4 Ethical and Social Issues in Information Systems

Learning Objectives

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

4-1 What ethical, social, and political issues are raised by information systems?

4-2 What specific principles for conduct can be used to guide ethical decisions?

4-3 Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?

4-4 How have information systems affected laws for establishing accountability and liability and the quality of everyday life?

MyMISLab™

Visit **mymislab.com** for simulations, tutorials, and end-of-chapter problems.

APTER CASES

Dark Side of Big Data

wagen Pollutes Its Reputation with Software to Cheat Emissions Testing

Ve Relying Too Much on Computers to Think for Us?

book Privacy: What Privacy?

EO CASES

Net Neutrality Means for You

ook and Google Privacy: What Privacy?

States v. Terrorism: Data Mining for Terrorists and Innocents

tional Video:

Mayer Schönberger on the Right to Be Forgotten

The Dark Side of Big Data

Organizations today are furiously mining big data, looking for ways to benefit from this technology. There are many big data success stories. For example, the Berg biopharmaceutical company is mining big data on patient tissue samples, clinical history, and demographic characteristics to pinpoint potential biomarkers for pancreatic cancer so that it can be detected much earlier and treated more effectively. The city of Barcelona has reduced its annual water bill by 25 percent by analyzing data from sensors installed in local parks to monitor soil moisture.

But there's a dark side to big data, and it has to do with privacy. We can now collect or analyze data on a much larger scale than ever before and use what we have learned about individuals in ways that may be harmful to them. The following are some examples.

Predictive policing In February 2014, the Chicago Police Department sent uniformed officers to make custom notification visits to individuals—especially gang members—whom a computer system had identified as likely to commit a crime in the future. The intent was to prevent crime by providing the targeted individuals with information about job training programs or informing them about increased penalties for people with certain backgrounds. Many community groups protested the practice as another form of racial profiling.

Insurance rates Auto insurance companies such as Progressive offer a small device to install in your car to analyze your driving habits, ostensibly to give you a better insurance rate. However, some of the criteria for lower auto insurance rates

© Sangoiri/123RF

are considered discriminatory. For example, insurance companies like people who don't drive late at night and don't spend much time in their cars. However, poorer people are more likely to work a late shift and to have longer commutes to work, which would increase their auto insurance rates.

Deloitte Consulting LLP developed a predictive modeling system for insurance applicants that predicts life expectancy by using data about individual consumers' buying habits as well as their personal and family medical histories. The company claims it can accurately predict whether people have any 1 of 17 diseases, including diabetes, tobacco-related cancer, cardiovascular disease, and depression, by analyzing their buying habits. What you pick up at the drugstore might increase your health insurance rates.

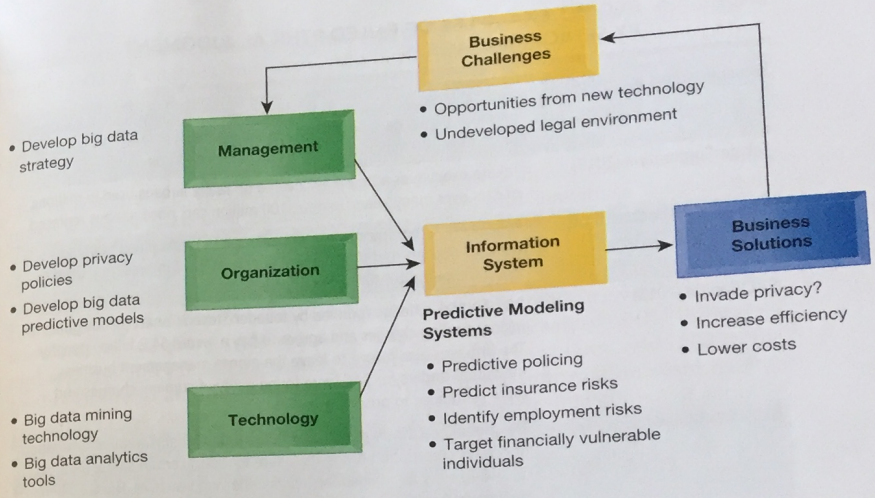
Computerized hiring More and more companies are turning to computerized systems to filter and hire job applicants, especially for lower-wage, service-sector jobs. The algorithms these systems use to evaluate job candidates may be preventing qualified applicants from obtaining these jobs. For example, some of these algorithms have determined that, statistically, people with shorter commutes are more likely to stay in a job longer than those with longer commutes or less reliable transportation or those who haven't been at their address for very long. If asked, "How long is your commute?" applicants with long commuting times will be scored lower for the job. Although such considerations may be statistically accurate, is it fair to screen job applicants this way?

