced the fears of power centralization in institutions. Yet much of the empowerment described in popular business magazines is trivial. Lower-level employees may be empowered to make minor decisions, but the key policy decisions may be as centralized as in the past.

Rapidity of Change: Reduced Response Time to Competition

Information systems have helped to create much more efficient national and international markets. The now-more-efficient global marketplace has reduced the normal social buffers that permitted businesses many years to adjust to competition. Time-based competition has an ugly side: The business you work for may not have enough time to respond to global competitors and may be wiped out in a year, along with your job. We stand the risk of developing a "just-in-time society" with "just-in-time jobs" and "just-in-time" workplaces, families, and vacations.

Maintaining Boundaries: Family, Work, and Leisure

Parts of this book were produced on trains and planes, as well as on vacations and during what otherwise might have been "family" time. The danger to ubiquitous computing, telecommuting, nomad computing, and the "do anything anywhere" computing environment is that it is actually coming true. The traditional boundaries that separate work from family and just plain leisure have been weakened.

Although authors have traditionally worked just about anywhere (typewriters have been portable for nearly a century), the advent of information

Although some people enjoy the convenience of working at home, the "do anything anywhere" computing environment can blur the traditional boundaries between work and family time.

systems, coupled with the growth of knowledge-work occupations, means that more and more people are working when traditionally they would have been playing or communicating with family and friends. The work umbrella now extends far beyond the eight-hour day.

Even leisure time spent on the computer threatens these close social relationships. Extensive Internet use, even for entertainment or recreational purposes, takes people away from their family and friends. Among middle school and teenage children, it can lead to harmful anti-social behavior, such as the recent upsurge in cyberbullying.

Weakening these institutions poses clear-cut risks. Family and friends historically have provided powerful support mechanisms for individuals, and they act as balance points in a society by preserving private life, providing a place for people to collect their thoughts, allowing people to think in ways contrary to their employer, and dream.

Dependence and Vulnerability

Today, our businesses, governments, schools, and private associations, such as churches, are incredibly dependent on information systems and are, therefore, highly vulnerable if these systems fail. With systems now as ubiquitous as the telephone system, it is startling to remember that there are no regulatory or standard-setting forces in place that are similar to telephone, electrical, radio, television, or other public utility technologies. The absence of standards and the criticality of some system applications will probably call forth demands for national standards and perhaps regulatory oversight.

Computer Crime and Abuse

New technologies, including computers, create new opportunities for committing crime by creating new valuable items to steal, new ways to steal them, and new ways to harm others. **Computer crime** is the commission of illegal acts through the use of a computer or against a computer system. Computers or computer systems can be the object of the crime (destroying a company's computer center or a company's computer files), as well as the instrument of a crime (stealing computer lists by illegally gaining access to a computer system using a home computer). Simply accessing a computer system without authorization or with intent to do harm, even by accident, is now a federal crime.

Computer abuse is the commission of acts involving a computer that may not be illegal but that are considered unethical. The popularity of the Internet and e-mail has turned one form of computer abuse—spamming—into a serious problem for both individuals and businesses. **Spam** is junk e-mail sent by an organization or individual to a mass audience of Internet users who have expressed no interest in the product or service being marketed. Spammers tend to market pornography, fraudulent deals and services, outright scams, and other products not widely approved in most civilized societies. Some countries have passed laws to outlaw spamming or to restrict its use. In the United States, it is still legal if it does not involve fraud and the sender and subject of the e-mail are properly identified.

Spamming has mushroomed because it only costs a few cents to send thousands of messages advertising wares to Internet users. According to Sophos, a leading vendor of security software, spam accounted for 97 percent of all business e-mail during the second quarter of 2010 (Schwartz, 2010). Spam costs for businesses are very high (estimated at over $50 billion per year) because of the computing and network resources consumed by billions of unwanted e-mail messages and the time required to deal with them.

Internet service providers and individuals can combat spam by using spam filtering software to block suspicious e-mail before it enters a recipient's e-mail inbox. However, spam filters may block legitimate messages. Spammers know how to skirt around filters by continually changing their e-mail accounts, by incorporating spam messages in images, by embedding spam in e-mail attachments and electronic greeting cards, and by using other people's computers that have been hijacked by botnets (see Chapter 7). Many spam messages are sent from one country while another country hosts the spam Web site.

Spamming is more tightly regulated in Europe than in the United States. On May 30, 2002, the European Parliament passed a ban on unsolicited commercial messaging. Electronic marketing can be targeted only to people who have given prior consent.

The U.S. CAN-SPAM Act of 2003, which went into effect on January 1, 2004, does not outlaw spamming but does ban deceptive e-mail practices by requiring commercial e-mail messages to display accurate subject lines, identify the true senders, and offer recipients an easy way to remove their names from e-mail lists. It also prohibits the use of fake return addresses. A few people have been prosecuted under the law, but it has had a negligible impact on spamming. Although Facebook and MySpace have won judgments against spammers, most critics argue the law has too many loopholes and is not effectively enforced (Associated Press, 2009).

Another negative impact of computer technology is the rising danger from people using cell phones to send text messages while driving. Many states have outlawed this behavior, but it has been difficult to eradicate. The Interactive Session on Organizations explores this topic.

Employment: Trickle-Down Technology and Reengineering Job Loss

Reengineering work is typically hailed in the information systems community as a major benefit of new information technology. It is much less frequently noted that redesigning business processes could potentially cause millions of mid-level managers and clerical workers to lose their jobs. One economist has raised the possibility that we will create a society run by a small "high tech elite of corporate professionals . . . in a nation of the permanently unemployed" (Rifkin, 1993).

