CHAPTER

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?

4-5 How will MIS help my career?

CHAPTER CASES

- Are Cars Becoming Big Brother on Wheels?
- The Boeing 737 MAX Crashes: What Happened and Why?
- How Harmful Are Smartphones?
- Facebook Privacy: Your Life for Sale

VIDEO CASES

- What Net Neutrality Means for You
- Facebook and Google Privacy: What Privacy?
- United States v. Terrorism: Data Mining for Terrorists and Innocents

Instructional Video:

- Viktor Mayer-Schönberger on the Right to Be Forgotten

MyLab MIS

- Discussion Questions: 4-5, 4-6, 4-7
- Hands-On MIS Projects: 4-8, 4-9, 4-10, 4-11

ARE CARS BECOMING BIG BROTHER ON WHEELS?

Cars today have become sophisticated listening posts on wheels. They can track phone calls and texts, record what radio stations you listen to, monitor the speed at which you drive and your braking actions, and even tell when you are breaking the speed limit, often without your knowledge.

Tens of millions of drivers in the United States are currently being monitored, with that number rising every time a new vehicle is sold or leased. There are at least 78 million cars on the road with an embedded cyberconnection that can be used for monitoring drivers. According to research firm Gartner Inc., 98 percent of new cars sold in the United States and Europe will be connected by 2021.

Since 2014, every new car in the United States comes with an event data recorder (EDR), which records and stores over a dozen data points, including vehicle speed, seat belt use, and braking activation. EDR data are available to any auto maker as well as to insurance companies, which use these stored EDR data to help establish responsibility for an accident or to detect fraud.

EDRs are mandated and regulated by the US government, but other data-gathering software in today's cars is not. Such software underlies numerous sensors, diagnostic systems, in-dash navigation systems, and built-in cellular connections, as well as driver-assistance systems to help drivers park, stay in their lane, avoid rear-ending another car, and steer for short time periods. All of this software keeps track of what drivers are doing. Newer cars may record driver eye movements, the weight of people in the front seats, and whether the driver's hands are on the wheel. Smartphones, whether connected to the car or not, can also track your activities, including any texting while driving. Auto makers are able to mine all this information, as are app developers and companies such as Google or Spotify.

With the exception of medical information, the United States has few regulations governing what data companies can gather and how they can use the data. Companies generally are not required to conceal names or other personal details. In most cases the driver must consent to allowing his or her personal information to be tracked or monitored. Many people unwittingly provide this consent when they check off a box on one of the lengthy service agreement forms required to register a car's in-dash system or navigation app.

Collecting such large amounts of personal data generated by drivers has raised concerns about whether automakers and others are doing enough to protect people's privacy. Drivers may welcome the use of information to relay helpful diagnostic information or updates on nearby traffic jams. But they do not necessarily endorse other uses, and automakers have refrained from commenting on future data collection plans and policies.

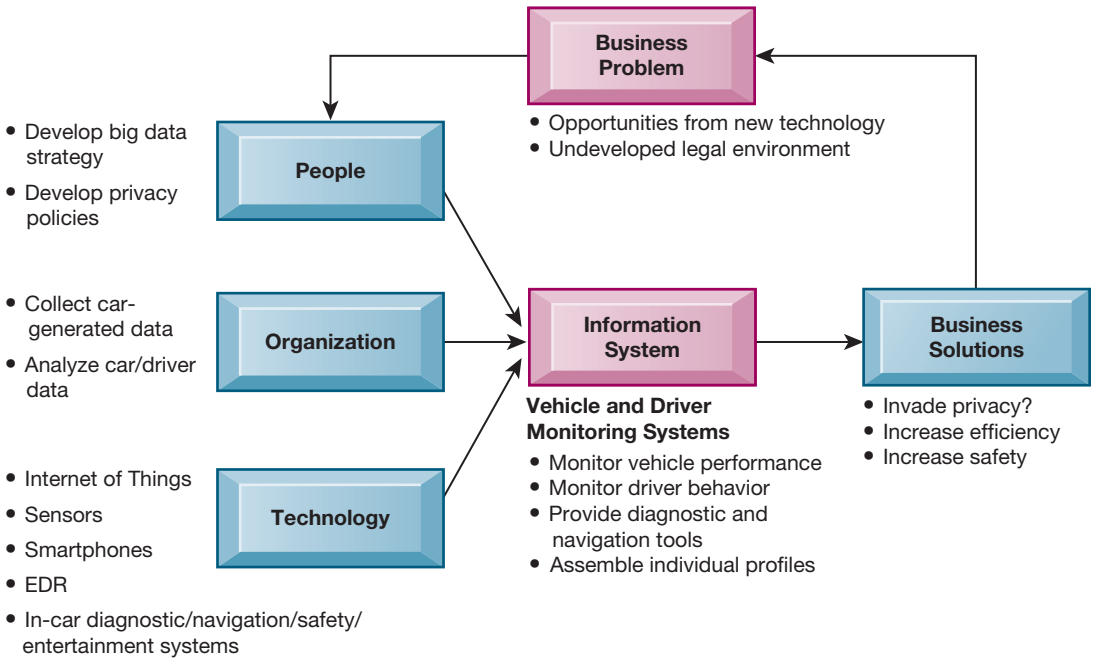
© Metamorworks/Shutterstock

Automakers argue that the data are valuable for improving vehicle performance and vehicle safety and soon will be able to reduce traffic accidents and fatalities. Amassing detailed data about human driving behavior is also essential for the development of self-driving cars. But privacy experts believe the practice is dangerous. With enough data about driver behavior, individual profiles as unique as fingerprints could be developed. Trips to businesses reveal buying habits and relationships that could be valuable to corporations, government agencies, or law enforcement. For example, frequent visits to a liquor store or mental health clinic could reveal information about someone's drinking habits or health problems. People obviously would not want such confidential data shared with others.

Sources: Jaclyn Trop, "The Spy Inside Your Car," *Fortune*, January 24, 2019; Peter Holley, "Big Brother on Wheels: Why Your Car Company May Know More About You Than Your Spouse." *Washington Post*, January 15, 2018; Christina Rogers, "What Your Car Knows about You," *Wall Street Journal*, August 18, 2018; John R. Quain, "Cars Suck Up Data About You. Where Does It All Go?" *New York Times*, July 27, 2017; and Russ Heaps, "Data Collection for Self-Driving Cars Could Be Risking Your Privacy," *Autotrader*, September 2016.

The challenges that connected vehicles and big data pose 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 capability to make driving safer and more efficient. At the same time, digital technology creates new opportunities for invading privacy and using information that could cause harm.

The chapter-opening diagram calls attention to important points this case and this chapter raise. Developments in data management technology, the Internet of Things (IoT), and analytics have created opportunities for organizations to use big data to improve operations and decision making. Big data analytics are now being applied to all the data generated by motor vehicles, especially those with Internet connections. The auto makers and other organizations described here are benefiting from using big data to monitor vehicle performance and driver behavior and to provide drivers with helpful tools for driving safely and caring for their cars. The use of big data from motor vehicles, however, is also taking benefits away from individuals. Individuals might be subject to job discrimination or higher insurance rates because organizations have new tools to assemble and analyze huge quantities of data about



their driving behavior. There are very few privacy protections for all the personal data gathered from car driving. 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 the data generated by connected vehicles 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 from motor vehicles create an ethical dilemma? Why or why not? Should there be new privacy laws to protect personal data collected from cars? Why or why not?

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

In the past 20 years, we have witnessed, arguably, one of the most ethically challenging periods for US 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 global legal environment, managers who violate the law and are convicted will most likely spend time in prison. US federal sentencing guidelines adopted in 1987 mandate that federal judges impose stiff sentences on 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 (US Sentencing Commission, 2004). International treaties and Interpol, enabled by global information systems, have made it possible to extradite, prosecute, arrest, and imprison business managers suspected of criminal activity on a global basis.