Targeting financially vulnerable individuals Data brokers have been around for decades, but their tools for collecting and finely analyzing huge quantities of personal data grow ever more powerful. These data brokers now sell reports that specifically highlight and target financially vulnerable individuals. For example, a data broker might provide a report on retirees with little or no savings to a company offering reverse mortgages, high-cost loans, or other financially risky products. Very few rules or regulations exist to prevent targeting of vulnerable groups. Privacy laws and regulations haven't caught up with big data technology.

Sources: Brian Brinkmann, "Big Data Privacy: What Privacy?" Business2Community, March 2, 2016; Bernard Marr, "The 5 Scariest Ways Big Data Is Used Today," *DataInformed*, May 20, 2015; Victoria Craig, "Berg Hopes Big Data Will Lead to Breakthrough for Pancreatic Cancer, *Fox Business*, June 11, 2015; and "Police Gang-warning Tactic of 'Custom Notifications' Is Working," *Chicago Sun-Times*, March 27, 2014.

The challenges of big data to privacy described in the chapter-opening case show that technology can be a double-edged sword. It can be the source of many benefits, including the ability to combat disease and crime and to achieve major cost savings and efficiencies for business. At the same time, digital technology creates new opportunities for invading your privacy and using information that could cause you harm.

The chapter-opening diagram calls attention to important points this case and this chapter raise. Developments in data management technology and analytics have created opportunities for organizations to use big data to improve operations and decision making. One popular use of big data analysis is for predictive modeling—sifting through data to identify how specific individuals will behave and react in the future. The organizations described here are benefiting from using predictive modeling to fight crime, select the best employees, and



lower insurance and credit lending risks. However, their use of big data is also taking benefits away from individuals. Individuals might be subject to job discrimination, racial profiling, or higher insurance rates because organizations have new tools to assemble and analyze huge quantities of data about them. New privacy protection laws and policies need to be developed to keep up with the technologies for assembling and analyzing big data.

This case illustrates an ethical dilemma because it shows two sets of interests at work, the interests of organizations that have raised profits or even helped many people with medical breakthroughs and those who fervently believe that businesses and public organizations should not use big data analysis to invade privacy or harm individuals. As a manager, you will need to be sensitive to both the positive and negative impacts of information systems for your firm, employees, and customers. You will need to learn how to resolve ethical dilemmas involving information systems.

Here are some questions to think about: Does analyzing big data about people create an ethical dilemma? Why or why not? Should there be new privacy laws to protect individuals from being targeted by companies analyzing big data? Why or why not?

4-1 What ethical, social, and political issues are raised by information 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 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

TABLE 4.1 RECENT EXAMPLES OF FAILED ETHICAL JUDGMENT BY SENIOR MANAGERS

General Motors Inc. (2015)	General Motors CEO admits the firm covered up faulty ignition switches for more than a decade, resulting in the deaths of at least 114 customers. More than 100 million vehicles worldwide need to be replaced.
Takata Corporation (2015)	Takata executives admit they covered up faulty airbags used in millions of cars over many years. To date, 100 million cars need airbags replaced.
Citigroup, JPMorgan Chase, Barclays, UBS (2012)	Four of the largest money center banks in the world plead guilty to criminal charges that they manipulated the LIBOR interest rate used to establish loan rates throughout the world.
SAC Capital (2013)	SAC Capital, a hedge fund led by founder Steven Cohen, pleads guilty to insider trading charges and agrees to pay a record $1.2 billion penalty. The firm was also forced to leave the money management business. Individual traders for SAC were found guilty of criminal charges and were sentenced to prison.
GlaxoSmithKline LLC (2012)	The global healthcare giant admitted to unlawful and criminal promotion of certain prescription drugs, its failure to report certain safety data, and its civil liability for alleged false price reporting practices. Fined $3 billion, the largest healthcare fraud settlement in U.S. history and the largest payment ever by a drug company.
McKinsey & Company (2012)	CEO Rajat Gupta heard on tapes leaking insider information. The former CEO of prestigious management consulting firm McKinsey & Company was found guilty in 2012 and sentenced to two years in prison.
Bank of America (2012)	Federal prosecutors accused Bank of America and its affiliate, Countrywide Financial, of defrauding government-backed mortgage agencies by churning out loans at a rapid pace without proper controls. Prosecutors sought $1 billion in penalties from the bank as compensation for the behavior that they say forced taxpayers to guarantee billions in bad loans.

business 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 business firms would, in the past, often pay for the legal defense of their employees enmeshed in civil charges and criminal investigations, firms are now 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 will 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

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.

