Ethics and Privacy

CHAPTER OUTLINE	LEARNING OBJECTIVES
3.1 Ethical Issues	**3.1** Define ethics and explain its three fundamental tenets and the four categories of ethical issues related to information technology.
3.2 Privacy	**3.2** Discuss at least one potential threat to the privacy of the data stored in each of three places that store personal data.

Opening Case

Case 3.1 The Huge Scope of Privacy Issues: All Data Are Accessible

Did you realize that when you use an Internet app, the app could also have access to your data? Other risks, discussed in our next chapter, also expose data, such as the actions of a dishonest employee. Here, we look at some examples of private or confidential data recently exposed.

Desjardins Group

In June 2019, Desjardins Group disclosed that one of its employees had taken unauthorized copies of data from close to 3 million of its consumer and business customers and shared those data with others. The Group sells personal and business insurance, and is a financial cooperative, providing savings plans, loans, registered retirement savings plans, and other financial services and instruments. Desjardins was proactive about the leak, calling in the Laval, Quebec police force to investigate the extent of the data exposure and to help determine how it had happened. Once the cause of the breach had been located and stopped, the financial organization informed the public, providing a one-year credit monitoring plan to all affected.

Desjardin's proactive actions are in contrast to some other organizations that are repeatedly being questioned about their privacy practices. Think about how organizations with good privacy policies and practices could prevent the actions of unethical employees.

Google

Google was being investigated for using personal information for advertising purposes. The investigation consisted of determining whether Google's advertising was in line with the European Union's General Data Protection Regulations (GDPR). A company by the name of Brave sued Google, stating that companies wanting to show ads received personal data from Google. Data privacy came into play as personal data were being used to target ads, and the individuals whose data were being used were not informed of the practice.

When you use your email, or an Internet browser, notice how rapidly the advertisements change in response to your searches. Look at a computer desk for sale online, and suddenly, you will start receiving advertisements for desks and accessories, such as printer stands. What access to data enables such targeted advertising?

LabCorp

LabCorp, headquartered in Burlington, North Carolina, has clinical laboratories and provides drug development services. In 2019, personal and financial data such as credit card numbers were exposed, although individual lab test results were protected. Close to 8 million customers had their financial data and personal information such as names, addresses, telephone numbers, and account numbers accessed.

Every time you access medical services and provide your health card number, more data are added to your electronic health file. Linking those data to your financial information could result in unscrupulous individuals attempting to sell health-related products or taking advantage of a known health condition.

First American

In 2019, a data leak affected about 900 million customers at First American Insurance Company. Records as far back as 2003, which included

bank account numbers, tax details, and social security numbers, were accessed. Apparently, this breach occurred because First American used unsecured URLs (Uniform Resource Locators) as website locator addresses to access the confidential records.

This breach shows the relationship between data management (how information is accessed) and security. Organizations must have effective business practices that include security over the storage and access of their data to effectively provide privacy protection to their data.

Evite

In early 2019, it was revealed that information from the Evite website, which enables the sending of free e-invites, had been stolen and put up for sale by the perpetrator. About 10 million names, email addresses, and passwords were being sold. The company stated that other personal information such as phone numbers, birth dates, and mailing addresses, including financial data on record, had not been stolen.

However, if users did not immediately change their passwords, then any information associated with their account would be accessible by using the password. Think about how you use your computer. Do you use common passwords on multiple applications? Then, if your password and user access code is compromised, it could potentially be used for other websites where you have registered yourself.

Sources: Compiled from S. Lim, "Grab Fined by Singapore Government for Data Breach in Email Marketing Campaigns," *The Drum*, June 12, 2019; C. Mihalcik and R. Nieva, "Google's Ad System under EU Probe for How It Spreads Your Private Data," *Cnet*, May 22, 2019; CBC News, June 10, 2019, **www.cbc.ca**; R. Siegel, "LabCorp Discloses Data Breach Affecting 7.7 Million Customers," *The Washington Post*, June 5, 2019; S. Ikeda, "Security Oversight at First American Causes Data Leak of 900 Million Records," *CPO magazine*, June 10, 2019; C. Cimpanu, "Evite E-Invite Website Admits Security Breach," *ZDNet*, June 11, 2019; J. Montpetit, "Personal Data of 2.7 Million People Leaked from Desjardins," CBC News, June 20, 2019.

Questions

1. Discuss the types of data that are stored electronically and how they could be used by unethical individuals.
2. The fundamental tenets of ethics include responsibility, accountability, and liability. Discuss each of these tenets as it applies to the storage of data by financial institutions such as Desjardins Group and First American Insurance Corp.

Introduction

You will encounter numerous ethical and privacy issues in your career, many of which will involve IT in some manner. The two issues are closely related to each other and also to IT, and both raise significant questions involving access to information in the digital age. The answers to these questions are not straightforward. In fact, IT has made finding answers to these questions even more difficult.

Consider the actions of the companies in the chapter opening case. Clearly, actions that allowed confidential data to be distributed were not ethical. In a further example, suppose your organization decides to adopt social computing technologies (which you will study in Chapter 9) to include business partners and customers in new product development. You will be able to analyze the potential privacy and ethical implications of implementing these technologies.