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

TABLE 4.1

Recent Examples of Failed Ethical Judgment by Senior Managers

Volkswagen AG (2015)	Installed "defeat-device" emissions software on over 500,000 diesel cars in the United States and roughly 10.5 million more worldwide that allowed them to meet US emissions standards during regulatory testing while actually spewing unlawful levels of pollutants into the air in real-world driving. Criminal charges were brought against six ranking VW executives, including Oliver Schmidt who was sentenced to seven years in prison and $400,000 fine.
Wells Fargo (2018)	Wells Fargo bank admitted to opening millions of false accounts, manipulating terms of mortgages, and forcing auto loan customers to purchase unneeded insurance. The bank was fined $2.5 billion by the federal government.
General Motors, Inc. (2015)	General Motors CEO admitted 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 were affected.
Takata Corporation (2015)	Takata executives admitted they covered up faulty airbags used in millions of cars over many years. Three executives were indicted on criminal charges and Takata was fined $1 billion. Takata filed for bankruptcy in June 2017.

obstructing investigations. More than ever, as a manager or an employee, you will have to decide for yourself what constitutes proper legal and ethical conduct.

These major instances of failed ethical and legal judgment were not masterminded by information systems departments, but 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.

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 free moral agents, use to make choices to guide their behavior. 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, and the telephone, 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 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, 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.

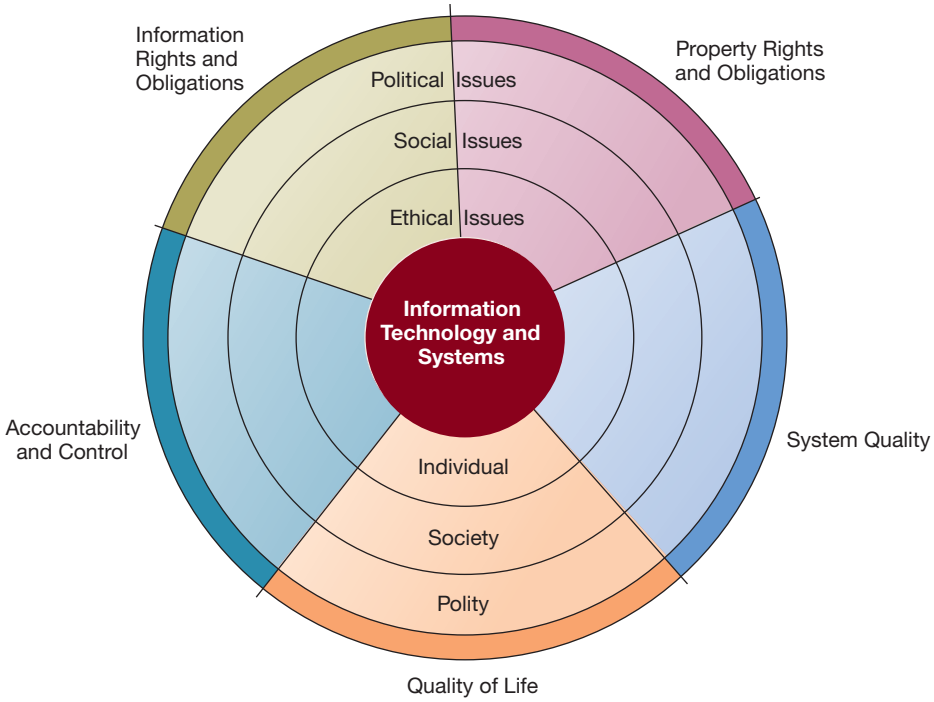


Figure 4.1
The Relationship among Ethical, Social, and Political Issues in an Information Society.
The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

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.

Advances in data storage techniques and rapidly declining storage costs have been responsible for the proliferation of databases on individuals—employees, customers,

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 data accessible from anywhere falls exponentially. Access to data becomes more difficult to control.
Mobile device growth	Individual cell phones may be tracked without user consent or knowledge. The always-on device becomes a tether, and a tracker.

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 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 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 11 describe how companies can analyze large pools of data from multiple sources to identify buying patterns of customers rapidly and make individualized recommendations.

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.

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 Google Marketing Platform (formerly DoubleClick), an Internet advertising broker, to track the activities of their visitors in exchange for revenue from advertisements based on visitor information the Google Platform gathers. The firm uses this information to create a profile of each online visitor, adding more detail to the profile as the visitor accesses an associated Google Platform site. Over time, the Platform 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. Advertisers can combine online consumer information with offline information, such as credit card purchases at stores.

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, Acxiom, Nielsen, Experian, Equifax, and CoreLogic, 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).

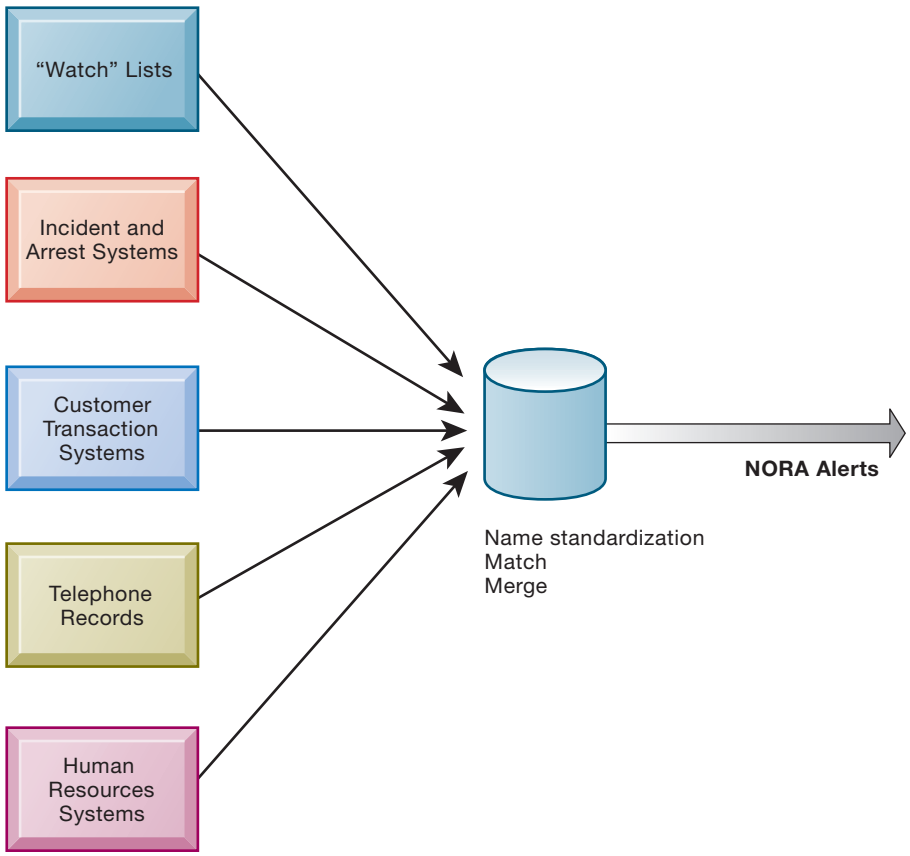


Figure 4.2 Nonobvious Relationship Awareness (NORA). *NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.*

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 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 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, or 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 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 that 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.

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 email 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.

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 Children's Online Privacy Protection Act (COPPA) of 1998 Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999

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 US 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 US 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 and updated in 2010 to take into account new privacy-invading technology (US 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. 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 FIP principles.

The FTC's FIP principles are being used as guidelines to drive changes in privacy legislation. In July 1998, the US 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 advertising networks that collect records of consumer web activity to develop detailed profiles, which other

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.

companies then use to target online ads. The FTC has also 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. 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 from individuals not covered by COPPA; and limiting the use of data mining for homeland security. The FTC has extended its privacy policies to address behavioral targeting, smartphone tracking, the Internet of Things (IoT), and mobile health apps (Federal Trade Commission, 2019; 2015). In 2018 the FTC reached settlements with Venmo, the P2P payment app, Uber, and RealPage to resolve privacy and data security issues in systems operated by these firms.

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 that 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 2018 the European Commission implemented the EU **General Data Protection Regulation (GDPR)**, which is arguably the most important privacy legislation in the last twenty years since the FTC's Fair Information Practices Principles. It applies to

all firms and organizations that collect, store, or process personal information of EU citizens, and these protections apply worldwide regardless of where the processing takes place (European Commission, 2018; Satariano, 2018).