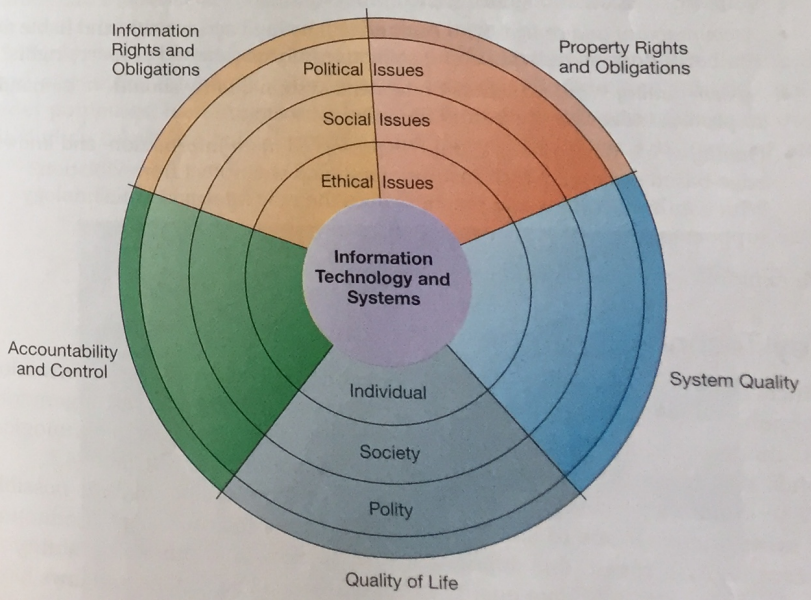
Ethical issues in information systems have been given new urgency by the rise of the Internet and e-commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information,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

Other pressing ethical issues that information systems raise 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 shown in Figure 4.1. Imagine society as a more or less calm pond on a summer day,

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

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.

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 that information systems raise 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 does the new information technology support?

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. Five key technological trends are responsible for these ethical stresses, 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.

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 and become more vulnerable to system failures.
Data storage costs rapidly decline	Organizations can easily maintain detailed databases on individuals. There are no limits on the data collected about you.
Data analysis advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individual behavior. Large-scale population surveillance is enabled.
Networking advances	The cost of moving data and making it accessible from anywhere falls exponentially. Access to data becomes more difficult to control.
Mobile device growth impact	Individual cell phones may be tracked without user consent or knowledge. The always-on device becomes a tether.

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 inexpensive and effective. Enormous data storage systems for terabytes and petabytes of data are now available on-site or as online services for firms of all sizes 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 can find out highly detailed personal information about individuals. With contemporary data management tools (see Chapter 6), 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 digital 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 websites. Put together and

© Andriy Popov/123RF

mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, what you read and watch, and your political interests.

Companies purchase relevant personal information from these sources to help them more finely target their marketing campaigns. Chapters 6 and 12 describe how companies can analyze large pools of data from multiple sources to identify buying patterns of customers rapidly and suggest individual responses. The use of computers to combine data from multiple sources and create digital dossiers of detailed information on individuals is called **profiling**.

For example, several thousand of the most popular websites 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.

LexisNexis Risk Solutions (formerly 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 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 Risk Solutions are flourishing. The two largest credit card networks, Visa Inc. and MasterCard Inc., have agreed to link credit card purchase information with consumer social network and other information to create customer profiles that could be sold to advertising firms.

A 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 connections that might help identify criminals or terrorists (see Figure 4.2).