This chapter provides insights into how to respond to ethical and privacy issues. Furthermore, it will help you to make immediate contributions to your company's code of ethics and its privacy policies. You will also be able to provide meaningful input concerning the potential ethical and privacy impacts of your organization's information systems on people within and outside the organization.

All organizations, large and small, must be concerned with ethics. In particular, small business (or startup) owners face a very difficult situation when their employees have access to sensitive customer information. There is a delicate balance between access to information and the appropriate use of that information. This balance is best maintained by hiring honest and trustworthy employees who abide by the organization's code of ethics. Ultimately this issue leads to another question: Does the small business, or a startup, even have a code of ethics to fall back on in this type of situation?

3.1 Ethical Issues

Ethics refers to the principles of right and wrong that individuals use to make choices that guide their behaviour. Deciding what is right or wrong is not always easy or clear-cut. Fortunately, there are many frameworks that can help us make ethical decisions.

Ethical Frameworks

There are many sources for ethical standards. Searches on the Internet for "ethical standards" will result in thousands of hits. For examples of some used in Canada, look at the Canadian Standards Association (**www.csa.ca**). Here we consider five widely used standards: the utilitarian approach, the rights approach, the fairness approach, the common good approach, and the deontology approach. There are many other sources, but these five are representative.

The *utilitarian approach* states that an ethical action is the one that provides the most good or does the least harm. The ethical corporate action would be the one that produces the greatest good and does the least harm for all affected parties—customers, employees, shareholders, the community, and the physical environment.

The *rights approach* maintains that an ethical action is the one that best protects and respects the moral rights of the affected parties. Moral rights can include the rights to make one's own choices about what kind of life to lead, to be told the truth, to not to be injured, and to enjoy a degree of privacy. Which of these rights people are actually entitled to—and under what circumstances—is widely debated. Nevertheless, most people acknowledge that individuals are entitled to some moral rights. An ethical organizational action would be one that protects and respects the moral rights of customers, employees, shareholders, business partners, and even competitors.

The *fairness approach* posits that ethical actions treat all human beings equally, or, if unequally, then fairly, based on some defensible standard. For example, most people might believe it is fair to pay people higher salaries if they work harder or if they contribute a greater amount to the firm. However, there is less certainty regarding chief executive officer (CEO) salaries that are hundreds or thousands of times larger than those of other employees. Many people question whether this huge disparity is based on a defensible standard or whether it is the result of an imbalance of power and hence is unfair.

The *common good approach* highlights the interlocking relationships that underlie all societies. This approach argues that respect and compassion for all others is the basis for ethical actions. It emphasizes the common conditions that are important to the welfare of everyone. These conditions can include a system of laws, effective police and fire departments, health care, a public educational system, and even public recreation areas.

Finally, the *deontology approach* states that the morality of an action is based on whether that action itself is right or wrong under a series of rules, rather than based on the consequences of that action. An example of deontology is the belief that killing someone is wrong, even if it was in self-defence.

These five standards are used to develop a general framework for ethics (or ethical decision making). Two such frameworks are shown in **Table 3.1**: a generic "traditional" approach and the GVV (Giving Voice to Values) approach.

Using the traditional ethical approach provides a tool for deciding the nature of an action response that you can take. The GVV approach provides tools for dealing with the ethical issue in a co-operative way. We now focus specifically on ethics in the corporate environment.

Ethics in the Corporate Environment

Many companies and professional organizations develop their own codes of ethics. A **code of ethics** is a collection of principles intended to guide decision making by members of the organization. For example, the Association for Computing Machinery (**www.acm.org**), an organization of computing professionals, has a thoughtful code of ethics for its members (see **www.acm.org/constitution/code.html**).

Keep in mind that different codes of ethics are not always consistent with one another. Therefore, an individual might be expected to conform to multiple codes. For example, a person who is a member of two large professional computing-related organizations may be simultaneously required by one organization to comply with all applicable laws and by the other organization to refuse to obey unjust laws.

TABLE 3.1 Traditional and GVV Approaches to Resolving Ethical Issues

Traditional Approach	Giving Voice to Values (GVV) Approach
1. Recognize an ethical issue • Could this decision or situation damage someone or some group? • Does this decision involve a choice between a good and a bad alternative? • Is this issue about more than what is legal? If so, how?	1. Identify an ethical issue • What are the different issues that give rise to this ethical issue? • What are the values of the individuals or organizations underlying this ethical issue? • Is there a possibility of action to resolve the ethical issue?
2. Get the facts • What are the relevant facts of the situation? • Do I know enough to make a decision? • Which individuals and/or groups have an important stake in the outcome? • Have I consulted all relevant persons and groups?	2. Purpose and choice • What personal choices do you have in reacting to this ethical issue? • What is your most appropriate professional choice, being guided by professional rules, and what would be a "good" choice?
3. Evaluate alternative actions • Which option will produce the most good and do the least harm? (the utilitarian approach) • Which option best respects the rights of all stakeholders? (the rights approach) • Which option treats people equally or proportionately? (the fairness approach) • Which option best serves the community as a whole, and not just some members? (the common good approach)	3. Stakeholder analysis • Who is affected by the ethical issue? • How are they affected, considering if I do give voice to resolving the issue? • How are they affected, considering if I do not give voice to resolving the issue? • How can I connect with the stakeholders to best deal with the ethical issue?
4. Make a decision and test it • Considering all the approaches, which option best addresses the situation? • Act and reflect on the outcome of your decision • How can I implement my decision with the greatest care and attention to the concerns of all stakeholders? • How did my decision turn out, and what did I learn from this specific situation?	4. Powerful response • Who is my audience? • What types of things could I say to provide a response to the ethical issue? • What are some *inhibiting arguments* that would prevent me from acting? • What could I say in response to the inhibiting arguments (called an *enabling argument*)? • What external arguments (called *levers*) support my enabling arguments? • What external research supports or refutes my arguments?
	5. Scripting and coaching • What words (script) could I use when talking about the ethical issue? (consider both positive and negative responses) • Who can I practise with? • How would I approach my audience to provide the best opportunity for discussing the ethical issue?