Other economists are much more sanguine about the potential job losses. They believe relieving bright, educated workers from reengineered jobs will result in these workers moving to better jobs in fast-growth industries. Missing from this equation are unskilled, blue-collar workers and older, less well-educated middle managers. It is not clear that these groups can be retrained easily for high-quality (high-paying) jobs. Careful planning and sensitivity to employee needs can help companies redesign work to minimize job losses.

Equity and Access: Increasing Racial and Social Class Cleavages

Does everyone have an equal opportunity to participate in the digital age? Will the social, economic, and cultural gaps that exist in the United States and other societies be reduced by information systems technology? Or will the cleavages be increased, permitting the better off to become even more better off relative to others?

These questions have not yet been fully answered because the impact of systems technology on various groups in society has not been thoroughly studied. What is known is that information, knowledge, computers, and access

INTERACTIVE SESSION: ORGANIZATIONS

THE PERILS OF TEXTING

Cell phones have become a staple of modern society. Nearly everyone has them, and people carry and use them at all hours of the day. For the most part, this is a good thing: the benefits of staying connected at any time and at any location are considerable. But if you're like most Americans, you may regularly talk on the phone or even text while at the wheel of a car. This dangerous behavior has resulted in increasing numbers of accidents and fatalities caused by cell phone usage. The trend shows no sign of slowing down.

In 2003, a federal study of 10,000 drivers by the National Highway Traffic Safety Administration (NHTSA) set out to determine the effects of using cell phones behind the wheel. The results were conclusive: talking on the phone is equivalent to a 10-point reduction in IQ and a .08 blood alcohol level, which law enforcement considers intoxicated. Hands-free sets were ineffective in eliminating risk, the study found, because the conversation itself is what distracts drivers, not holding the phone. Cell phone use caused 955 fatalities and 240,000 accidents in 2002. Related studies indicated that drivers that talked on the phone while driving increased their crash risk fourfold, and drivers that texted while driving increased their crash risk by a whopping 23 times.

Since that study, mobile device usage has grown by an order of magnitude, worsening this already dangerous situation. The number of wireless subscribers in America has increased by around 1,000 percent since 1995 to nearly 300 million overall in 2010, and Americans' usage of wireless minutes increased by approximately 6,000 percent. This increase in cell phone usage has been accompanied by an upsurge in phone-related fatalities and accidents: In 2010, it's estimated that texting caused 5,870 fatalities and 515,000 accidents, up considerably from prior years. These figures are roughly half of equivalent statistics for drunk driving. Studies show that drivers know that using the phone while driving is one of the most dangerous things you can do on the road, but refuse to admit that it's dangerous when they themselves do it.

Of users that text while driving, the more youthful demographic groups, such as the 18–29 age group, are by far the most frequent texters. About three quarters of Americans in this age group regularly text, compared to just 22 percent of the 35–44 age group. Correspondingly, the majority of accidents involving mobile device use behind the wheel involve young adults. Among this age group, texting behind the wheel is just one of a litany of problems raised by frequent texting: anxiety, distraction, failing grades, repetitive stress injuries, and sleep deprivation are just some of the other problems brought about by excessive use of mobile devices. Teenagers are particularly prone to using cell phones to text because they want to know what's happening to their friends and are anxious about being socially isolated.

Analysts predict that over 800 billion text messages will be sent in 2010. Texting is clearly here to stay, and in fact has supplanted phone calls as the most commonly used method of mobile communication. People are unwilling to give up their mobile devices because of the pressures of staying connected. Neurologists have found that the neural response to multitasking by texting while driving suggests that people develop addictions to the digital devices they use most, getting quick bursts of adrenaline, without which driving becomes boring.

There are interests opposed to legislation prohibiting cell phone use in cars. A number of legislators believe that it's not state or federal government's role to prohibit poor decision making. Auto makers, and some safety researchers, are arguing that with the proper technology and under appropriate conditions, communicating from a moving vehicle is a manageable risk. Louis Tijerina, a veteran of the NHTSA and Ford Motor Co. researcher, notes that even as mobile phone subscriptions have surged to over 250 million during the past decade, the death rate from accidents on the highways has fallen.

Nevertheless, lawmakers are increasingly recognizing the need for more powerful legislation barring drivers from texting behind the wheel. Many states have made inroads with laws prohibiting texting while operating vehicles. In Utah, drivers crashing while texting can receive 15 years in prison, by far the toughest sentence for texting while driving in the nation when the legislation was enacted. Utah's law assumes that drivers understand the risks of texting while driving, whereas in other states, prosecutors must prove that the driver knew about the risks of texting while driving before doing so.

Utah's tough law was the result of a horrifying accident in which a speeding college student, texting at the wheel, rear-ended a car in front. The car lost control, entered the opposite side of the road, and was hit head-on by a pickup truck hauling a trailer, killing the driver instantly. In September 2008, a train engineer in California was texting within a minute prior to the most fatal train accident in almost two decades. Californian authorities responded by banning the use of cell phones by train workers while on duty.

In total, 31 states have banned texting while driving in some form, and most of those states have a full ban for phone users of all ages. The remaining states are likely to follow suit in coming years as well. President Obama also banned texting while driving for all federal government employees in October 2009. Still, there's more work to be done to combat this dangerous and life-threatening practice.