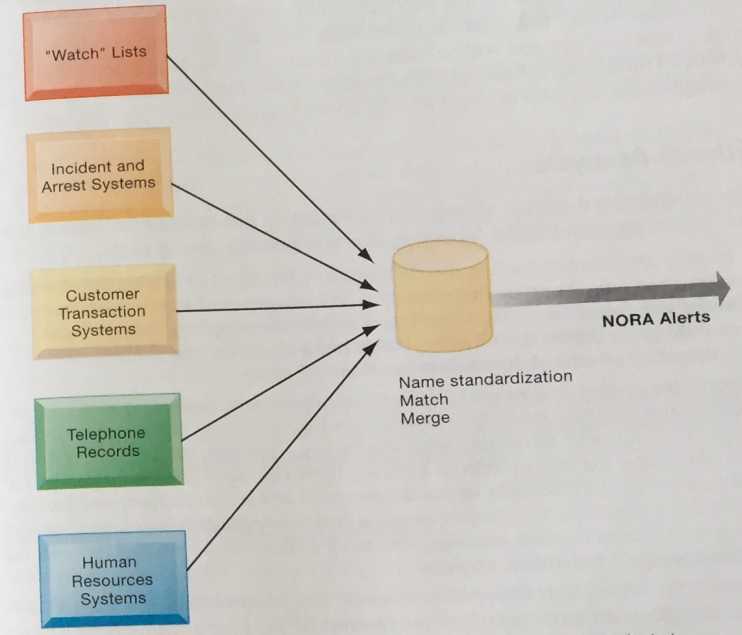
NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool 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 reduce greatly the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely by using small desktop machines, mobile devices, and cloud servers, permitting an invasion of privacy on a scale and with a precision heretofore unimaginable.

4-2 What specific principles for conduct can be used to guide ethical decisions?

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 [illegible] the main features of ethical choice?

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.

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 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 ability exists 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 effects 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 the facts clearly* 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-opening case study illustrates two competing values: the need to make organizations more efficient and cost-effective and the need to respect 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 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 in 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. 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 actions which have extremely high failure costs; focus on reducing the probability of accidents occurring.
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 companies use voice recognition software to reduce the size of their customer support staff 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 nonbusiness activities. Facebook monitors its subscribers and then sells the information to advertisers and app developers (see the chapter-ending case study).

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

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 digital and other forms of high-tech surveillance. 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 United States, Canadian, and German constitutions in a variety of 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 and digital 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. There were 20 major privacy bills before Congress in 2015, although few of them are likely to be passed in the near future (Kosseff, 2014).

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 and updated most recently in 2010 to take into account new privacy-invading technology (Federal Trade Commission [FTC], 2010; 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

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 (HIPAA) of 1996 Childrens Online Privacy Protection Act (COPPA) of 1998 Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999

agency—requires information about the individual to support the transaction. After 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 Federal Trade Commission (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 websites to obtain parental permission before collecting information on children under the age of 13. The FTC has recommended additional legislation to protect online consumer privacy in

TABLE 4.4 FEDERAL TRADE COMMISSION FAIR INFORMATION PRACTICE PRINCIPLES

Notice/awareness (core principle). Websites 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.
Choice/consent (core principle). A choice regime must be 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.
Access/participation. Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security. Data collectors must take responsible steps to ensure that consumer information is accurate and secure from unauthorized use.
Enforcement. A mechanism must be in place to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulations.

advertising networks that collect records of consumer web activity to develop detailed profiles, which other companies then use to target online ads. In 2010, the FTC added three practices to its framework for privacy. Firms should adopt privacy by design, building products and services that protect privacy, firms should increase the transparency of their data practices, and firms should require consumer consent and provide clear options to opt out of data collection schemes (FTC, 2012). 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 2012, the FTC extended its FIP doctrine to address the issue of 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 that an opt-out capability is the only way to avoid tracking. Nevertheless, there is an emerging consensus among all parties that greater transparency and user control (especially making opting out of tracking the default option) is required to deal with behavioral tracking. Public opinion polls show an ongoing distrust of online marketers. Although there are many studies of privacy issues at the federal level, there has been no significant legislation in recent years. A 2016 survey by the Pew Research Center found 91 percent of Americans feel consumers have lost control of their personal information online and 86 percent have taken steps to protect their information online.

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 that healthcare providers, hospitals, and health insurers maintain and the right to authorize how protected information about themselves can be used or disclosed. Doctors, hospitals, and other healthcare 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 consumer's 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. In 2009, the European Parliament passed new rules governing the use of third-party cookies for behavioral tracking purposes. These new rules were implemented in May 2011 and require website visitors to give explicit consent to be tracked by cookies. Websites will be required to have highly visible warnings on their pages if third-party cookies are being used (European Parliament, 2009).

In January 2012, the EU issued significant proposed changes to its data protection rules, the first overhaul since 1995. The new rules would apply to all companies providing services in Europe and require Internet companies such as Amazon, Facebook, Apple, Google, and others to obtain explicit consent from consumers about the use of their personal data, delete information at the user's request (based on the right to be forgotten), and retain information only as long as absolutely necessary. In 2014, the European Parliament gave strong support to significant changes in privacy policies by extending greater control to users of the Internet. Although the privacy policies of United States firms (in contrast to the government's) are largely voluntary, in Europe, corporate privacy policies are mandated and more consistent across jurisdictions.