Fundamental tenets of ethics include:

- **Responsibility** means that you accept the consequences of your decisions and actions.
- **Accountability** refers to determining who is responsible for actions that were taken.
- **Liability** is a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

Before you go any further, it is critical that you realize that what is *unethical* is not necessarily *illegal.* For example, a bank's decision to foreclose on a home can be technically legal, but it can raise many ethical questions. In most instances, an individual or organization faced with an ethical decision is not considering whether to break the law. As the foreclosure example

illustrates, however, ethical decisions can have serious consequences for individuals, organizations, and society at large.

Unfortunately, we have seen a large number of extremely poor ethical decisions, not to mention outright criminal behaviour. Three of the most highly publicized fiascos in the United States occurred at Enron Corporation (now Enron Creditors Recovery Corporation), WorldCom (now MCI Inc.), and Tyco International. At each company, executives were convicted of various types of fraud using illegal accounting practices. These illegal acts resulted, at least in part, in the passage of the Sarbanes–Oxley Act in 2002 in the United States. This law requires that public companies implement financial controls and that, to ensure accountability, executives must personally certify financial reports. Similar problems occurred in Canada at companies like Nortel and Southam. In Canada, Bill 198, the Budget Measures Act, imposes similar requirements of management.

Advancements in information technologies have generated a new set of ethical problems. Computing processing power doubles roughly every 18 months, meaning that organizations are more dependent than ever on their information systems. Organizations can store increasing amounts of data at decreasing costs. As a result, they can maintain more data on individuals for longer periods of time. Going further, computer networks, particularly the Internet, enable organizations to collect, integrate, and distribute enormous amounts of information on individuals, groups, and institutions. These developments have created numerous ethical problems concerning the appropriate collection and use of customer information, personal privacy, and the protection of intellectual property. IT's About Business 3.1 illustrates how Google is analyzing credit- and debit-card data to link its users' searches with their offline (physical) purchases.

IT's About Business 3.1

Google Links Online Search Data and Offline Purchase Data

Data from the U.S. Census Bureau reveal that in the first quarter of 2018, 90 percent of retail purchases took place offline (physically at brick-and-mortar stores), and 9.5 percent took place online through retail e-commerce. Data for Canada indicate approximately 8 percent of sales were online in 2018. These figures indicate that the vast majority of retail sales are difficult to link to online advertising. These findings present a problem for Google (and Facebook), which must convince advertisers that online ads are effective. Google must also respond to Facebook's partnership with Square and Marketo, which enabled Facebook to track consumer store visits and some transactions. This partnership was a reaction to Google's store visit metrics, which had been part of the firm's AdWords product since 2014.

Google understands that to attract digital advertising dollars from advertisers who are still primarily spending on television ads, the company must prove that digital ads work. Google must therefore identify customers by analyzing their search histories, the ads they clicked on, and, ultimately, the items they purchased at brick-and-mortar stores. (It is important to note that Google is not the only company performing these analyses. Facebook, for example, also performs these analyses.)

For years, Google has been analyzing location data from Google Maps in an effort to prove that knowledge of people's physical locations can link the physical and digital worlds. This location-tracking ability has enabled Google to inform retailers whether people who viewed an ad for a lawn mower later visited or passed by a Home Depot store. Users can block their location data by adjusting the settings on their smartphones, but privacy experts contend that few users actually do so.

In addition to location data from Google Maps, Google has been analyzing users' Web browsing and search histories, using data from Google apps such as YouTube, Gmail, and the Google Play store. All of these data items are linked to the real identities of users when they log into Google's services.

Princeton University researchers used software called OpenWPM to survey the Internet's 1 million most popular websites in order to find evidence of tracking code on each website. OpenWPM automatically visits websites using the Firefox browser, and it logs any tracking code that it finds. The researchers found Google code on a majority of these sites. For example, they found Google Analytics, a product used to collect data on visitors to websites that integrates with Google's ad-targeting systems, on almost 70 percent of the websites. They also found DoubleClick, a dedicated ad-serving system from Google, on almost 50 percent of the websites. Perhaps the key finding was that the five most common tracking tools are all owned by Google.

Online publishers use tracking code from Google, Facebook, and many other companies to help target their advertising. When a company's tracking code is embedded on multiple websites, then the company can construct detailed profiles on individuals as they browse the Web, assigning them unique identifiers so they can be recognized. Privacy advocates argue that this practice needs to be scrutinized more carefully.