The GDPR is an updated framework for protecting PII (personally identifiable information), and replaces an earlier Data Protection Directive of 1998. In Europe, privacy protection is historically much stronger than it is in the United States. In the United States, there is no federal agency charged with enforcing privacy laws. And there is no single privacy statute governing private corporation use of PII. Instead, privacy laws are piecemeal, sector by sector, for example, medical privacy, educational privacy, and financial privacy laws. These are enforced by the FTC, through self-regulation by businesses, and by individuals who must sue agencies or companies in court to recover damages. This is expensive and rarely done.

In the EU data protection laws are comprehensive, applying to all organizations, and enforced by data protection agencies in each country to pursue complaints brought by citizens and actively enforce privacy laws. The GDPR protects a wide variety of PII: basic identity information such as name, address, and ID numbers; web data such as location, IP address, cookie data, and RFID tags; health and genetic data; mobile phone number; driver's license and passport number; biometric and facial data; racial and ethnic data; political opinions; and sexual orientation.

The main objective of this new framework is to strengthen the rights of citizens to their own personal information and to strengthen oversight of firms to ensure they implement these individual rights. A second thrust was to harmonize conflicting data protection standards among the 28 European block nations and create a single EU agency to implement and enforce the regulation. And third, to enforce these conditions worldwide for all organizations that operate in the EU, or process data pertaining to EU citizens, regardless of where the organization is located.

For individuals, the GDPR requires organizations to allow consumers to access all their personal information without charge within one month; delete personal data (right to be forgotten); ensure data portability so consumers are not locked into a particular service; and guarantee the right to sue providers for damages or abuse of PII, including class action law suits.

Organizational requirements have been strengthened to include requiring organizations to have a data protection officer that reports to senior management; requiring explicit consent before collecting data (positive opt-in), and eliminating default opt-in processes; publishing the rationale for data collection and the length of retention; reporting of breaches and hacks within 72 hours; liability for data they share with partners or other firms, and a listing of all firms they share data with; building privacy protections into all new systems (privacy by design); limit targeting and retargeting of individuals to audience-level, anonymized data, rather than targeting based on intimate, personal profiles; limiting the collection of personal data to only that which is needed to support a task, or a transaction, and then deleting it shortly thereafter. Abuse of PII can be fined up to $20 million or 4% of the organization's global revenue, whichever is greater. Finally, the EU will enforce the GDPR requirements with non-EU countries like the United States using intergovernmental privacy shield agreements that ensure that EU data processed in non-EU nations meets GDPR standards. Privacy shield agreements are a more enforceable version of earlier **safe harbor** agreements. 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 (Lomas, 2018).

The GDPR is clearly aimed at Facebook, Google, Twitter, and other ad-based web businesses that build collections of personal data by tracking individuals across the web, merging that data with other data from firms and data brokers, in order to build comprehensive digital images (profiles) and to target these persons with ads. Google and Facebook are both extremely popular in Europe, and dominate their markets, but at the same time are widely criticized for invading privacy and not protecting PII.

Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. 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 Marketing Platform 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 this 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.

There are now even more subtle and surreptitious tools for surveillance of Internet users. **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 whoever owns the tracking file, which is invisibly embedded in email messages and web pages to monitor the behavior of the user visiting a website or sending email. 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

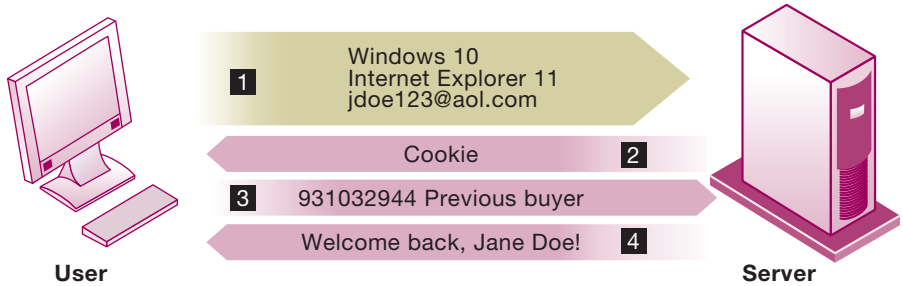


Figure 4.3
How Cookies Identify Web Visitors.
Cookies are written by a website on a visitor's computer. When the visitor returns to that website, the web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The website can then use these data to display personalized information.

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.
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.

on 50 of the most popular US 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% 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, it began using behavioral targeting to help 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 its Marketing Platform, 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 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. Google now displays targeted ads on YouTube and Google mobile applications, and its 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. Members of the advertising network industry, including Google's Marketing Platform, have created an 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 this was changed to opt-in by default because most websites ignored 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 access to 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, 2020). Today, 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.

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 email, for making email 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.

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 that the user's behavior not be tracked, but websites are not obligated to honor these requests. 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 defined as 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 four legal traditions: copyright, patents, trademarks, and trade secrets.

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 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 awarded Apple $1 billion in damages and prohibited Samsung from selling its new Galaxy 10 tablet computer in the United States. 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. Samsung subsequently won a patent infringement case against Apple that banned a handful of older iPhone and iPad devices. In 2014, Apple sued Samsung again, claiming infringement of five patents covering hardware and software techniques for handling photos, videos, and lists used on the Samsung Galaxy 5. In 2015, the US Court of Appeals reaffirmed that Samsung had copied specific design patents, but reduced the damages asked by Apple from $2 billion to $930 million. After seven years of battling in court, the two firms finally settled in 2018 with Apple receiving an estimated $500 million from Samsung.

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.

Trademarks

Trademarks are the marks, symbols, and images used to distinguish products in the marketplace. Trademark laws protect consumers by ensuring they receive what they paid for. These laws also protect the investments that firms have made to bring products to market. Typical trademark infringement violations occur when one firm appropriates or pirates the marks of a competing firm. Infringement also occurs when firms dilute the value of another firm's marks by weakening the connection between a mark and the product. For instance, if a search engine firm copies the trademarked Google icon, colors, and images, it would be infringing on Google's trademarks. It would also be diluting the connection between the Google search service and its trademarks, potentially creating confusion in the marketplace.

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 considered 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.

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 37 percent of the software installed on personal computers was unlicensed in 2018 (The Software Alliance, 2018).

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 US authorities to shut down illegal sharing sites, with mixed results.

As legitimate online music stores such as iTunes and streaming services such as Pandora expanded, illegal file sharing significantly declined. The Apple iTunes Store legitimized 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 inhibit piracy because the streams cannot be easily recorded on separate devices and videos cannot be downloaded so easily. Despite these gains in legitimate online music platforms, artists and record labels have experienced a 50 percent decline in revenues and the loss of thousands of jobs since 2000. By 2019 the music industry generated $10 billion in revenue, equaling its peak revenue in 2010, entirely on the basis of streaming music revenue (RIAA, 2019).

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 it 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 2018 Under Armour, maker of athletic clothing, disclosed that hackers had breached its fitness app called MyFitnessPal and had stolen data from over 150 million user accounts. The data included email addresses, passwords, and usernames, along with other information not disclosed. The firm's stock took a hit of 2% following the announcement and likely caused MyFitnessPal users to lose confidence in the app (Shaban, 2018). Credit card information was not involved, but the app's 2 million users also enter into the app their detailed exercise and diet information. Who is liable for any economic or personal harm caused to individuals or businesses whose personal and business data is stolen from firms with whom they interact, often on a daily basis?

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.

In general, it is 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. However, if the software controls a machine that involves people, the manufacturer of the machine can be held liable for damages, as in the case of the Boeing 737 Max plane where software and sensors malfunctioned, or were poorly designed.

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 airwaves 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

In 2018 many of the largest cloud providers experienced significant outages, taking out sites and services throughout the United States and Europe. Google Cloud experienced an outage that took down entire platforms like Snapchat, Spotify, and Pokemon GO. Amazon Web Services (AWS) experienced an outage that took down Amazon's own Alexa, and several enterprise services such as Atlassian, Slack, and Twilio. Microsoft's Azure service had an outage that effected its storage and networking service in Northern Europe.

Outages at cloud computing services are still infrequent. As more and more firms rely on cloud providers, and centralize their data and operations with a small group of cloud providers, however, the 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 (see the Interactive Session on Technology). The gray area is that some system errors are foreseeable and correctable only at great expense, expense so great that pursuing this level of perfection is not feasible economically—no one could afford the product.