Among the changes being discussed are a requirement for firms to inform users before collecting data, every time they collect data, and how it will be used. Users would have to give consent to any data collection. Other proposals call for users to have a right of access to personal data, and the right to be forgotten. The right to be forgotten was upheld by a European Union court in 2014, and since then, Google has had to respond to more than 200,000 requests to remove personal information from its search engine.

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 by using self-policing, regulation, and government enforcement of fair trade statutes. However, in October 2015, Europe's highest court struck down the safe harbor agreement entirely, in large part due to the revelations by Edward Snowden that Facebook had shared personal information on European citizens with the NSA and therefore violated the terms of the agreement. In 2016 a new agreement was reached that allows European regulators to monitor American use of European private information.

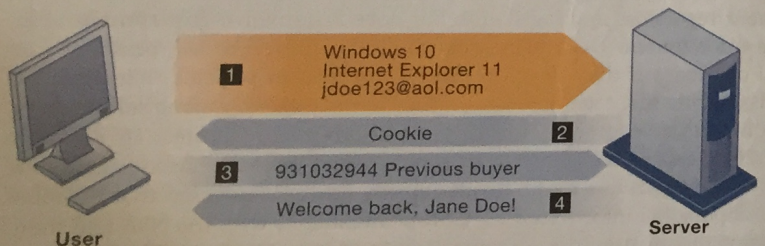
Internet Challenges to Privacy

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

Websites track searches that have been conducted, the websites and web pages visited, the online content a person has accessed, and what items that person has inspected or purchased over the web. This monitoring and tracking of website visitors occurs in the background without the visitor's knowledge. It is conducted not just by individual websites but by advertising networks such as Microsoft Advertising, Yahoo, and Google's DoubleClick that are capable of tracking personal browsing behavior across thousands of websites. Both website publishers and the advertising industry defend tracking of individuals across the web because doing so allows more relevant ads to be targeted to users, and it pays for the cost of publishing websites. In this sense, it's like broadcast television: advertiser-supported content that is free to the user. The commercial demand for this personal information is virtually insatiable. However, these practices also impinge on individual privacy. **Cookies** are small text files deposited on a computer hard drive when a user visits websites. Cookies identify the visitor's web browser software and track visits to the website. When the visitor returns to a site that has stored a cookie, the website software searches the visitor's computer, finds the cookie, and knows 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 content 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 examine the behavior of website visitors. Figure 4.3 illustrates how cookies work.

Websites 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. Website owners can also combine the data they have gathered from cookies and other website 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.

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 website, 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 website on a visitor's hard drive. When the visitor returns to that website, 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 website can then use these data to display personalized information.

There are now even more subtle and surreptitious tools for surveillance of Internet users. So-called super cookies or Flash cookies cannot be easily deleted and can be installed whenever a person clicks a Flash video. Flash uses these so-called local shared object files to play videos and puts them on the user's computer without his or her consent. Marketers use web beacons as another tool to monitor online behavior. **Web beacons**, also called *web bugs* (or simply tracking files), are tiny software programs that keep a record of users' online clickstreams. They report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and web pages that are designed to monitor the behavior of the user visiting a website or sending e-mail. Web beacons are placed on popular websites by third-party firms who pay the websites a fee for access to their audience. So how common is web tracking? In a path-breaking series of articles in the *Wall Street Journal*, researchers examined the tracking files on 50 of the most popular U.S websites. What they found revealed a very widespread surveillance system. On the 50 sites, they discovered 3,180 tracking files installed on visitor computers. Only one site, Wikipedia, had no tracking files. Two-thirds of the tracking files came from 131 companies whose primary business is identifying and tracking Internet users to create consumer profiles that can be sold to advertising firms looking for specific types of customers. The biggest trackers were Google, Microsoft, and Quantcast, all of whom are in the business of selling ads to advertising firms and marketers. A follow-up study found tracking on the 50 most popular sites had risen nearly fivefold due to the growth of online ad auctions where advertisers buy the data about users' web-browsing behavior.

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

Nearly 80 percent of global Internet users use Google Search and other Google 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 believe that Google possesses the largest collection of personal information in the world—more data on more people than any government agency. The nearest competitor is Facebook.