Compounding this issue, new credit card data enable Google to integrate these data sources to real-world purchase records. Google is now using billions of credit card transaction records to prove that its online ads are prompting people to make purchases,

even when the transactions occur offline in physical stores. This process gives Google a clearer method to analyze purchases than simply using location data. Furthermore, Google can now analyze purchase activity even when consumers deactivate location tracking on their smartphones.

Today, Google can determine the number of purchases generated by digital ad campaigns, a goal that marketing experts describe as the "holy grail" of online advertising. For example, Google can inform a company such as Sephora how many shoppers viewed an ad for eyeliner and then later visited a Sephora store and made a purchase. Advertisers can access this information with a new product called Google Attribution. They can identify which clicks and keywords had the largest impact on a consumer's purchasing decision.

Not surprisingly, Google's enhanced analytic tools have led to complaints about how the company uses personal information. Privacy advocates note that few people understand that their purchases are being analyzed in this way. Google responds that it has taken steps to protect the personal information of its users. In fact, the company claims to have developed a new, custom encryption technology that ensures that users' data remain private, secure, and anonymous.

Google further maintains that it is using patent-pending mathematical formulas to protect the privacy of consumers when it matches one of its users with a shopper who makes a purchase in a brick-and-mortar store. These formulas convert people's names and other purchase information, including the time stamp, location, and the amount of the purchase, into anonymous strings of numbers, a process called *encryption*. (We discuss encryption in Chapter 4.) These formulas make it impossible for Google to know the identity of the real-world shoppers and for the retailers to know the identities of Google's users. The retailers know only that a certain number of matches have been made. Google calls this process "double-blind" encryption.

Google has declined to explain how its new system works or to identify which companies are analyzing records of credit and debit cards on Google's behalf. Google states that it does not handle the records directly. It acknowledges, however, that its undisclosed partner companies had access to 70 percent of all transactions made with credit and debit cards in the United States.

Google does contend that all users who signed into Google's services consented to Google's sharing their data with third parties. However, Google would not disclose how merchants have obtained consent from consumers to share their credit card information. The company claims that it requires its partners to use only personal data that they have the "rights" to use. However, it would not say whether that meant that consumers had explicitly consented.

In the past, Google has obtained purchase data for a more limited set of consumers who participate in store loyalty programs. Those consumers are more heavily tracked by retailers, and they often give consent to share their data with third parties as a condition of signing up for the loyalty program.

Marc Rotenberg, executive director of the Electronic Privacy Information Center, notes that as companies are becoming increasingly intrusive in terms of their data collection, they are also becoming more secretive as to how they gather and use those data. He urged government regulators and the U.S. Congress to demand answers about how Google and other technology companies are collecting and using data from their users.

Paul Stephens of Privacy Rights Clearinghouse, a consumer advocacy group, has asserted that a marketing organization can identify an individual by examining only a few pieces of data. He expressed scepticism that Google's system for guarding the identities of users will stand up to the efforts of hackers who in the past have successfully stripped away privacy protections created by other companies after they experienced data breaches. He maintains that it is extremely difficult to keep data anonymous.

Sources: Compiled from "Facebook Is Even Keeping Track of You Offline," *Huffington Post*, March 25, 2018; J. Glenday, "Google Facing Possible Regulatory Review over Offline Tracking," *The Drum*, August 1, 2017; A. Kieler, "Google's Tracking of Offline Spending Sparks Call for Federal Investigation," *The Consumerist*, July 31, 2017; J. Naughton, "Google, Not GCHQ, Is the Truly Chilling Spy Network," *The Guardian*, June 18, 2017; N. Dawar, "Has Google Finally Proven that Online Ads Cause Offline Purchases?" *Harvard Business Review*, June 1, 2017; "Google Starts Tracking Retail Purchases for Online-to-Offline Attribution," *IPG Media Lab*, May 25, 2017; L. Tung, "Google: We'll Track Your Offline Credit Card Use to Show that Online Ads Work," *ZDNet*, May 24, 2017; R. Whitwam, "Google Can Now Track Your Offline Purchases," CNBC, May 24, 2017; H. Peterson, "Google Is under Fire for Watching You While You Shop Even When You're Not Online," AOL.com, May 24, 2017; R. Kilpatrick, "Google's New Feature Can Match Ad Clicks with In-Store Purchases," *Fortune*, May 23, 2017; "Google Starts Tracking Offline Shopping–What You Buy at Stores in Person," *Los Angeles Times*, May 23, 2017; E. Dwoskin and C. Timberg, "Google Now Knows When Its Users Go to the Store and Buy Stuff," *Washington Post*, May 23, 2017; "Internet Advertising Expenditure to Exceed US $200bn This Year," *Zenith Media*, March 26, 2017; T. Simonite, "Largest Study of Online Tracking Proves Google Really Is Watching Us All," *MIT Technology Review*, May 18, 2016; T. Simonite, "Probing the Dark Side of Google's Ad-Targeting System," *MIT Technology Review*, July 6, 2015; **www.google.com**, accessed October 3, 2018.

Questions

1. Describe the role that information technology plays as Google moves forward in its efforts to integrate online search data with offline purchase data.
2. The fundamental tenets of ethics include responsibility, accountability, and liability. Discuss each of these tenets as it applies to Google's actions in integrating online search data and offline purchase data.