The Boeing 737 MAX Crashes: What Happened and Why?

Shortly after takeoff from Jakarta, Indonesia, on October 29, 2018, Lion Air Flight 610 crashed into the Java Sea. All of the flight's 189 passengers and crew perished. On March 10, 2019 Ethiopian Airlines Flight 302 crashed under similar circumstances, killing all 157 on board. Both flights had used the same aircraft, a Boeing 737 MAX 8, and both accidents had been caused by the same automated system in the 737 MAX designed to prevent the plane from stalling.

Although there are many models of Boeing 737 aircraft, the Maneuvering Characteristics Augmentation System (MCAS) appears only on the Boeing 737 MAX, which was created a decade ago and first took to the air in 2017. MCAS was designed to correct a design flaw in the 737 MAX. Boeing wanted to add a more fuel-efficient airplane to its narrow-body fleet to compete with the Airbus A320neo. This would have taken Boeing years. Instead of designing a completely new plane, Boeing opted to make its existing 737s more fuel-efficient and competitive by adding a more economical but larger engine to the 737 airframe. The new engine was too large to be located midwing as it was on the standard 737, so Boeing positioned the engine higher up the wing. This new engine position could make the plane's nose point upward in midflight, causing the plane to stall and then crash. MCAS was intended to prevent the plane's nose from getting too high.

A sensor outside the airplane automatically activated the MCAS and straightened the airplane whenever it detected the airplane's nose going up. MCAS could activate even when the airplane was not on autopilot—and it could repeat this as many times as it wanted even if pilots overrode it. In the Lion Air crash, the sensor had miscalculated the airplane's nose as pointing upward when it was actually straight. These false readings were passed to the MCAS, which repeatedly tried to straighten the plan by pointing it nose to the ground. Eventually MCAS aimed the airplane's nose to the ground so severely that the pilots could not bring it back up and the plane crashed nose-down into the ocean.

Boeing was so intent on saving time and money with the 737 MAX that safety took a back seat. The company pressured the Federal Aviation Administration (FAA) to allow it to self-certify a large portion of the 737 MAX's development. With little oversight, Boeing focused on improving fuel efficiency as much as possible in record time. According to an FAA official, by 2018 Boeing was allowed to certify 96% of its own work.

The FAA does allow every US airplane manufacturer to self-certify a portion of a new airplane's development. This is because the agency would require an additional 10,000 staff and over $1.8 billion to take on all this work. Boeing was allowed to self-certify the new MCAS software, and Boeing certified that MCAS was safe. The FAA turned nearly complete control over to Boeing, assigning two relatively inexperienced FAA engineers to oversee Boeing's early work on the system. When FAA engineers started looking into the first Boeing 737 MAX crash, they had very little information on the MCAS system and didn't fully understand it. Their files on the aircraft did not contain a complete safety review.

The original version of MCAS relied on data from at least two types of sensors, but Boeing's final version used just one. In both the Lion Air and Ethiopian Air crashes, it was a single damaged sensor that sent the planes into irrecoverable nosedives. According to three FAA officials, Boeing never disclosed this change to MCAS to FAA staff involved in determining pilot training needs. When Boeing asked to remove the description of the system from the pilot's manual, the F.A.A. agreed. Consequently, most MAX pilots did not know about the software until after the first crash. Boeing did not provide 737 MAX test pilots with detailed briefings about how fast or steeply MCAS could push down a plane's nose, and that the system relied on a single sensor—rather than two—to verify the accuracy of incoming data about the angle of a plane's nose.

Regulators had determined that pilots could fly the new 737 MAX airplanes without extensive retraining because they were essentially the same as previous generations, saving Boeing more money. All pilots flying 737 MAX planes were never trained using flight simulators. Instead, Boeing presented two-hour lessons about the new plane using iPads and gave pilots a 13-page handbook explaining differences between the 737 MAX and earlier 737 models. Boeing never trained pilots on the new MCAS software, and many pilots did not know this capability existed. Boeing later claimed it did not want to overload pilots with information, but 737 MAX production was so rushed that a flight simulator was not ready by the time the 737 MAX was completed.

Boeing sold expensive add-on safety features that could have prevented both crashes. The first was two exterior sensors to inform pilots of their angle of attack (how they are flying against the wind). The second was a disagreement alert, which switches on whenever the sensor gives false readings. Both Lion Air and Ethiopian Airlines flew standard 737 MAX models that did not have these safety features because their management thought they could not afford them. (Boeing now includes one of these features in its standard 737 MAX package.)

A day after the Ethiopian crash, China grounded all of its 737 MAX planes. Other nations followed, including Ethiopia, Indonesia, Singapore, the United Kingdom, the European Union, Australia, Malaysia, and Canada. The FAA initially defended the 737 MAX, but finally succumbed to intense pressure to ground the plane. Boeing stopped delivery of all MAX jets to its customers, with unfilled orders worth half a trillion dollars in revenue. The 737 MAX was supposed to be a major moneymaker for Boeing, representing an estimated two-thirds of future deliveries and 40 percent of its annual profit. As of March 2019, Boeing had lost around $28 billion in its stock market value. While regulators await a fix from Boeing, the 737 MAX planes remain grounded, and if the ban persists too long, Boeing may have to halt production. Families of crash victims have filed more than one hundred lawsuits against the company. The future of the 737 MAX and Boeing itself looks very clouded.

Sources: Oliver Taylor, "10 Facts about the Boeing 737 MAX Air Crashes," *ListVerse*, April 8, 2019; Natalie Kitroeff, Daid Gelles, and Jack Nicas, "The Roots of Boeing's 737 MAX Crisis: A Regulator Relaxes Its Oversight," *New York Times*, July 27, 2019; Jack Nicas, Natalie Kitroeff, David Gelles and James Glanz, "Boeing Built Deadly Assumptions into 737 Max, Blind to a Late Design Change," *New York Times,* June 1, 2019; Andrew Tangel and Andy Pasztor, "Boeing's Own Test Pilots Lacked Key Details of 737 MAX Flight-Control System," *Wall Street Journal,* May 3, 2019; Robert Wall and Andrew Tangel, "Safety Fears Put Boeing on the Defensive," *Wall Street Journal*, March 11, 2019; Andrew J. Hawkins, "Everything You Need to Know about the Boeing 737 MAX Airplane Crashes," *The Verge*, March 22, 2019; and Zach Wichter, "The Boeing Crashes: A Brief Guide to What Happened," *New York Times*, March 22, 2019.

CASE STUDY QUESTIONS

1. What is the problem described in this case? Would you consider it an ethical dilemma? Why or why not?
2. Describe the role of people, organization, and technology factors in the Boeing 737 MAX safety problems. To what extent was management responsible?
3. Is the solution provided by Boeing adequate? Explain your answer.
4. What steps could Boeing and the FAA have taken to prevent this problem from occurring?

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 human errors or natural events, and (3) poor input data quality. The 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 (see Chapter 6). Few companies routinely measure the quality of their data, but individual organizations report data error rates ranging from 0.5 to 30%.

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, whom 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.

Big Tech: Concentrating Economic and Political Power

In 2019 Amazon accounted for over half of all e-commerce retail sales, along with 75 percent of all book sales. Google accounts for 87 percent of online search. Facebook (including Instagram) accounts for over 86 percent of all social network users, and has 60 percent of the total Internet audience. Ninety percent of new online ad dollars went to Google or Facebook. Seventy-five percent of video streamers use Netflix, 53 percent use YouTube, and 33 percent use Amazon. In the office, Microsoft dominates with over 90 percent of the world's 2 billion PCs using Windows software and software products. Apple accounts for 48 percent of the US market in smartphones (Google accounts for the remaining 52 percent). The millions of Apple apps run only on Apple phones, likewise for Android apps running only on Android phones. In the new world of these so-called Big Tech firms, oligopolies and monopolies dominate the Web and mobile platforms. The wealth created by these firms inevitably translates into political influence: these same firms have amassed an army of lobbyists in Washington and state capitals to ensure legislation, or legislative inquiries, that might affect their market and tax concerns, reflects their interests. Big Tech firms have increased their lobbying efforts in Washington to over $30 billion annually, second only to financial firm lobbying (Lohr, Isaac, and Popper, 2019).