After Google acquired the advertising network DoubleClick in 2007, Google began using behavioral targeting to help it display more relevant ads based on users' search activities and to target individuals as they move from one site to another to show them display or banner ads. Google allows tracking software on its search pages, and using DoubleClick, it can track users across the Internet. 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 such as age, demographics, region, and other web activities (such as blogging). Google's AdSense program enables Google to help advertisers select keywords and design ads for various market segments based on search histories such as helping a clothing website create and test ads targeted at teenage females. A recent study found that 88 percent of 400,000 websites had at least one Google tracking bug.

Google also scans the contents of messages users receive 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 Google mobile applications, and its DoubleClick ad network serves up targeted banner ads.

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. These firms argue that when users agree to the sites' terms of service, they are also agreeing to allow the site to collect information about their online activities. An **opt-out** model of informed consent permits the collection of personal information until the consumer specifically requests the data not to 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. Here, the default option is no collection of user information.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. The online advertising 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 websites 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 such as Microsoft, Mozilla Foundation, Yahoo, and Google have recently adopted policies on their own in an effort to address public concern about tracking people online. Microsoft's Internet Explorer 11 web browser was released in 2015 with the opt-out option as the default, but by 2016 Microsoft removed this feature in large part because most websites ignore the request to opt out. Other browsers have opt-out options, but users need to turn them on, and most users fail to do this. AOL established an opt-out policy that allows users of its site to choose not to be tracked. Yahoo follows NAI guidelines and 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. For commercial websites that depend on advertising to support themselves, most revenue derives from selling customer information. Of the companies that do post privacy policies on their websites, about half do not monitor their sites to ensure that they adhere to these policies. The vast majority of online customers claim they are concerned about online privacy, but fewer than half read the privacy statements on websites. In general, website privacy policies require a law degree to understand and are ambiguous about key terms (Laudon and Traver, 2015). In 2016, what firms such as Facebook and Google call a privacy policy is in fact a data use policy. The concept of privacy is associated with consumer rights, which firms do not wish to recognize. A data use policy simply tells customers how the information will be used without any mention of rights.

In one of the more insightful studies of consumer attitudes toward Internet privacy, a group of Berkeley students conducted surveys of online users and of complaints filed with the FTC involving privacy issues. Some of their results show that people feel they have no control over the information collected about them, and they don't know who to complain to. Websites collect all this information but do not let users have access, the website policies are unclear, and they share data with affiliates but never identify who the affiliates are and how many there are. Web bug trackers are ubiquitous, and users are

not informed of trackers on the pages they 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, there are a few technologies that can protect user privacy during interactions with websites. 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. For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another.

Because of growing public criticism of behavioral tracking, targeting of ads, and the failure of industry to self-regulate, attention has shifted to browsers. Many browsers have Do Not Track options. For users who have selected the Do Not Track browser option, their browser will send a request to websites requesting the user's behavior not be tracked, but websites are not obligated to honor their visitors' requests not to be tracked. There is no online advertising industry agreement on how to respond to Do Not Track requests nor, currently, any legislation requiring websites to stop tracking. Private browser encryption software or apps on mobile devices provide consumers a powerful opportunity to at least keep their messages private.

Property Rights: Intellectual Property

Contemporary information systems have severely challenged existing laws and social practices that protect **intellectual property**. Intellectual property is considered to be tangible and intangible products of the mind created by individuals or 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 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 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 copies of the original sold in commerce; it sets forth the rights of the purchaser to use the software while the creator retains legal title.

Copyright protects against copying 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 v. 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 v. 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 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.

In what some call the patent trial of the century, in 2011, Apple sued Samsung for violating its patents for iPhones, iPads, and iPods. On August 24, 2012, a California jury in federal district court delivered a decisive victory to Apple and a stunning defeat to Samsung. The jury awarded Apple $1 billion in damages. The decision established criteria for determining just how close a competitor can come to an industry-leading and standard-setting product like Apple's iPhone before it violates the design and utility patents of the leading firm. The same court ruled that Samsung could not sell its new tablet computer (Galaxy 10.1) in the United States. In a later patent dispute, Samsung won an infringement case against Apple. In June 2013, the United States International Trade Commission issued a ban for a handful of older iPhone and iPad devices because they violated Samsung patents from years ago. In 2014, Apple sued Samsung again, claiming infringement of five patents. The patents cover hardware and software techniques for handling photos, videos, and lists used on the popular Galaxy 5. Apple sought $2 billion in damages. In 2015, the U.S. Court of Appeals reaffirmed that Samsung had copied specific design patents, but dropped the damages Apple was granted to $930 million.