Sources: Paulo Salazar, "Banning Texting While Driving," WCBI.com, August 7, 2010; Jerry Hirsch, "Teen Drivers Dangerously Divide Their Attention," *Los Angeles Times*, August 3, 2010; www.drivinglaws.org, accessed July 2010; www.drivinglaws.org, accessed July 7, 2010; Matt Richtel, "Driver Texting Now an Issue in the Back Seat," *The New York Times*, September 9, 2009; Matt Richtel, "Utah Gets Tough With Texting Drivers," *The New York Times*, August 29, 2009; Matt Richtel, "In Study, Texting Lifts Crash Risk by Large Margin," *The New York Times*, July 28, 2009; Matt Richtel, "Drivers and Legislators Dismiss Cellphone Risks," *The New York Times*, July 19, 2009; Tom Regan, "Some Sobering Stats on Texting While Driving," *The Christian Science Monitor*, May 28, 2009; Katie Hafner, "Texting May be Taking a Toll on Teenagers," *The New York Times*, May 26, 2009; and Tara Parker-Pope, "Texting Until Their Thumbs Hurt," The *New York Times*, May 26, 2009.

CASE STUDY QUESTIONS

1. Which of the five moral dimensions of information systems identified in this text is involved in this case?
2. What are the ethical, social, and political issues raised by this case?
3. Which of the ethical principles described in the text are useful for decision making about texting while driving?

MIS IN ACTION

1. Many people at state and local levels are calling for a federal law against texting while driving. Use a search engine to explore what steps the federal government has taken to discourage texting while driving.
2. Most people are not aware of the widespread impact of texting while driving across the United States. Do a search on "texting while driving." Examine all the search results for the first two pages. Enter the information into a two-column table. In the left column put the locality of the report and year. In the right column give a brief description of the search result, e.g., accident, report, court judgment, etc. What can you conclude from these search results and table?

to these resources through educational institutions and public libraries are inequitably distributed along ethnic and social class lines, as are many other information resources. Several studies have found that certain ethnic and income groups in the United States are less likely to have computers or online Internet access even though computer ownership and Internet access have soared in the past five years. Although the gap is narrowing, higher-income families in each ethnic group are still more likely to have home computers and Internet access than lower-income families in the same group.

A similar **digital divide** exists in U.S. schools, with schools in high-poverty areas less likely to have computers, high-quality educational technology programs, or Internet access availability for their students. Left uncorrected, the digital divide could lead to a society of information haves, computer literate and skilled, versus a large group of information have-nots, computer illiterate

and unskilled. Public interest groups want to narrow this digital divide by making digital information services—including the Internet—available to virtually everyone, just as basic telephone service is now.

Health Risks: RSI, CVS, and Technostress

The most common occupational disease today is **repetitive stress injury (RSI)**. RSI occurs when muscle groups are forced through repetitive actions often with high-impact loads (such as tennis) or tens of thousands of repetitions under low-impact loads (such as working at a computer keyboard).

The single largest source of RSI is computer keyboards. The most common kind of computer-related RSI is **carpal tunnel syndrome (CTS)**, in which pressure on the median nerve through the wrist's bony structure, called a carpal tunnel, produces pain. The pressure is caused by constant repetition of keystrokes: in a single shift, a word processor may perform 23,000 keystrokes. Symptoms of carpal tunnel syndrome include numbness, shooting pain, inability to grasp objects, and tingling. Millions of workers have been diagnosed with carpal tunnel syndrome.

RSI is avoidable. Designing workstations for a neutral wrist position (using a wrist rest to support the wrist), proper monitor stands, and footrests all contribute to proper posture and reduced RSI. Ergonomically correct keyboards are also an option. These measures should be supported by frequent rest breaks and rotation of employees to different jobs.

RSI is not the only occupational illness computers cause. Back and neck pain, leg stress, and foot pain also result from poor ergonomic designs of workstations. **Computer vision syndrome (CVS)** refers to any eyestrain condition related to display screen use in desktop computers, laptops, e-readers, smartphones, and hand-held video games. CVS affects about 90 percent of people who spend three hours or more per day at a computer (Beck, 2010). Its symptoms, which are usually temporary, include headaches, blurred vision, and dry and irritated eyes.

The newest computer-related malady is **technostress**, which is stress induced by computer use. Its symptoms include aggravation, hostility toward humans, impatience, and fatigue. According to experts, humans working continuously with computers come to expect other humans and human institutions to behave like computers, providing instant responses, attentiveness, and

Repetitive stress injury (RSI) is the leading occupational disease today. The single largest cause of RSI is computer keyboard work.

an absence of emotion. Technostress is thought to be related to high levels of job turnover in the computer industry, high levels of early retirement from computer-intense occupations, and elevated levels of drug and alcohol abuse.

The incidence of technostress is not known but is thought to be in the millions and growing rapidly in the United States. Computer-related jobs now top the list of stressful occupations based on health statistics in several industrialized countries.

To date, the role of radiation from computer display screens in occupational disease has not been proved. Video display terminals (VDTs) emit nonionizing electric and magnetic fields at low frequencies. These rays enter the body and have unknown effects on enzymes, molecules, chromosomes, and cell membranes. Long-term studies are investigating low-level electromagnetic fields and birth defects, stress, low birth weight, and other diseases. All manufacturers have reduced display screen emissions since the early 1980s, and European countries, such as Sweden, have adopted stiff radiation emission standards.

In addition to these maladies, computer technology may be harming our cognitive functions. Although the Internet has made it much easier for people to access, create, and use information, some experts believe that it is also preventing people from focusing and thinking clearly. The Interactive Session on Technology highlights the debate that has emerged about this problem.