Ethics and Information Technology

All employees have a responsibility to encourage ethical uses of information and information technology. Many of the business decisions you will face at work will have an ethical dimension. Consider the following decisions that you might have to make:

- Should organizations monitor employees' Web surfing and email?
- Should organizations sell customer information to other companies?
- Should organizations audit employees' computers for unauthorized software or illegally downloaded music or video files?

The diversity and ever-expanding use of IT applications have created a variety of ethical issues. These issues fall into four general categories: privacy, accuracy, property, and accessibility.

1. *Privacy issues* involve collecting, storing, and disseminating information about individuals.
2. *Accuracy issues* involve the authenticity, fidelity, and correctness of information that is collected and processed.
3. *Property issues* involve the ownership and value of information.
4. *Accessibility issues* revolve around who should have access to information and whether they should pay a fee for this access.

Table 3.2 lists representative questions and issues for each of these categories. IT's About Business 3.2 presents another ethical issue that is important to students.

IT's About Business 3.2

Quizlet

Quizlet (**https://quizlet.com/**) is a mobile and Web-based study application that allows students to study information with learning tools and games. The app is free and makes money from advertising and paid subscriptions for additional features. Quizlet claims to have over 30 million active users around the world.

Quizlet states that it continuously adds features, both seen and unseen, to ensure that the app is used properly to support learning. The app has an honour code that asks that students "be aware of and uphold their teacher or institution's policies regarding posting or sharing course materials online." Quizlet's community guidelines explicitly prohibit cheating and publicly posting copyrighted material, including test banks, exam questions, and other confidential course content.

Quizlet says that its goal is to help students learn and that it provides internal tools targeted at detecting current, active test material. Further, the company says it relies heavily on users to submit removal requests if they come across such material. Quizlet maintains that students also frequent other online sharing resources such as Brainly (**https://brainly.co**) and Google Docs (**https://docs.google.com**).

In the past, students have kept and shared paper copies of old exams but the world has changed. The digitization of learning materials, the standardization of curricula through online providers, and apps such as Quizlet could possibly increase the potential for academic dishonesty.

Quizlet is popular with students and many use the site legitimately. However, some students have openly tweeted about using Quizlet to cheat, either opening Quizlet in another browser while taking an online test or studying questions on Quizlet in advance that they knew were likely to be on their exam.

In May 2018, Texas Christian University (TCU; **www.tcu.edu**) suspended 12 students for using Quizlet to cheat on an exam. The incident spanned several semesters and involved a variety of classes in TCU's Bob Schieffer College of Communication.

Students contested the decision, saying that they used Quizlet to study but did not know that the questions they saw on the app would be on their exam. The accusation of cheating stemmed from the professor of the course stating that students should have notified him when they noticed that actual, current exam questions had appeared on the app.

The ensuing legal fight highlighted broader issues about learning in an educational environment with easily accessible digitized information. Many students reviewing material on the app have no knowledge of who put it there, how it was obtained, or whether the questions they are reviewing are current, active test questions. For example, many of the suspended TCU students said that they were unaware that the materials they had reviewed online were active test questions. Furthermore, they alleged that TCU-employed tutors had directed them to the site.

The students' lawyer defended their use of Quizlet by saying that the incident showed that universities had to "adapt to changes in technology" and that professors needed to adapt to new technologies and create new exam questions each term rather than reusing old questions.

The increasing popularity of widely used online resources that rely on crowdsourcing raises questions about what learning actually looks like for students today, and poses challenges for instructors. In fact, many educators say that in most disciplines, it may no longer be useful for students to memorize lists and regurgitate facts.

TCU later overturned yearlong suspensions for some students who were accused of using Quizlet to cheat on exams. The students' lawyer stated that all the students represented in the case had their suspensions overturned. Other steps that TCU took—including failing grades, academic probation, and charges of academic misconduct—remained in place and were still being appealed. TCU also stated that the professor in this incident was not at fault for not changing the questions on the exam.

Sources: Compiled from E. Kerr, "What a Controversy over an App Tells Us About How Students Learn Now," *The Chronicle of Higher Education*, May 15, 2018; T. Steele, "TCU Overturns Suspensions for Some Students Accused of Using Quizlet App to Cheat," *Dallas Morning News*, May 14, 2018; L. McKenzie, "Learning Tool or Cheating Aid?" *Inside Higher Ed*, May 14, 2018; "Texas Christian University Tutors Accused in Alleged Cheating Case," *CBS News,* May 10, 2018; S. English, "TCU Suspends 12 Students Accused of Cheating via a Popular Study App," *Star-Telegram*, May 10, 2018; J. Prothro, "TCU Suspends a Dozen Students over Scheme to Use Quizlet App to Cheat," *Dallas Morning News*, May 9, 2018; L. Kologny, "Popular Study App Quizlet Faces a Moment of Truth as a New School Year Begins," CNBC, August 23, 2017; **https://quizlet.com**, accessed September 17, 2018.

Questions

1. Discuss the ethics of students' use of Quizlet (and similar apps) to study for exams.
2. Discuss the ethics of students' not telling the course instructor that current, actual exam questions were on Quizlet.