To make matters more complicated, Apple has been one of Samsung's largest customers for flash memory processors, graphic chips, solid-state drives, and display parts that are used in Apple's iPhones, iPads, iPod Touch devices, and MacBooks. The Samsung and Apple patent cases are indicative of the complex relationships among the leading computer firms.

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; compactness—making theft easy; and difficulties in establishing uniqueness.

The proliferation of digital 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 BSA Global Software Survey conducted by International Data Corporation and The Software Alliance (also known as BSA) reported that the rate of global software piracy was 39 percent in 2015 (The Software Alliance, 2016).

The Internet was designed to transmit information freely around the world, including copyrighted information. You can easily copy and distribute virtually anything to millions of people worldwide, 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 music files on the Internet for several decades. File-sharing services such as Napster and, later, Grokster, Kazaa, Morpheus, Megaupload, and The Pirate Bay sprang up to help users locate and swap digital music and video files, including those protected by copyright. Illegal file sharing became so widespread that it threatened

the viability of the music recording industry and, at one point, consumed 20 percent of Internet bandwidth. The recording industry won several legal battles for shutting these services down, but it has not been able to halt illegal file sharing entirely. The motion picture and cable television industries are waging similar battles. Several European nations have worked with U.S. authorities to shut down illegal sharing sites, with mixed results.

As legitimate online music stores such as the iTunes Store expanded, some forms of illegal file sharing have declined. Technology has radically altered the prospects for intellectual property protection from theft, at least for music, videos, and television shows (less so for software). The Apple iTunes Store legitimated paying for music and entertainment and created a closed environment from which music and videos could not be easily copied and widely distributed unless played on Apple devices. Amazon's Kindle also protects the rights of publishers and writers because its books cannot be copied to the Internet and distributed. Streaming of Internet radio, on services such as Pandora and Spotify, and Hollywood movies (at sites such as Hulu and Netflix) also inhibits piracy because the streams cannot be easily recorded on separate devices, and videos can be downloaded so easily. Despite these gains in legitimate online music platforms, Apple's iTunes based on downloads of singles and streaming services' unwillingness to pay labels and artists a reasonable fee for playing have resulted in a 50 percent decline in record industry revenues since 2000 and the loss of thousands of jobs.

The **Digital Millennium Copyright Act (DMCA)** of 1998 also provides 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 they are hosting when the ISPs 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.

4-4 How have information systems affected laws for establishing accountability and liability and the quality of everyday life?

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 social network site like Facebook or Twitter be held liable and accountable for the posting of pornographic material or racial insults, or should they be held harmless against any liability for what users post (as is true of common carriers, such as the telephone system)? What about the Internet? If you outsource your information processing to the cloud, and the cloud provider fails to provide adequate service, what can you do? Cloud providers often claim the software you are using is the problem, not the cloud servers.

Computer-Related Liability Problems

In late 2013 hackers obtained credit card, debit card, and additional personal information about 70 to 110 million customers of Target, one of the largest U.S. retailers. Target's sales took an immediate hit from which it has still not completely recovered. Target says it has spent over $60 million to strengthen its systems. In 2015, Target agreed to pay $10 million to customers and $19 million to MasterCard. It has paid an even greater price through the loss of sales and trust.

Who is liable for any economic harm caused to individuals or businesses whose credit cards were compromised? Is Target responsible for allowing the breach to occur despite efforts it did make to secure the information? Or is this just a cost of doing business in a credit card world where customers and businesses have insurance policies to protect them against losses? Customers, for instance, have a maximum liability of $50 for credit card theft under federal banking law.

Are information system managers responsible for the harm that corporate systems can do? Beyond IT managers, 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); hence, courts have been wary of holding software authors liable for 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 of books and periodicals have not been held liable because of fears that liability claims would interfere with First Amendment rights guaranteeing freedom of expression. The kind of harm software failures causes is rarely fatal and typically inconveniences users but does not physically harm them (the exception being medical devices).

What about software as a service? ATMs are a service provided to bank customers. If this service fails, 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 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. Likewise, cable networks are considered private networks not subject to regulation, but broadcasters using the public air waves are subject to a wide variety of federal and local constraints on content and facilities. In the United States, with few exceptions, websites are not held liable for content posted on their sites regardless of whether it was placed there by the website owners or users.

System Quality: Data Quality and System Errors

White Christmas turned into a blackout for millions of Netflix customers and social network users on December 24, 2012. The blackout was caused by the failure of Amazon's cloud computing service (AWS), which provides storage and computing power for all kinds of websites and services, including Netflix. The loss of service lasted for a day. Amazon blamed it on elastic load balancing, a software program that balances the loads on all its cloud servers to prevent overload. Amazon's cloud computing services have had several subsequent outages, although not as long-lasting as the Christmas Eve outage. In September 2015 AWS experienced a major outage again. Outages at cloud computing services are rare but recurring. These outages have called into question the reliability and quality of cloud services. Are these outages acceptable?