The computer has become a part of our lives—personally as well as socially, culturally, and politically. It is unlikely that the issues and our choices will become easier as information technology continues to transform our world. The growth of the Internet and the information economy suggests that all the ethical and social issues we have described will be heightened further as we move into the first digital century.

INTERACTIVE SESSION: TECHNOLOGY

TOO MUCH TECHNOLOGY?

Do you think that the more information managers receive, the better their decisions? Well, think again. Most of us can no longer imagine the world without the Internet and without our favorite gadgets, whether they're iPads, smartphones, laptops, or cell phones. However, although these devices have brought about a new era of collaboration and communication, they also have introduced new concerns about our relationship with technology. Some researchers suggest that the Internet and other digital technologies are fundamentally changing the way we think—and not for the better. Is the Internet actually making us "dumber," and have we reached a point where we have too much technology? Or does the Internet offer so many new opportunities to discover information that it's actually making us "smarter." And, by the way, how do we define "dumber" and "smarter" in an Internet age?

Wait a second, you're saying. How could this be? The Internet is an unprecedented source for acquiring and sharing all types of information. Creating and disseminating media has never been easier. Resources like Wikipedia and Google have helped to organize knowledge and make that knowledge accessible to the world, and they would not have been possible without the Internet. And other digital media technologies have become indispensable parts of our lives. At first glance, it's not clear how such advancements could do anything but make us smarter.

In response to this argument, several authorities claim that making it possible for millions of people to create media—written blogs, photos, videos—has understandably lowered the quality of media. Bloggers very rarely do original reporting or research but instead copy it from professional resources. YouTube videos contributed by newbies to video come nowhere near the quality of professional videos. Newspapers struggle to stay in business while bloggers provide free content of inconsistent quality.

But similar warnings were issued in response to the development of the printing press. As Gutenberg's invention spread throughout Europe, contemporary literature exploded in popularity, and much of it was considered mediocre by intellectuals of the era. But rather than being destroyed, it was simply in the early stages of fundamental change. As people came to grips with the new technology and the new norms governing it, literature, newspapers, scientific journals, fiction, and non-fiction all began to contribute to the intellectual climate instead of detracting from it. Today, we can't imagine a world without print media.

Advocates of digital media argue that history is bound to repeat itself as we gain familiarity with the Internet and other newer technologies. The scientific revolution was galvanized by peer review and collaboration enabled by the printing press. According to many digital media supporters, the Internet will usher in a similar revolution in publishing capability and collaboration, and it will be a resounding success for society as a whole.

This may all be true, but from a cognitive standpoint, the effects of the Internet and other digital devices might not be so positive. New studies suggest that digital technologies are damaging our ability to think clearly and focus. Digital technology users develop an inevitable desire to multitask, doing several things at once while using their devices.

Although TV, the Internet, and video games are effective at developing our visual processing ability, research suggests that they detract from our ability to think deeply and retain information. It's true that the Internet grants users easy access to the world's information, but the medium through which that information is delivered is hurting our ability to think deeply and critically about what we read and hear. You'd be "smarter" (in the sense of being able to give an account of the content) by reading a book rather than viewing a video on the same topic while texting with your friends.

Using the Internet lends itself to multitasking. Pages are littered with hyperlinks to other sites; tabbed browsing allows us to switch rapidly between two windows; and we can surf the Web while watching TV, instant messaging friends, or talking on the phone. But the constant distractions and disruptions that are central to online experiences prevent our brains from creating the neural connections that constitute full understanding of a topic. Traditional print media, by contrast, makes it easier to fully concentrate on the content with fewer interruptions.

A recent study conducted by a team of researchers at Stanford found that multitaskers are not only more easily distracted, but were also surprisingly poor at

multitasking compared to people who rarely do so themselves. The team also found that multitaskers receive a jolt of excitement when confronted with a new piece of information or a new call, message, or e-mail.

The cellular structure of the brain is highly adaptable and adjusts to the tools we use, so multitaskers quickly become dependent on the excitement they experience when confronted with something new. This means that multitaskers continue to be easily distracted, even if they're totally unplugged from the devices they most often use.

Eyal Ophir, a cognitive scientist on the research team at Stanford, devised a test to measure this phenomenon. Subjects self-identifying as multitaskers were asked to keep track of red rectangles in series of images. When blue rectangles were introduced, multitaskers struggled to recognize whether or not the red rectangles had changed position from image to image. Normal testers significantly outperformed the multitaskers. Less than three percent of multitaskers (called "supertaskers") are able to manage multiple information streams at once; for the vast majority of us, multitasking does not result in greater productivity.

Neuroscientist Michael Merzenich argues that our brains are being 'massively remodeled' by our constant and ever-growing usage of the Web. And it's not just the Web that's contributing to this trend. Our ability to focus is also being undermined by the constant distractions provided by smart phones and other digital technology. Television and video games are no exception. Another study showed that when presented with two identical TV shows, one of which had a news crawl at the bottom, viewers retained much more information about the show without the news crawl. The impact of these technologies on children may be even greater than the impact on adults, because their brains are still developing, and they already struggle to set proper priorities and resist impulses.

The implications of recent research on the impact of Web 2.0 "social" technologies for management decision making are significant. As it turns out, the "always-connected" harried executive scurrying through airports and train stations, holding multiple voice and text conversations with clients and co-workers on sometimes several mobile devices, might not be a very good decision maker. In fact, the quality of decision making most likely falls as the quantity of digital information increases through multiple channels, and managers lose their critical thinking capabilities. Likewise, in terms of management productivity, studies of Internet use in the workplace suggest that Web 2.0 social technologies offer managers new opportunities to waste time rather than focus on their responsibilities. Checked your Facebook page today? Clearly we need to find out more about the impacts of mobile and social technologies on management work.