Concentrations of market power are not new in the United States or Europe. Beginning in 1890 with the Sherman Antitrust Act in the United States, and continuing through the 1960s, monopolies have been considered threats to competition and to smaller start-up businesses, generally restraining free trade. Monopolies typically achieve their size by purchasing smaller competitors, or crushing them by developing similar products, or engaging in predatory pricing by dropping prices drastically for short periods of time to force smaller firms out of business. Big Tech firms have a well-documented history of these behaviors. But antitrust thinking changed in the 1970s to a different standard of harm: consumer welfare. In this view, bigness per se was not a danger, or even anticompetitive behavior. Instead price and consumer welfare became paramount. As long as consumers were not forced to pay higher prices, then market power was not important, not a social or economic harm. In this view, because the offerings of Facebook, Google, and Amazon are either free or very low cost, there can be no harm.

Critics point out that consumer welfare is harmed in other ways than price, namely, by preventing new, innovative companies from market access, or surviving long enough to prosper as independent firms. Complaints and law suits originated by small start-up firms alleging anticompetitive and unfair practices, and concerns about the abuse of personal privacy by Big Tech firms, have led to a torrent of critical articles and several congressional investigations. Heretofore the poster children of American capitalism at its best, Big Tech firms are today the targets of stinging public criticism, legislative investigations, and regulatory actions. Many commentators are calling for breaking up Big Tech firms into separate businesses much as the Sherman Antitrust act broke up Standard Oil in 1911, as well as other monopolies in photography, tobacco, steel, railroads, meat packing, telecommunications, and computers (Kang, Streitfeld, and Karni, 2019).

Rapidity of Change: Reduced Response Time to Competition

Information systems have helped to create much more efficient national and international markets. Today's rapid-moving 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

The danger of 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 writers 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 face-to-face relationships with their families and friends. Among middle school and teenage children, it can lead to harmful antisocial 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, 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. Think of what would happen if the nation's electric power grid shut down, with no backup structure to 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

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.

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. 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, email, and mobile phones has turned one form of computer abuse—spamming—into a serious problem for both individuals and businesses. Originally, **spam** was junk email an organization or individual sent to a mass audience of Internet users who had expressed no interest in the product or service being marketed. 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 email 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 email that is spam was estimated at around 55 percent in 2018 (Symantec, 2019). Most spam originates from bot networks, which consist of thousands of captured PCs that can initiate and relay spam messages. Spam costs for businesses are very high (estimated at more than $50 billion per year) because of the computing and network resources and the time required to deal with billions of unwanted email messages.

Identity and financial-theft cybercriminals are targeting smartphones as users check email, 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 News feed and messaging service as well.

ISPs and individuals can combat spam by using spam filtering software to block suspicious email before it enters a recipient's email inbox. However, spam filters may block legitimate messages. Spammers know how to skirt filters by continually changing their email accounts, by incorporating spam messages in images, by embedding spam in email 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. Australia, South Africa, the European Union, Sweden, and Malaysia are among the countries that have anti-spam laws.

The US CAN-SPAM Act of 2003, which went into effect in 2004, does not outlaw spamming but does ban deceptive email practices by requiring commercial email messages to display accurate subject lines, identify the true senders, and offer recipients an easy way to remove their names from email lists. It also prohibits the use of fake return addresses. The law has had a negligible impact on spamming, in large part because of 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. One of the largest spam networks 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.

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 has caused millions of mid-level factory managers and clerical workers to lose their jobs. Some economists have sounded new alarms about information and computer technology threatening middle-class, white-collar jobs (in addition to blue-collar factory jobs). Erik Brynjolfsson and Andrew P. McAfee argue that the pace of automation has picked up in recent years because of a combination of technologies, including robotics, numerically controlled machines, computerized inventory control, pattern recognition, voice recognition, and online commerce. One result is that machines can now do a great many jobs heretofore reserved for humans, including tech support, call center work, X-ray examination, and even legal document review (Brynjolfsson and McAfee, 2011).

These views contrast with other economists' assessments that new technologies created as many or more new jobs than they destroyed. In some cases, employment has grown or remained unchanged in industries like finance, where investment in IT capital is highest. For instance, the growth of e-commerce has led to a decline in retail sales jobs but an increase in jobs for warehouse workers, supervisors, and delivery work. These economists also believe that bright, educated workers who are displaced by technology will move 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. The Chapter 1 Interactive Session on People explores this issue.

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 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 low-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 in computer access is narrowing, higher-income families in each ethnic group are still more likely to have home computers and broadband Internet access than lower-income families in the same group. Moreover, the children of higher-income families are far more likely to use their Internet access to pursue educational goals, whereas lower-income children are much more likely to spend time on entertainment and games. This is called the "time-wasting" gap.

Left uncorrected, this **digital divide** could lead to a society of information haves, who are computer literate and skilled, versus a large group of information have-nots, who are 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 COGNITIVE DECLINE

A 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 incidence of RSI is estimated to affect as much as one-third of the labor force and accounts for one-third of all disability cases.

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 CTS include numbness, shooting pain, inability to grasp objects, and tingling. Millions of workers have been diagnosed with CTS. It affects an estimated 3 to 6 percent of the workforce (LeBlanc and Cestia, 2011).

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 handheld video games. CVS affects about 90 percent of people who spend three hours or more per day at a computer. Its symptoms, which are usually temporary, include headaches, blurred vision, and dry and irritated eyes.

In addition to these maladies, computer technology may be harming our cognitive functions or at least changing how we think and solve problems. 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 on their own. They argue that excessive use of computers (and smartphones—see the Interactive Session on People) reduces intelligence. One MIT scholar believes exposure to computers encourages looking up answers rather than engaging in real problem solving. Students, in this view, don't learn much surfing the web or answering email when compared to listening, drawing, arguing, looking, and exploring (Henry, 2011).

The computer has become 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 further into the first digital century.

© Ian Allenden/123RF

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

How Harmful Are Smartphones?

For many of us, smartphones have become indispensable, but they have also come under fire for their impact on the way we think and behave, especially among children. There is a growing wariness among parents, educators, psychologists, and even Silicon Valley luminaries that the benefits of screens are overblown, even as learning tools, and the risks for addiction and stunting development seem high.

The average American teenager who uses a smartphone receives his or her first phone at age 10 and spends over 4.5 hours a day on it (excluding texting and talking). Seventy-eight percent of teens check their phones at least hourly, and 50 percent report feeling "addicted" to their phones. A number of studies have pointed out the negative effects of heavy smartphone and social media use on the mental and physical health of children whose brains are still developing. These range from distractions in the classroom to a higher risk of suicide and depression.

A recent survey of over 2,300 teachers by the Center on Media and Child Health and the University of Alberta found that 67 percent of the teachers reported that the number of students who are negatively distracted by digital technologies in the classroom is growing. Seventy-five percent of these teachers think students' ability to focus on educational tasks has decreased. Research by psychology professor Jean Twenge of San Diego State University found that US teenagers who spend 3 hours a day or more on electronic devices are 35 percent more likely, and those who spend 5 hours or more are 71 percent more likely, to have a risk factor for suicide than those who spend less than 1 hour. This research also showed that eighth-graders who are heavy users of social media have a 27 percent higher risk of depression. Those who spend more than the average time playing sports, hanging out with friends in person, or doing homework have a significantly lower risk. Additionally, teens who spend 5 or more hours a day on electronic devices are 51 percent more likely to get less than 7 hours of sleep per night (versus the recommended 9).

Nicholas Carr, who has studied the impact of technology on business and culture, shares these concerns. He has been highly critical of the Internet's effect on cognition, and these cognitive effects extend to smartphone use. Carr worries that excessive use of mobile devices diminishes the capacity for concentration and contemplation.

Carr recognizes that smartphones provide many useful functions in a handy form. This extraordinary usefulness, however, gives them too much influence on our attention, thinking, and behavior. Smartphones shape our thoughts in deep and complicated ways, and their effects persist even when we aren't using the devices. Research suggests that the intellect weakens as the brain grows dependent on the technology.

Carr points to the work of Adrian Ward, a cognitive psychologist and marketing professor at the University of Texas at Austin, who for a decade has been studying how smartphones and the Internet affect people's thoughts and judgment. Ward has observed that using a smartphone, or even hearing one ring or vibrate, produces distractions that make it harder to concentrate on a difficult problem or job. Divided attention impedes reasoning and performance.