TABLE 3.2 Categories and Questions for Ethical Issues

Privacy Issues
What information about oneself should an individual be required to reveal to others?
What kinds of surveillance can an employer use on its employees?
What types of personal information can people keep to themselves and not be forced to reveal to others?
What information about individuals should be kept in databases, and how secure is the information there?
Accuracy Issues
Who is responsible for the authenticity, integrity, and accuracy of the information collected?
How can we ensure that the information will be processed properly and presented accurately to users?
How can we ensure that errors in databases, data transmissions, and data processing are accidental and not intentional?
Who is to be held accountable for errors in information, and how should the injured parties be compensated?
Property Issues
Who owns the information?
What are the just and fair prices for its exchange?
How should we handle software piracy (illegally copying copyrighted software)?
Under what circumstances can one use proprietary databases?
Can corporate computers be used for private purposes?
How should experts who contribute their knowledge to create expert systems be compensated?
How should access to information channels be allocated?
Accessibility Issues
Who is allowed to access information?
How much should companies charge for permitting access to information?
How can access to computers be provided for employees with disabilities?
Who will be provided with the equipment needed for accessing information?
What information does a person or an organization have a right to obtain, under what conditions, and with what safeguards?

Table 3.2 uses four categories of ethical issues (privacy, accuracy, property, and accessibility), listing questions that organizations could ask themselves to develop effective policies for handling the issues. Many of the issues and scenarios discussed in this chapter involve privacy as well as ethics. In the next section, you will learn about privacy issues in more detail.

Before You Go On . . .

1. What does a code of ethics contain?
2. Describe the fundamental tenets of ethics.

3.2 Privacy

In general, **privacy** is the right to be left alone and to be free of unreasonable personal intrusions. **Information privacy** is the right to determine when, and to what extent, information about you can be gathered or communicated to others. Privacy rights apply to individuals, groups, and institutions. The right to privacy is recognized today in all Canadian provinces, the U.S. states, and by both federal governments, either by statute or in common law. Most countries around the world also have privacy rights laws or regulations.

Privacy can be interpreted quite broadly. However, court decisions in many countries have followed two rules fairly closely:

1. The right of privacy is not absolute. Privacy must be balanced against the needs of society.
2. The public's right to know supersedes the individual's right of privacy.

These two rules illustrate why determining and enforcing privacy regulations can be difficult.

As we discussed earlier, rapid advances in information technologies have made it much easier to collect, store, and integrate vast amounts of data on individuals in large databases. On an average day, data about you are generated in many ways: surveillance cameras located on toll roads, on other roadways, in busy intersections, in public places, and at work; credit card transactions; telephone calls (landline and cellular); banking transactions; queries to search engines; and government records (including police records). These data can be integrated to produce a **digital dossier,** which is an electronic profile of you and your habits. The process of forming a digital dossier is called **profiling**.

Data aggregators in the United States, such as LexisNexis (**www.lexisnexis.com**) and Acxiom (**www.acxiom.com**), are prominent examples of profilers. These companies collect public data such as real estate records and published telephone numbers in addition to nonpublic information such as social security numbers (and social insurance numbers in Canada); financial data; and police, criminal, and motor vehicle records. Statistics Canada (**www.statcan.gc.ca**), Canada's national statistics agency, provides aggregated information about businesses and individuals.

Data aggregators then integrate these data to form digital dossiers on most adults in the United States. They ultimately sell these dossiers to law enforcement agencies and companies that conduct background checks on potential employees. They also sell the dossiers to companies that want to know their customers better, a process called *customer intimacy.*

Electronic Surveillance

Electronic surveillance is rapidly increasing, particularly with the emergence of new technologies. Electronic surveillance is conducted by employers, the government, and other institutions.

Canadians today live with a degree of surveillance that would have been unimaginable just a few years ago. For example, surveillance cameras track you at airports, subways, banks, and other public venues. Inexpensive digital sensors are also everywhere now. They are incorporated into laptop webcams, video-game motion sensors, smartphone cameras, utility meters, passports, and employee ID cards. Step out your front door and you could be captured in a high-resolution photograph taken from the air or from the street by Google or Microsoft, as they update their mapping services. Drive down a city street, cross a toll bridge, or park at a shopping mall, and your licence plate can be recorded and time-stamped.

Emerging technologies such as low-cost digital cameras, motion sensors, and biometric readers are helping to increase the monitoring of human activity. The costs of storing and using digital data are also rapidly decreasing. The result is an explosion of sensor data collection and storage.

In fact, your smartphone has become a sensor. The average price of a smartphone has increased by 17 percent since 2000. However, the phone's processing capability has increased by *13,000 percent* during that time, according to technology market research firm ABI Research (**www.abiresearch.com**). As you will study in Chapter 8, smartphones can now record video, take pictures, send and receive email, search for information, access the Internet, and locate you on a map, among many other things. Your phone also stores large amounts of information about you that can be collected and analyzed. A special problem arises with smartphones that are equipped with global positioning system (GPS) sensors. These sensors routinely *geotag* photos and videos, embedding images with the longitude and latitude of the location shown in the image. Thus, you could be inadvertently supplying criminals with useful intelligence by posting personal images on social networks or photo-sharing websites. These actions would show the criminals exactly where you live and when you're there.