Sources: Randall Stross, "Computers at Home: Educational Hope vs. Teenage Reality," *The New York Times*, July 9, 2010; Matt Richtel, "Hooked on Gadgets, and Paying a Mental Price," *The New York Times*, June 6, 2010; Clay Shirky, "Does the Internet Make you Smarter?" *The Wall Street Journal*, June 4, 2010; Nicholas Carr, "Does the Internet Make you Dumber?" *The Wall Street Journal*, June 5, 2010; Ofer Malamud and Christian Pop-Echeles, "Home Computer Use and the Development of Human Capital," January 2010; and "Is Technology Producing a Decline in Critical Thinking and Analysis?" Science Daily, January 29, 2009.

CASE STUDY QUESTIONS

1. What are some of the arguments for and against the use of digital media?
2. How might the brain affected by constant digital media usage?
3. Do you think these arguments outweigh the positives of digital media usage? Why or why not?
4. What additional concerns are there for children using digital media? Should children under 8 use computers and cellphones? Why or why not?

MIS IN ACTION

1. Make a daily log for 1 week of all the activities you perform each day using digital technology (such as cell phones, computers, television, etc.) and the amount of time you spend on each. Note the occasions when you are multitasking. On average, how much time each day do you spend using digital technology? How much of this time do you spend multitasking? Do you think your life is too technology-intense? Justify your response.

4.4 Hands-on MIS Projects

The projects in this section give you hands-on experience in analyzing the privacy implications of using online data brokers, developing a corporate policy for employee Web usage, using blog creation tools to create a simple blog, and using Internet newsgroups for market research.

Management Decision Problems

1. USAData's Web site is linked to massive databases that consolidate personal data on millions of people. Anyone with a credit card can purchase marketing lists of consumers broken down by location, age, income level, and interests. If you click on Consumer Leads to order a consumer mailing list, you can find the names, addresses, and sometimes phone numbers of potential sales leads residing in a specific location and purchase the list of those names. One could use this capability to obtain a list, for example, of everyone in Peekskill, New York, making $150,000 or more per year. Do data brokers such as USAData raise privacy issues? Why or why not? If your name and other personal information were in this database, what limitations on access would you want in order to preserve your privacy? Consider the following data users: government agencies, your employer, private business firms, other individuals.
2. As the head of a small insurance company with six employees, you are concerned about how effectively your company is using its networking and human resources. Budgets are tight, and you are struggling to meet payrolls because employees are reporting many overtime hours. You do not believe that the employees have a sufficiently heavy work load to warrant working longer hours and are looking into the amount of time they spend on the Internet.

WEB USAGE REPORT FOR THE WEEK ENDING JANUARY 9, 2010.

USER NAME	MINUTES ONLINE	WEB SITE VISITED
Kelleher, Claire	45	www.doubleclick.net
Kelleher, Claire	107	www.yahoo.com
Kelleher, Claire	96	www.insweb.com
McMahon, Patricia	83	www.itunes.com
McMahon, Patricia	44	www.insweb.com
Milligan, Robert	112	www.youtube.com
Milligan, Robert	43	www.travelocity.com
Olivera, Ernesto	40	www.CNN.com
Talbot, Helen	125	www.etrade.com
Talbot, Helen	27	www.nordstrom.com
Talbot, Helen	35	www.yahoo.com
Talbot, Helen	73	www.ebay.com
Wright, Steven	23	www.facebook.com
Wright, Steven	15	www.autobytel.com

Each employee uses a computer with Internet access on the job. You requested the preceding weekly report of employee Web usage from your information systems department.

- Calculate the total amount of time each employee spent on the Web for the week and the total amount of time that company computers were used for this purpose. Rank the employees in the order of the amount of time each spent online.

- Do your findings and the contents of the report indicate any ethical problems employees are creating? Is the company creating an ethical problem by monitoring its employees' use of the Internet?
- Use the guidelines for ethical analysis presented in this chapter to develop a solution to the problems you have identified.

Achieving Operational Excellence: Creating a Simple Blog

Software skills: Blog creation
Business skills: Blog and Web page design

In this project, you'll learn how to build a simple blog of your own design using the online blog creation software available at Blogger.com. Pick a sport, hobby, or topic of interest as the theme for your blog. Name the blog, give it a title, and choose a template for the blog. Post at least four entries to the blog, adding a label for each posting. Edit your posts, if necessary. Upload an image, such as a photo from your hard drive or the Web to your blog. (Google recommends Open Photo, Flickr: Creative Commons, or Creative Commons Search as sources for photos. Be sure to credit the source for your image.) Add capabilities for other registered users, such as team members, to comment on your blog. Briefly describe how your blog could be useful to a company selling products or services related to the theme of your blog. List the tools available to Blogger (including Gadgets) that would make your blog more useful for business and describe the business uses of each. Save your blog and show it to your instructor.

Improving Decision Making: Using Internet Newsgroups for Online Market Research

Software Skills: Web browser software and Internet newsgroups
Business Skills: Using Internet newsgroups to identify potential customers

This project will help develop your Internet skills in using newsgroups for marketing. It will also ask you to think about the ethical implications of using information in online discussion groups for business purposes.

You are producing hiking boots that you sell through a few stores at this time. You think your boots are more comfortable than those of your competition. You believe you can undersell many of your competitors if you can significantly increase your production and sales. You would like to use Internet discussion groups interested in hiking, climbing, and camping both to sell your boots and to make them well known. Visit groups.google.com, which stores discussion postings from many thousands of newsgroups. Through this site you can locate all relevant newsgroups and search them by keyword, author's name, forum, date, and subject. Choose a message and examine it carefully, noting all the information you can obtain, including information about the author.