A study published in Applied Cognitive Psychology in April 2017 examined how smartphones affected learning in a lecture class with 160 students at the University of Arkansas at Monticello. It found that students who didn't bring their phones to the classroom scored a full letter-grade higher on a test of the material presented than those who brought their phones. It didn't matter whether students who brought their phones used them or not. A study of 91 UK secondary schools, published in 2016 in the journal *Labour Economics*, found that when schools ban smartphones, students' examination scores go up substantially, and the weakest students benefit the most.

Carr also observes that using smartphones extensively can be detrimental to social skills and relationships. Connecting with "friends" electronically via smartphones is not a substitute for genuine person-to-person relationships and face-to-face conversations.

In early 2018 two of the largest investors in Apple called for the iPhone maker to take more action against smartphone addiction among children .The investors urged Apple to offer more tools to prevent smartphone addiction and to provide more parental options for monitoring children's smartphone usage. The iOS operating system for Apple smartphones and tablets already has limited parental controls for restricting apps, features such as location sharing, and access to certain types of content. The investors felt Apple needed to do

more—for example, enable parents to specify the age of the user of the phone during setup, establish limits on screen time, select hours of the day the phone can be used, and block social media services.

Apple created its own screen-time tracker to help parents limit the time they and their children spent on iPhones. But Apple also has removed or restricted at least 11 of the 17 most downloaded screen-time and parental-control apps, according to an analysis by the *New York Times* and Sensor Tower, an app-data firm. Apple has also removed some lesser-known apps. In some cases, Apple forced companies to remove features that allowed parents to control their children's devices or that blocked children's access to certain apps and adult content. In other cases, it simply pulled the apps from its App Store.

Sources: Jack Nicas, "Apple Cracks Down on Apps that Fight iPhone Addiction," *New York Times*, April 27, 2019; Nellie Bowles, "Human Contact Is Now a Luxury Good," *New York Times*, March 23, 2019, and "A Dark Consensus about Screens and Kids Begins to Emerge in Silicon Valley," *New York Times*, October 26, 2018; Samuel Gibbs, "Apple Investors Call for Action over iPhone 'Addiction' among Children," *The Guardian*, January 8, 2018; David Benoit, "iPhones and Children Are a Toxic Pair, Say Two Big Apple Investors," *Wall Street Journal*, January 7, 2018; and Nicholas Carr, "How Smartphones Hijack Our Minds," *Wall Street Journal*, October 7, 2017.

CASE STUDY QUESTIONS

1. Identify the problem described in this case study. In what sense is it an ethical dilemma?
2. Should restrictions be placed on children's and teenagers' smartphone use? Why or why not?
3. Can the problem of smartphones reducing cognitive skills be solved? Why or why not? Explain your answer.

4-5 How will MIS help my career?

Here is how Chapter 4 and this book can help you find a job as a junior privacy analyst.

THE COMPANY

Pinnacle Air Force Base in Sweden has an open entry-level position for a junior privacy analyst in its human resources office. The office maintains detailed personnel records, including work history, compensation, healthcare, and retirement benefits, on more than 6,800 military members and their families and 1,250 civilian employees.

POSITION DESCRIPTION

The junior privacy analyst will assist with employee recordkeeping and help ensure compliance with all federal and state privacy regulations. Job responsibilities include:

- Analyzing and developing policy and procedures related to privacy office functions.
- Logging and tracking Privacy Act requests, assistance with review, redaction and preparation of responsive records, and tracking all privacy office correspondence.
- Monitoring and responding to written, verbal, and electronic correspondence and inquiries directed to the government privacy office, including sensitive beneficiary/personnel correspondence.
- Coordinating privacy office meetings.
- Reviewing and analyzing data and documents and assessing options, issues, and positions for a variety of program planning, reporting, and execution activities.

JOB REQUIREMENTS

- Bachelor's degree in liberal arts or business
- Strong communication and organizational skills
- Experience with recordkeeping and file systems desirable

INTERVIEW QUESTIONS

1. What background or job experience do you have in the privacy protection field?
2. What do you know about the Privacy Act?
3. What do you know about privacy protection practices for both written and electronic correspondence?
4. If you were asked to improve privacy protection for our organization, how would you proceed?
5. Have you ever dealt with a problem involving privacy protection? What role did you play in its solution?

AUTHOR TIPS

1. Review this chapter, with special attention to the sections dealing with information systems and privacy.
2. Use the web to find out more about the Privacy Act and privacy protection procedures and policies for personnel records.
3. Try to find out more about employee recordkeeping and privacy protection at US military bases or other organizations.
4. If you do not have any hands-on experience in the privacy area, explain what you do know about privacy and why it is so important to protect sensitive personal data, and indicate you would be very interested in learning more and doing privacy-related work.

Review Summary

4-1 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 information systems raise center on information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life.

4-2 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, the slippery slope rule, 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.

4-3 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 enable companies to gather personal data from many sources easily about individuals and analyze these data to create detailed digital 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 website visitors. Not all websites 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 locations simultaneously over the Internet.

4-4 How have information systems affected laws for establishing accountability and liability and the quality of everyday life? New information technologies are challenging existing liability laws and social practices for holding individuals and institutions accountable for harm done to others. 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 ethnic groups and social classes. Widespread use of computers increases opportunities for computer crime and computer abuse. Computers can also create health and cognitive problems such as repetitive stress injury, computer vision syndrome, and the inability to think clearly and perform complex tasks.

Key Terms

Accountability, 148
Carpal tunnel syndrome (CTS), 167
Computer abuse, 165
Computer crime, 165
Computer vision syndrome (CVS), 167
Cookies, 154
Copyright, 156
Digital divide, 166
Digital Millennium Copyright Act (DMCA), 159
Due process, 148
Ethical no-free-lunch rule, 149
Ethics, 144
Fair Information Practices (FIP), 151
General Data Protection Regulation (GDPR), 152
Golden Rule, 149
Immanuel Kant's categorical imperative, 149
Information rights, 145
Informed consent, 155
Intellectual property, 156
Liability, 148
Nonobvious relationship awareness (NORA), 147
Opt-in, 155
Opt-out, 155
Patent, 157
Privacy, 150
Profiling, 147
Repetitive stress injury (RSI), 166
Responsibility, 148
Risk aversion principle, 149
Safe harbor, 153
Slippery slope rule, 149
Spam, 165
Spyware, 155
Trade secret, 158
Trademarks, 158
Utilitarian principle, 149
Web beacons, 154

Review Questions

4-1 What ethical, social, and political issues are raised by information systems?
- Explain what nonobvious relationship awareness is.
- Describe the net impact of the doubling of computer power every eighteen months.
- List some of the ethical issues in information systems that have been given new urgency by the rise of the Internet and electronic commerce.

4-2 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.

4-3 Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?
- Explain the purpose and the significance of GDPR in its current form.
- Distinguish between opt-in and opt-out with respect to data collection online.
- Explain the value of a patent and how it protects the intellectual property of an individual or organization.
- List and define the three regimes that protect intellectual property rights.

4-4 How have information systems affected laws for establishing accountability and liability and the quality of everyday life?
- Identify the most common reason for business system failure.

- Describe why all organizations have become dependent and vulnerable as a result of using information systems.
- Describe computer crime using an example.
- Explain what is meant by the term digital divide.

MyLab MIS™
To complete the problems with **MyLab MIS**, go to the EOC Discussion Questions in MyLab MIS.

Discussion Questions

4-5 MyLab MIS Should producers of software-based services, such as ATMs, be held liable for economic injuries suffered when their systems fail?

4-6 MyLab MIS Should companies be responsible for unemployment their information systems cause? Why or why not?

4-7 MyLab MIS Discuss the pros and cons of allowing companies to amass personal data for behavioral targeting.

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 analyzing web browser privacy. Visit MyLab MIS to access this chapter's Hands-On MIS Projects.