Another example of how new devices can contribute to electronic surveillance is facial recognition technology (see Chapter 4). Just a few years ago, this software worked only in very controlled settings such as passport checkpoints. However, this technology can now match faces even in regular snapshots and online images. For example, Intel and Microsoft have introduced in-store digital billboards that can recognize your face. These billboards can keep track of the products you are interested in based on your purchases or browsing behaviour. One marketing analyst has predicted that your experience in every store will soon be customized.

The rapidly increasing use of facial recognition technologies in China is causing much concern as the Chinese government planned to implement its *Social Credit Score* (SCS) by 2020. In this system, every citizen in China would be given a score that, as a matter of public record, would be available for all to see. The score comes from monitoring an individual's social behaviour, from their spending habits and how regularly they pay their bills, to their social interactions. The SCS will become the basis of that person's trustworthiness, which would also be publicly ranked. A citizen's SCS would affect their eligibility for a number of services, including the kinds of jobs or mortgages they can get, and it would also impact the schools for which their children qualify.

In 2018, China had already begun a voluntary implementation of the SCS by partnering with private companies in order to develop the algorithms needed for such a large-scale, data-driven system. These private companies included China Rapid Finance, a partner of social network giant Tencent, and Sesame Credit, a subsidiary of an Alibaba affiliate company, Ant Financial Services Group. Both Rapid Finance and Sesame Credit have access to huge amounts of data, the former through its WeChat messaging app with some 850 million users and the latter through its AliPay payment service.

Google and Facebook are using facial recognition software—Google Picasa and Facebook Photo Albums—in their popular online photo-editing and sharing services. Both companies encourage users to assign names to people in photos, a practice referred to as *photo tagging.* Facial recognition software then indexes facial features. Once an individual in a photo is tagged, the software searches for similar facial features in untagged photos. This process allows the user to quickly group photos in which the tagged person appears. Significantly, the individual is not aware of this process.

Why is tagging important? The reason is that once you are tagged in a photo, that photo can be used to search for matches across the entire Internet or in private databases, including databases fed by surveillance cameras. How could this type of surveillance affect you? As one example, a car dealer can take a picture of you when you step onto the car lot. They could then quickly profile you (find out information about where you live, your employment history, for example) on the Web to achieve a competitive edge in making a sale. Even worse, a stranger in a restaurant could photograph you with a smartphone and then go online to profile you for reasons of their own. One privacy lawyer has asserted that losing your right to anonymity would have a chilling effect on where you go, whom you meet, and how you live your life.

Drones are presenting additional surveillance concerns. Low-cost drones with high-performance cameras can be used for persistent aerial surveillance. Since the beginning of modern aviation, landowners have had rights to the airspace above their property up to 150 metres. However, to regulate small, low-flying drones, aviation authorities in some countries have assumed authority all the way down to the ground.

IT's About Business 3.3 and this chapter's closing case illustrate two other types of surveillance technology employed by law enforcement agencies.

IT's About Business 3.3

Licence Plate Readers

Law enforcement agencies have been using licence plate readers (LPRs) for some time to track stolen cars and to apprehend criminals. Today, private automobile repossession companies and towing companies photograph millions of plates every day with scanners on their tow trucks. They also use camera cars that drive around and collect plate scans from offices, malls, roadways, and driveways.

Each scan is stamped with the location (via global positioning system coordinates), date, and time. The databases of repossession and towing companies contain a huge amount of scans, which they sell to both law enforcement agencies and private companies. These private companies—which we call LPR companies here—also scan

licence plates themselves and use software to analyze the licence plate scans. LPR companies include Digital Recognition Network (**www.drndata.com**), Vigilant Solutions (**www.vigilantsolutions.com**), and MVTrac (**www.mvtrac.com**), among others. Canada's Border Services Agency also uses LPRs, with access to both U.S. and Canadian licence plate data (**www.cbc.ca/news/investigates/cbsa-perceptics-licence-plate-still-using-1.5187540**).

In total, there were at least 3 billion licence-plate photos in the private databases of LPR companies in 2018. Vigilant Solutions and Digital Recognition Network claimed they had scanned 2 billion licence plates since 2009 when they began the largest private licence-plate database in the United States, the National Vehicle Location Service.

Vigilant decided to offer the use of its database to U.S. police departments for free. In exchange, cities would give Vigilant their records of outstanding arrest warrants and overdue court fees, which the company would use to create a database of "flagged" vehicles. When licence plate readers spotted a flagged plate, officers would pull the driver over and instruct them either to pay the fine or to face arrest. For every transaction completed between police and civilians stopped with flagged plates, Vigilant would receive a 25 percent service fee.

With that much data, analytics can reveal much information about the owner of a car. Predicting where and when someone will drive is straightforward because the database contains data on how many times, and at what times, a car is spotted in a certain area. Analytics can therefore generate a person's driving history over time. In fact, Digital Recognition Network claimed that owners were typically within 300 metres of the vehicle. So, find the vehicle, and you find the owner.