- How could you use these newsgroups to market your boots?
- What ethical principles might you be violating if you use these messages to sell your boots? Do you think there are ethical problems in using newsgroups this way? Explain your answer.
- Next use Google or Yahoo.com to search the hiking boots industry and locate sites that will help you develop other new ideas for contacting potential customers.
- Given what you have learned in this and previous chapters, prepare a plan to use newsgroups and other alternative methods to begin attracting visitors to your site.

Learning Track Modules

The following Learning Tracks provide content relevant to the topics covered in this chapter:

1. Developing a Corporate Code of Ethics for Information Systems
2. Creating a Web Page

Review Summary

1. *What ethical, social, and political issues are raised by information systems?*

   Information technology is introducing changes for which laws and rules of acceptable conduct have not yet been developed. Increasing computing power, storage, and networking capabilities—including the Internet—expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information is now communicated, copied, and manipulated in online environments pose new challenges to the protection of privacy and intellectual property. The main ethical, social, and political issues raised by information systems center around information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life.

2. *What specific principles for conduct can be used to guide ethical decisions?*

   Six ethical principles for judging conduct include the Golden Rule, Immanuel Kant's Categorical Imperative, Descartes' rule of change, the Utilitarian Principle, the Risk Aversion Principle, and the ethical "no free lunch" rule. These principles should be used in conjunction with an ethical analysis.

3. *Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?*

   Contemporary data storage and data analysis technology enables companies to easily gather personal data about individuals from many different sources and analyze these data to create detailed electronic profiles about individuals and their behaviors. Data flowing over the Internet can be monitored at many points. Cookies and other Web monitoring tools closely track the activities of Web site visitors. Not all Web sites have strong privacy protection policies, and they do not always allow for informed consent regarding the use of personal information. Traditional copyright laws are insufficient to protect against software piracy because digital material can be copied so easily and transmitted to many different locations simultaneously over the Internet.

4. *How have information systems affected everyday life?*

   Although computer systems have been sources of efficiency and wealth, they have some negative impacts. Computer errors can cause serious harm to individuals and organizations. Poor data quality is also responsible for disruptions and losses for businesses. Jobs can be lost when computers replace workers or tasks become unnecessary in reengineered business processes. The ability to own and use a computer may be exacerbating socioeconomic disparities among different racial groups and social classes. Widespread use of computers increases opportunities for computer crime and computer abuse. Computers can also create health problems, such as RSI, computer vision syndrome, and technostress.

Key Terms

Accountability, 129
Carpal tunnel syndrome (CTS), 149
Computer abuse, 145
Computer crime, 145
Computer vision syndrome (CVS), 149
Cookies, 134
Copyright, 139
Descartes' rule of change, 130
Digital divide, 148
Digital Millennium Copyright Act (DMCA), 141
Due process, 129
Ethical "no free lunch" rule, 130
Ethics, 124
Fair Information Practices (FIP), 132
Golden Rule, 130
Immanuel Kant's Categorical Imperative, 130
Information rights, 125
Informed consent, 134
Intellectual property, 138
Liability, 129
Nonobvious relationship awareness (NORA), 128
Opt-in, 137
Opt-out, 136

P3P, 137
Patent, 140
Privacy, 131
Profiling, 127
Repetitive stress injury (RSI), 149
Responsibility, 129
Risk Aversion Principle, 130
Safe harbor, 134
Spam, 145
Spyware, 135
Technostress, 149
Trade secret, 139
Utilitarian Principle, 130
Web beacons, 135

Review Questions

1. What ethical, social, and political issues are raised by information systems?
   - Explain how ethical, social, and political issues are connected and give some examples.
   - List and describe the key technological trends that heighten ethical concerns.
   - Differentiate between responsibility, accountability, and liability.
2. What specific principles for conduct can be used to guide ethical decisions?
   - List and describe the five steps in an ethical analysis.
   - Identify and describe six ethical principles.
3. Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?
   - Define privacy and fair information practices.
   - Explain how the Internet challenges the protection of individual privacy and intellectual property.
   - Explain how informed consent, legislation, industry self-regulation, and technology tools help protect the individual privacy of Internet users.
   - List and define the three different regimes that protect intellectual property rights.
4. How have information systems affected everyday life?
   - Explain why it is so difficult to hold software services liable for failure or injury.
   - List and describe the principal causes of system quality problems.
   - Name and describe four quality-of-life impacts of computers and information systems.
   - Define and describe technostress and RSI and explain their relationship to information technology.

Discussion Questions

1. Should producers of software-based services, such as ATMs, be held liable for economic injuries suffered when their systems fail?
2. Should companies be responsible for unemployment caused by their information systems? Why or why not?
3. Discuss the pros and cons of allowing companies to amass personal data for behavioral targeting.

Video Cases

Video Cases and Instructional Videos illustrating some of the concepts in this chapter are available. Contact your instructor to access these videos.

Collaboration and Teamwork: Developing a Corporate Ethics Code

With three or four of your classmates, develop a corporate ethics code that addresses both employee privacy and the privacy of customers and users of the corporate Web site. Be sure to consider e-mail privacy and employer monitoring of worksites, as well as corporate use of information about employees concerning their off-the-job behavior (e.g., lifestyle, marital arrangements, and so forth). If possible, use Google Sites to post links to Web pages, team communication announcements, and work assignments; to brainstorm; and to work collaboratively on project documents. Try to use Google Docs to develop your solution and presentation for the class.