MANAGEMENT DECISION PROBLEMS

4-8 FashionToday is an online fashion shop catering to Belgium, the Netherlands, and Luxembourg. They keep track of each customer's email address, home address, age, gender, clothing preferences, and body-size measurements. Yara is a young woman who struggles to find things her size but is a regular shopper at FashionToday. One day, she receives a text message announcing a new line of clothes named FTXL. Clearly, she has been selected based on her submitted body size measurements. Five days later, she receives an ad for weight-loss supplements from Herbs4Life, an affiliate of FashionToday. Has FashionToday violated Yara's privacy? Is this potentially offensive to people like Yara? Explain your answer.

4-9 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 workload to warrant working longer hours and are looking into the amount of time they spend on the Internet.

Each employee uses a computer with Internet access on the job. Review a sample of your company's weekly report of employee web usage, which can be found in MyLab MIS.

- 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

4-10 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 computer, or the web, to your blog. 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 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: ANALYZING WEB BROWSER PRIVACY

Software skills: Web browser software
Business skills: Analyzing web browser privacy protection features

4-11 This project will help develop your Internet skills for using the privacy protection features of leading web browser software.

Examine the privacy protection features and settings for two leading web browsers such as Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome. Make a table comparing the features of two of these browsers in terms of functions provided and ease of use.

- How do these privacy protection features protect individuals?
- How do these privacy protection features affect what businesses can do on the Internet?
- Which browser does the best job of protecting privacy? Why?

COLLABORATION AND TEAMWORK PROJECT

Developing a Corporate Code of Ethics

4-12 With three or four of your classmates, develop a corporate ethics code on privacy that addresses both employee privacy and the privacy of customers and users of the corporate website. Be sure to consider email 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 Docs and Google Drive or Google Sites to brainstorm, organize, and develop a presentation of your findings for the class.

BUSINESS PROBLEM SOLVING CASE

FACEBOOK PRIVACY: YOUR LIFE FOR SALE

Facebook describes its corporate mission as giving people the power to build community and bring the world closer together. In 2017 and 2018 these lofty objectives took a serious blow when it became known that Facebook had lost control of the personal information users share on the site. Facebook had allowed its platform to be exploited by Russian intelligence and political consultants with the intention of intensifying existing political cleavages, driving people away from community and from one another during the US presidential election of 2016.

In January 2018, a founder and former employee of a political consulting and voter profiling company called Cambridge Analytica revealed that his firm had harvested the personal information of as many as 87 million users of Facebook, and used this information in an effort to influence the US presidential election of 2016. Facebook does not sell the personal information of its users, but it did allow third-party apps to obtain the personal information of Facebook users. In this case, a UK researcher was granted access to 50,000 Facebook users for the purpose of research. He developed an app quiz that claimed to measure users' personality traits. Facebook's design allowed this app to not only collect the personal information of people who agreed to take the survey, but also the personal information of all the people in those users' Facebook social networks. The researcher sold the data to Cambridge Analytica, who in turn used it to send targeted political ads in the presidential election.

In a Senate hearing in October 2017, Facebook testified that Russian operatives had exploited Facebook's social network in an effort to influence the 2016 presidential election. More than 130,000 fake messages and stories had been sent to Facebook users in the United States using an army of automated software bots, built and operated by several thousand Russian-based hackers working for a Russian intelligence agency, the Internet Research Agency. (A bot is a software program that performs an automated task, and is often on the Internet for malicious purposes—see Chapter 8.) Using 75,000 fake Facebook accounts, and 230,000 bots, the Russian messages were sent to an estimated 146 million people on Facebook. The messages targeted people based on their personal information collected by Facebook in the normal course of business, including users' religion, race, ethnicity, personal interests, and political views. The ads targeted groups who had opposing political views, with the intention of intensifying social conflict among them.

How could all this happen? As it turns out, it was quite easy and inexpensive, given the design and management of Facebook. Once Facebook grants access to advertisers, app developers, or researchers, it has a very limited capability to control how that information is used. Third-party agreements and policies are rarely reviewed by Facebook to check for compliance. Facebook executives claimed they were as shocked as others that 87 million Facebook users had their personal information harvested by Russian intelligence agencies and used by Cambridge Analytica to target political ads.

It gets worse: In early June 2018, several months after Facebook was forced to explain its privacy measures and pledge reforms in the wake of the Cambridge Analytica scandal, the *New York Times* reported that Facebook had data-sharing partnerships with at least 60 device makers, as well as selected app developers. Facebook allowed Apple, Samsung, Amazon, and other companies that sell mobile phones, tablets, TVs, and video game consoles to gain access not only to data about Facebook users but also personal data about their friends—without their explicit consent. All of these practices were in violation of a 2012 privacy settlement with the FTC (Federal Trade Commission) in which Facebook agreed to stop deceiving users about their ability to control their personal data, and to stop sharing data with third parties without informing users.

Facebook did not in fact change its behavior and instead deceived its users by claiming it could control their privacy. Senior managers at Facebook, including founder and CEO Mark Zuckerberg, were apparently aware of this deception according to company emails. In 2019 Facebook's privacy issues finally resulted in a record-breaking $5 billion dollar fine by the FTC for obviously and intentionally violating the 2012 settlement. Facebook also agreed to new oversight by regulators in privacy matters, and to develop new practices and policies for handling personal information. While $5 billion is a large sum of money, for a company with $56 billion

in annual revenue, the fine may not be enough to change its actual behavior. The fine was, in the words of critics, barely a dent in Facebook's revenue. There are no specific restrictions on its mass surveillance of users, and the new privacy policies will be created by Facebook not the FTC. The settlement also provided immunity to Facebook executives and directors from any personal liability for the past violations of the 2012 settlement, and of users' privacy, and shielded the company from any claims of past violations. In other words, the past was wiped clean.

Facebook has a diverse array of compelling and useful features. It has helped families find lost pets and allows active-duty soldiers to stay in touch with their families; and it gives smaller companies a chance to further their e-commerce efforts and larger companies a chance to solidify their brands. Pserhaps most obviously, Facebook makes it easier for you to keep in touch with your friends, relatives, local restaurants, and, in short, just about all the things you are interested in. These are the reasons so many people use Facebook—it provides real value to users. But at a cost. The cost of participating in the Facebook platform is that your personal information is shared with advertisers and with others you may not know.

Facebook's checkered past of privacy violations and missteps raises doubts about whether it should be trusted with the personal data of billions of people. Unlike European nations, there are no laws in the United States that give consumers the right to know what data companies like Facebook have compiled. You can challenge information in credit reports because of the Fair Credit Reporting Act, but until recently, you could not obtain what data Facebook has gathered about you.

Think you own your face? Not on Facebook, thanks to the firm's facial recognition software for photo tagging of users. This "tag suggestions" feature is automatically on when you sign up, and there is no user consent. A federal court in 2016 allowed a lawsuit to go forward contesting Facebook's right to photo tag without user consent. This feature is in violation of several state laws that seek to secure the privacy of biometric data.

A *Consumer Reports* study found that among 150 million Americans on Facebook every day, at least 4.8 million were willingly sharing information that could be used against them in some way. That includes plans to travel on a particular day, which burglars could use to time robberies, or Liking a page about a particular health condition or treatment, which might prompt insurers to deny coverage. Credit card companies and similar organizations have begun engaging in weblining, taken from the term *redlining*, by altering their treatment of you based on the actions of other people with profiles similar to yours. Employers can assess your personality and behavior by using your Facebook Likes. Millions of Facebook users have never adjusted Facebook's privacy controls, which allow friends using Facebook applications to transfer your data unwittingly to a third party without your knowledge.

Why, then, do so many people share sensitive details of their life on Facebook? Often, it's because users do not realize that their data are being collected and transmitted in this way. A Facebook user's friends are not notified if information about them is collected by that user's applications. Many of Facebook's features and services are enabled by default when they are launched without notifying users, and a study by Siegel+Gale found that Facebook's privacy policy is more difficult to comprehend than government notices or typical bank credit card agreements, which are notoriously dense. Did you know that whenever you log into a website using Facebook, Facebook shares some personal information with that site and can track your movements on that site? Next time you visit Facebook, click Privacy Settings and see whether you can understand your options.