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. The gray area is that some system errors are foreseeable and correctable only at very great expense, 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 falter 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 imperfect 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, they 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 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 client–server computing, coupled with an ideology of empowerment of Twitter and social media users, and the decentralization of decision making to lower organizational levels, up until recently reduced the fears of power centralization in government 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. At the same time, corporate Internet behemoths such as Google, Apple, Yahoo, Amazon, and Microsoft have come to dominate the collection and analysis of personal private information of all citizens. Since the terrorist attacks against the United States on September 11, 2001, the federal government has greatly expanded its use of this private sector information under the authority of the Patriot Act of 2001 and subsequent and secret executive orders. In this sense, power has become more centralized in the hands of a few private oligopolies and large government agencies.

Rapidity of Change: Reduced Response Time to Competition

Information systems have helped to create much more efficient national and international markets. Today's 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. One impact of Uber (see Chapter 10) and other on-demand services firms is to create just-in-time jobs with no benefits or insurance for employees.

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, mobile 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, the advent of information 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 into commuting time, vacation time, and leisure time. The explosive growth and use of smartphones have only heightened the sense of many employees that they are never away from work.

Even leisure time spent on the computer threatens these close social relationships. Extensive Internet and cell phone 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 antisocial behavior, such as the recent upsurge in cyberbullying.

enience of working at
e do-anything-anywhere
g environment can blur
ional boundaries between
family time.

© Hongqi Zhang/123RF

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, 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. Secondary schools, for instance, increasingly use and rely on educational software. Test results are often stored off campus. If these systems were to shut down, there is no backup educational structure or content that can make up for the loss of the system. 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 by using a computer or against a computer system. Simply accessing a computer system without authorization or with intent to do harm, even by accident, is now a federal crime. The most frequent types of incidents comprise a greatest hits list of cybercrime: malware, phishing, network interruption, spyware, and denial of service attacks. (PwC, 2015). The true cost of all computer crime is unknown, but it is estimated to be in the billions of dollars. You can find a more detailed discussion of computer crime in Chapter 8.

Computer abuse is the commission of acts involving a computer that may not be illegal but 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. Originally, **spam** was junk e-mail an organization or individual sent to a mass audience of Internet

users who had expressed no interest in the product or service being marketed. However, as cell phone use has mushroomed, spam was certain to follow. Identity and financial-theft cybercriminals are turning their attention to smartphones as users check e-mail, do online banking, pay bills, and reveal personal information. Cell phone spam usually comes in the form of SMS text messages, but increasingly, users are receiving spam in their Facebook Newsfeed and messaging service as well. 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 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 costs only a few cents to send thousands of messages advertising wares to Internet users. The percentage of all e-mail that is spam was estimated at around 65 percent in 2015 (Kaspersky, 2015). Most spam originates from bot networks, which consist of thousands of captured PCs that can initiate and relay spam messages. Spam volume has declined somewhat since authorities took down the Rustock botnet in 2011. Spam costs for businesses are very high (estimated at more than $50 billion per year) because of the computing and network resources billions of unwanted e-mail messages and the time required to deal with them consume.

ISPs 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 filters by continually changing their e-mail accounts, by incorporating spam messages in images, by embedding spam in e-mail attachments and digital greeting cards, and by using other people's computers that have been hijacked by botnets (see Chapter 8). Many spam messages are sent from one country although another country hosts the spam website.

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

The U.S. CAN-SPAM Act of 2003, which went into effect in 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 in large part because of the Internet's exceptionally poor security and the use of offshore servers and botnets. Most large-scale spamming has moved offshore to Russia and Eastern Europe where hackers control global botnets capable of generating billions of spam messages. The largest spam network in recent years was the Russian network Festi based in St. Petersburg. Festi is best known as the spam generator behind the global Viagra-spam industry, which stretches from Russia to Indian pharmaceutical firms selling counterfeit Viagra.

For a many years automobile manufacturers around the globe have tried to find ways of manipulating mileage and emissions tests to produce more favorable results on paper than what actually takes place on the road. The use of software for this purpose recently came to light with revelations that Volkswagen Group installed "cheating" software in some of its car models to violate the U.S. Clean Air Act, as described in the Interactive Session on Technology.