When Radiation Therapy Kills

CASE STUDY

When new expensive medical therapies come along, promising to cure people of illness, one would think that the manufacturers, doctors, and technicians, along with the hospitals and state oversight agencies, would take extreme caution in their application and use. Often this is not the case. Contemporary radiation therapy offers a good example of society failing to anticipate and control the negative impacts of a technology powerful enough to kill people.

For individuals and their families suffering through a battle with cancer, technical advancements in radiation treatment represent hope and a chance for a healthy, cancer-free life. But when these highly complex machines used to treat cancers go awry or when medical technicians and doctors fail to follow proper safety procedures, it results in suffering worse than the ailments radiation aims to cure. A litany of horror stories underscores the consequences when hospitals fail to provide safe radiation treatment to cancer patients. In many of these horror stories, poor software design, poor human-machine interfaces, and lack of proper training are root causes of the problems.

The deaths of Scott Jerome-Parks and Alexandra Jn-Charles, both patients of New York City hospitals, are prime examples of radiation treatments going awry. Jerome-Parks worked in southern Manhattan near the site of the World Trade Center attacks, and suspected that the tongue cancer he developed later was related to toxic dust that he came in contact with after the attacks. His prognosis was uncertain at first, but he had some reason to be optimistic, given the quality of the treatment provided by state-of-the-art linear accelerators at St. Vincent's Hospital, which he selected for his treatment. But after receiving erroneous dosages of radiation several times, his condition drastically worsened.

For the most part, state-of-the-art linear accelerators do in fact provide effective and safe care for cancer patients, and Americans safely receive an increasing amount of medical radiation each year. Radiation helps to diagnose and treat all sorts of cancers, saving many patients' lives in the process, and is administered safely to over half of all cancer patients. Whereas older machines were only capable of imaging a tumor in two dimensions and projecting straight beams of radiation, newer linear accelerators are capable of modeling cancerous tumors in three dimensions and shaping beams of radiation to conform to those shapes.

One of the most common issues with radiation therapy is finding ways to destroy cancerous cells while preserving healthy cells. Using this beam-shaping technique, radiation doesn't pass through as much healthy tissue to reach the cancerous areas. Hospitals advertised their new accelerators as being able to treat previously untreatable cancers because of the precision of the beam-shaping method. Using older machinery, cancers that were too close to important bodily structures were considered too dangerous to treat with radiation due to the imprecision of the equipment.

How, then, are radiation-related accidents increasing in frequency, given the advances in linear acceleration technology? In the cases of Jerome-Parks and Jn-Charles, a combination of machine malfunctions and user error led to these frightening mistakes. Jerome-Parks's brain stem and neck were exposed to excessive dosages of radiation on three separate occasions because of a computer error. The linear accelerator used to treat Jerome-Parks is known as a multi-leaf collimator, a newer, more powerful model that uses over a hundred metal "leaves" to adjust the shape and strength of the beam. The St. Vincent's hospital collimator was made by Varian Medical Systems, a leading supplier of radiation equipment.

Dr. Anthony M. Berson, St. Vincent's chief radiation oncologist, reworked Mr. Jerome Parks's radiation treatment plan to give more protection to his teeth. Nina Kalach, the medical physicist in charge of implementing Jerome-Parks's radiation treatment plan, used Varian software to revise the plan. State records show that as Ms. Kalach was trying to save her work, the computer began seizing up, displaying an error message. The error message asked if Ms. Kalach wanted to save her changes before the program aborted and she responded that she did. Dr. Berson approved the plan.

Six minutes after another computer crash, the first of several radioactive beams was turned on, followed by several additional rounds of radiation the next few days. After the third treatment, Ms. Kalach ran a test to verify that the treatment plan was carried out as prescribed, and found that the multileaf collimator,

which was supposed to focus the beam precisely on Mr. Jerome Parks's tumor, was wide open. The patient's entire neck had been exposed and Mr. Jerome-Parks had seven times the prescribed dose of radiation.

As a result of the radiation overdose, Mr. Jerome-Parks's experienced deafness and near-blindness, ulcers in his mouth and throat, persistent nausea, and severe pain. His teeth were falling out, he couldn't swallow, and he was eventually unable to breathe. He died soon after, at the age of 43.

Jn-Charles's case was similarly tragic. A 32-year old mother of two from Brooklyn, she was diagnosed with an aggressive form of breast cancer, but her outlook seemed good after breast surgery and chemotherapy, with only 28 days of radiation treatments left to perform. However, the linear accelerator used at the Brooklyn hospital where Jn-Charles was treated was not a multi-leaf collimator, but instead a slightly older model, which uses a device known as a "wedge" to prevent radiation from reaching unintended areas of the body.

On the day of her 28th and final session, technicians realized that something had gone wrong. Jn-Charles's skin had slowly begun to peel and seemed to resist healing. When the hospital looked into the treatment to see why this could have happened, they discovered that the linear accelerator lacked the crucial command to insert the wedge, which must be programmed by the user. Technicians had failed to notice error messages on their screens indicating the missing wedge during each of the 27 sessions. This meant that Jn-Charles had been exposed to almost quadruple the normal amount of radiation during each of those 27 visits.

Ms. Jn-Charles's radiation overdose created a wound that would not heal despite numerous sessions in a hyperbaric chamber and multiple surgeries. Although the wound closed up over a year later, she died shortly afterwards.