There are some signs, however, that Facebook might become more responsible with its data collection processes, whether by its own volition or because it is forced to do so. As a publicly traded company, Facebook now invites more scrutiny from investors and regulators. In 2018, in response to a maelstrom of criticism in the United States, and Europe's new General Data Protection Regulation (GDPR), Facebook changed its privacy policy to make it easier for users to select their privacy preferences; to know exactly what they are consenting to; to download users' personal archives and the information that Facebook collects and shares, including facial images; to restrict click bait and spam in newsfeeds; to more closely monitor app developers' use of personal information; and to increase efforts to eliminate millions of fake accounts. Facebook hired 10,000 new employees and several hundred fact-checking firms to identify and eliminate fake news. For the first time in its history, Facebook is being forced to apply editorial controls to the content posted by users and, in that sense, become more like a traditional publisher

and news outlet that takes responsibility for its content. Unfortunately, as researchers have long known, and Facebook executives understand, very few users—estimated to be less than 12 percent—take the time to understand and adjust their privacy preferences. In reality, user choice is not a powerful check on Facebook's use of personal information.

Although US Facebook users have little recourse to access data that Facebook has collected on them, users from other countries have done better. In Europe, over 100,000 Facebook users have already requested their data, and European law requires Facebook to respond to these requests within 40 days. Government privacy regulators from France, Spain, Italy, Germany, Belgium, and the Netherlands have been actively investigating Facebook's privacy controls as the European Union pursues more stringent privacy protection legislation.

While Facebook has shut down several of its more egregious privacy-invading features, and enhanced its consent process, the company's data use policies make it very clear that, as a condition of using the service, users grant the company wide latitude in using their personal information in advertising. The default option for users is "opt-in"; most users do not know how to control use of their information; and they cannot "opt out" of all sharing if they want to use Facebook. This is called the "control paradox" by researchers: even when users are given controls over the use of their personal information, they typically choose not to use those controls. Although users can limit some uses of their information, extensive knowledge of Facebook data features is required. Facebook shows you ads not only on Facebook but across the web through its Facebook Audience Network, which keeps track of what its users do on other websites and then targets ads to those users on those websites.

Critics have asked Facebook why it doesn't offer an ad-free service—like music streaming sites—for a monthly fee. Others want to know why Facebook does not allow users just to opt out of tracking. But these kinds of changes would be very difficult for Facebook because its business model depends entirely on the largely unfettered use of its users' personal private information, just as it declares in its data use policy. That policy states openly that if you use Facebook you agree to their terms of service, which enable it to share your information with third parties of their choosing. As Apple CEO Tim Cook noted, at Facebook, the product they sell is you.

Sources: Mike Isaac and Natasha Singer, "On Wednesday, the Federal Trade Commission Placed New Conditions on Facebook for Privacy Violations," *New York Times*, July 24, 2019; "A $5 Billion Fine for Facebook Won't Fix Privacy," *New York Times*, July 25, 2019; Devin Coldewey and Natasha Lomas, "Facebook Settles with FTC: $5 Billion and New Privacy Guarantees," *Techcrunch*, July 24, 2019; John D. McKinnon, Emily Glazer, Deepa Seetharaman, and Jeff Horwitz, "Facebook Worries Emails Could Show Zuckerberg Knew of Questionable Privacy Practices," *New York Times*, June 12, 2019; Federal Trade Commission, "In the Matter of Facebook, a Corporation," FTC, July 24, 2019; Deepa Seetharaman and Kirsten Grind, "Facebook Gave Some Companies Access to Additional Data About Users' Friends," *Wall Street Journal,* June 8, 2018; Cecilia Kang and Sheera Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users," *New York Times*, April 24, 2018; Eduardo Porter, "The Facebook Fallacy: Privacy Is Up to You," *New York Times*, April 24, 2018; David Mayer, "Facebook Is Giving You New Privacy Options, But It's Clear What It Wants You to Choose," *Fortune*, March 19, 2018; Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, March 17, 2018; Georgia Wells and Deepa Seetharaman, "New Facebook Data Shows Russians Targeted Users by Education, Religion, Politics," *Wall Street Journal*, November 1, 2017; Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, March 2017.

CASE STUDY QUESTIONS

4-13 Perform an ethical analysis of Facebook. What is the ethical dilemma presented by this case?

4-14 What is the relationship of privacy to Facebook's business model?

4-15 Describe the weaknesses of Facebook's privacy policies and features. What people, organization, and technology factors have contributed to those weaknesses?

4-16 Will Facebook be able to have a successful business model without invading privacy? Explain your answer. Could Facebook take any measures to make this possible?

Chapter 4 References

Adjerid, Idris, Eyal Peer, and Alessandro Acquisti. "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making." *MIS Quarterly* 42, No. 2 (June 2018).

Anderson, Chad, Richard L. Baskerville, and Mala Kaul. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information." *Journal of Management Information Systems* 34, No. 4 (2017).

Bilski v. Kappos, 561 US (2010).

Brown Bag Software vs. Symantec Corp. 960 F2D 1465 (Ninth Circuit, 1992).

Brynjolfsson, Erik, and Andrew McAfee. *Race Against the Machine* (Digital Frontier Press, 2011).

Culnan, Mary J., and Cynthia Clark Williams. "How Ethics Can Enhance Organizational Privacy." *MIS Quarterly* 33, No. 4 (December 2009).

Davenport, Thomas H., and Julia Kirby. "Beyond Automation." *Harvard Business Review* (June 2015).

European Commission. "2018 Reform of EU Data Protection Rules," https://ec.europa.eu (2018).

European Commission. "The EU-U.S. Privacy Shield Factsheet." July 2016. http://ec.europa.eu, accessed June 15, 2017.

European Parliament. "Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009." European Parliament (2009).

Federal Trade Commission. "FTC Releases 2018 Privacy and Data Security Update" (March 2019)

———. "Internet of Things (IoT): Privacy & Security in a Connected World" (January 2015).

Gopal, Ram D., Hooman Hidaji, Raymond A. Patterson, Erik Rolland, and Dmitry Zhdanov. "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas." *MIS Quarterly* 42, No. 1 (March 2018).

Henry, Patrick. "Why Computers Make Us Stupid." *Slice of MIT* (March 6, 2011).

Kang, Cecelia, David Streitfeld and Annie Karni. "Antitrust Troubles Snowball for Tech Giants as Lawmakers Join In." *New York Times* (June 3, 2019).

Kang, Cecelia, and Kenneth P. Vogel. "Tech Giants Amass a Lobbying Army for an Epic Washington Battle." *New York Times* (June 5, 2019).

Laudon, Kenneth C. *Dossier Society: Value Choices in the Design of National Information Systems*. (New York: Columbia University Press, 1986).

Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce: Business, Technology, Society*, 15th ed. (Upper Saddle River, NJ: Prentice-Hall, 2020).

LeBlanc, K. E., and W. Cestia. "Carpal Tunnel Syndrome." *American Family Physician* 83, No. 8 (2011).

Lohr, Steve, Mike Isaac, and Nathaniel Popper. "Tech Hearings: Congress Unites to Take Aim at Amazon, Apple, Facebook and Google." *New York Times* (July 16, 2019).

Lomas, Natasha. "EU Parliament Calls for Privacy Shield to Be Pulled Until US Complies." *TechCrunch* (July 5, 2018).

Manyika, James, and Michael Spence. "The False Choice Between Automation and Jobs." *Harvard Business Review* (February 5, 2018).

Pew Research Center. "The State of Privacy in America" (January 20, 2016).

RIAA. "2018 RIAA Shipment & Revenue Statistics" RIAA (May 2019).

Satariano, Adam. "The European Union on Friday Enacts the World's Toughest Rules to Protect People's Online Data." *New York Times* (May 24, 2018).

Shaban, Hamza, "Under Armour Announces Data Breach, Affecting 150 Million Myfitnesspal App Accounts." *Washington Post* (March 29, 2018).

The Software Alliance. "BSA Global Software Survey 2018" (June 2018).

Symantec. "2019 Internet Security Threat Report" (2019).

US Department of Health, Education, and Welfare. *Records, Computers, and the Rights of Citizens* Cambridge, MA: MIT Press (1973).

US Senate. "Do-Not-Track Online Act of 2011." Senate 913 (May 9, 2011).

US Sentencing Commission. "Sentencing Commission Toughens Requirements for Corporate Compliance Programs" (April 13, 2004).

Wolcott, Robert C. "How Automation Will Change Work, Purpose, and Meaning." *Harvard Business Review* (January 11, 2018).