It might seem that the carelessness or laziness of the medical technicians who administered treatment is primarily to blame in these cases, but other factors have contributed just as much. The complexity of new linear accelerator technology has not been accompanied with appropriate updates in software, training, safety procedures, and staffing. St. Vincent's hospital stated that system crashes similar to those involved in the improper therapy for Mr. Jerome-Parks "are not uncommon with the Varian software, and these issues have been communicated to Varian on numerous occasions."

Manufacturers of these machines boast that they can safely administer radiation treatment to more and more patients each day, but hospitals are rarely able to adjust their staffing to handle those workloads or increase the amount of training technicians receive before using newer machines. Medical technicians incorrectly assume that the new systems and software are going to work correctly, but in reality they have not been tested over long periods of time.

Many of these errors could have been detected if the machine operators were paying attention. In fact, many of the reported errors involve mistakes as simple and as egregious as treating patients for the wrong cancers; in one example, a brain cancer patient received radiation intended for breast cancer. Today's linear accelerators also lack some of the necessary safeguards given the amounts of radiation that they can deliver. For example, many linear accelerators are unable to alert users when a dosage of radiation far exceeds the necessary amount to effectively damage a cancerous tumor. Though responsibility ultimately rests with the technician, software programmers may not have designed their product with the technician's needs in mind.

Though the complexity of newer machines has exposed the inadequacy of the safety procedures hospitals employ for radiation treatments, the increasing number of patients receiving radiation due to the speed and increased capability of these machines has created other problems. Technicians at many of the hospitals reporting radiation-related errors reported being chronically overworked, often dealing with over a hundred patients per day. These already swamped medical technicians are not forced to check over the settings of the linear accelerators that they are handling, and errors that are introduced to the computer systems early on are difficult to detect. As a result, the same erroneous treatment may be administered repeatedly, until the technicians and doctors have a reason to check it. Often, the reason is a seriously injured patient.

Further complicating the issue is the fact that the total number of radiation-related accidents each year is essentially unknown. No single agency exists to collect data across the country on these accidents, and many states don't even require that accidents be reported. Even in states that do, hospitals are often reluctant to report errors that they've made, fearful that it will scare potential patients away, affecting their bottom lines. Some instances of hospital error are difficult to detect, since radiation-related cancer may appear a long while after the faulty treatment,

and under-radiation doesn't result in any observable injury. Even in New York, which has one of the strictest accident reporting requirements in place and keeps reporting hospitals anonymous to encourage them to share their data, a significant portion of errors go unreported—perhaps even a majority of errors.

The problem is certainly not unique to New York. In New Jersey, 36 patients were over-radiated at a single hospital by an inexperienced team of technicians, and the mistakes continued for months in the absence of a system that detected treatment errors. Patients in Louisiana, Texas, and California repeatedly received incorrect dosages that led to other crippling ailments. Nor is the issue unique to the United States. In Panama, 28 patients at the National Cancer Institute received overdoses of radiation for various types of cancers. Doctors had ordered medical physicists to add a fifth "block," or metal sheet similar to the "leaves" in a multi-leaf collimator, to their linear accelerators, which were only designed to support four blocks. When the staff attempted to get the machine software to work with the extra block, the results were miscalculated dosages and over-radiated patients.

The lack of a central U.S. reporting and regulatory agency for radiation therapy means that in the event of a radiation-related mistake, all of the groups involved are able to avoid ultimate responsibility. Medical machinery and software manufacturers claim that it's the doctors and medical technicians' responsibility to properly use the machines, and the hospitals' responsibility to properly budget time and resources for training. Technicians claim that they are understaffed and overworked, and that there are no procedures in place to check their work and no time to do so even if there were. Hospitals claim that the newer machinery lacks the proper fail-safe mechanisms and that there is no room on already limited budgets for the training that equipment manufacturers claim is required.

Currently, the responsibility for regulating these incidents falls upon the states, which vary widely in their enforcement of reporting. Many states require no reporting at all, but even in a state like Ohio, which requires reporting of medical mistakes within 15 days of the incident, these rules are routinely broken. Moreover, radiation technicians do not require a license in Ohio, as they do in many other states.

Dr. Fred A. Mettler, Jr., a radiation expert who has investigated radiation accidents worldwide, notes that "while there are accidents, you wouldn't want to scare people to death where they don't get needed radiation therapy." And it bears repeating that the vast majority of the time, radiation works, and saves some people from terminal cancer. But technicians, hospitals, equipment and software manufacturers, and regulators all need to collaborate to create a common set of safety procedures, software features, reporting standards, and certification requirements for technicians in order to reduce the number of radiation accidents.

Sources: Walt Bogdanich, "Medical Group Urges New Rules on Radiation," *The New York Times*, February 4, 2010; "As Technology Surges, Radiation Safeguards Lag," *The New York Times*, January 27, 2010; "Radiation Offers New Cures, and Ways to Do Harm," *The New York Times*, January 24, 2010; and "Case Studies: When Medical Radiation Goes Awry," *The New York Times*, January 21, 2010.

CASE STUDY QUESTIONS

1. What concepts in the chapter are illustrated in this case? What ethical issues are raised by radiation technology?
2. What management, organization, and technology factors were responsible for the problems detailed in this case? Explain the role of each.
3. Do you feel that any of the groups involved with this issue (hospital administrators, technicians, medical equipment and software manufacturers) should accept the majority of the blame for these incidents? Why or why not?
4. How would a central reporting agency that gathered data on radiation-related accidents help reduce the number of radiation therapy errors in the future?
5. If you were in charge of designing electronic software for a linear accelerator, what are some features you would include? Are there any features you would avoid?