LPR companies do not have access to the U.S. Department of Motor Vehicles (DMV) registrations. Therefore, although they can track a car, they cannot identify the owner. That information is protected by the Driver's Privacy Protection Act of 1994, which keeps drivers' names, addresses, and driving histories hidden from public view. However, the law makes exceptions for insurance companies and private investigators. LPR companies maintain that only two groups can use their software to find the owner of a car: law enforcement agencies and repossession companies. In Canada, private data related to vehicles is covered by general privacy legislation that is not specific to vehicles.

LPR companies are controversial regarding privacy issues. MVTrac contends that LPRs simply automate what police officers and the repossession industry have always done—check licence plates by eye—and that most Americans have accepted that the days of having true privacy have passed.

Significantly, LPR companies are not regulated in most U.S. states. In 2007, New Hampshire was the first state to ban LPRs completely except for toll collections and security on certain bridges.

LPRs have also caused controversy with their usage by law enforcement. In December 2013, the city of Boston suspended its LPR program after police accidentally revealed DMV-related information from its cameras to the *Boston Globe*.

Some law enforcement agencies keep data for days; others do so for years. In most states, police can monitor motorists with LPRs without having to obtain a search warrant or a court order. In February 2015, a U.S. Department of Homeland Security proposal for a privately hosted federal plate-tracking system was dropped days after the *Washington Post* exposed it.

In 2014, police in Tempe, Arizona, refused an offer from Vigilant for free LPR cameras. To receive the cameras, every month, officers would have to serve 25 warrants from a list supplied by Vigilant. If the department missed the quota, then it would lose the cameras. Such lists, according to the *Los Angeles Times* investigation that uncovered the offer, commonly come from debt-collector "warrants" against drivers with unpaid municipal fines.

At the same time, however, licence plate readers have proven valuable to police departments. For example, between January and September 2017, police in Danville, California, reported that they had made 31 arrests related directly to their LPR system. In addition, they recovered 15 stolen vehicles and made 11 more arrests when they recovered other stolen property. The Danville police chief asserted that the arrests would not have been made without the LPR system.

LPR systems immediately alert police officers if a vehicle has any associated police records, including if the car is stolen. LPRs in police patrol cars emit an audible alert each time they detect a licence plate that could be linked to a possible driving violation, a wanted individual, or a crime.

If the LPR system flags a car that is being driven, police officers manually run the licence plate through their dispatch centre to check the accuracy of the LPR system's data. Officers verify that the vehicle and driver match descriptions contained in law enforcement databases, and they then continue to build a case in the same way that they would without the LPR system.

LPR companies can also analyze their databases of licence plate scans in other ways. For instance, MVTrac analyzed its scans to track Honda Acuras at specific areas and times, including the exact models and colours. These data would be extremely valuable to automakers, marketers, and insurance companies.

As with technology in general, LPRs are improving faster than the legislation to regulate them. Today, LPR companies are exploring smaller cameras, smartphone apps that can pick out plates from live video, and the potential integration of public records, DMV databases, and facial-recognition software. Because police ostensibly use LPRs for public safety, people will likely have to accept some further loss of privacy when they drive.

Despite serious privacy concerns, there is some good news concerning the use of licence plate readers. For instance, the sheriff of Volusia County in central Florida stated that, between January 2017 and September 2018, the LPRs identified 67 people whom they were searching for and deputies were able to apprehend the driver of the vehicle. Furthermore, between January and September 2018, police in Miami Beach, Florida made 49 felony arrests using LPRs.

Sources: Compiled from E. von Ancken, "License Plate Readers Catch Dozens of Crooks, Rescue People in Need," ClickOrlando.com, August 15, 2018; A. Perez, "License Plate Readers Help Miami Beach Police Crack Down on Crime," Local10.com/Miami-Beach, July 31, 2018; S. Reese, "License Plate Readers Alert Police of Potential Crimes in Real-Time," NWI.com, October 1, 2017; S. Richards, "License-Plate Readers Credited with Helping Solve Crimes in Danville," *East Bay Times*, September 29, 2017; "California Supreme Court: Access to License Plate Data May Be Possible," *CBS,* August 31, 2017; T. Jackman, "Va. Supreme Court to Hear Case Challenging Police Retention of License Plate Data," *Washington Post*, June 27, 2017; D. Maass, "The Four Flavors of Automated License Plate Reader Technology," Electronic Frontier Foundation, April 6, 2017; K. Waddell, "How License-Plate Readers Have Helped Police and Lenders Target the Poor," *The Atlantic*, April 22, 2016; R. Sachs, "How Police License Plate Readers Can Invade Your Privacy," PRI.org, March 22, 2016;

C. Young, "Lawmakers Warned Plate Readers Could Lead to 'Dragnet Monitoring'," *Boston Globe*, March 1, 2016; C. Friedersdorf, "An Unprecedented Threat to Privacy," *The Atlantic*, January 27, 2016; C. Atiyeh, "How License Plate Readers Are Eroding Your Privacy," *Popular Mechanics*, January 29, 2015; **www.vigilantsolutions.com**, **www.drndata.com**, **www.mvtrac.com**, accessed October 3, 2018 C. Tunney and S. Gilchrist, "Border agency still using licence plate reader linked to U.S. hack," CBC News, Jun 25, 2019.

Questions

1. Discuss the ethics and the legality of licence plate readers.
2. Discuss the ethics and the legality of Vigilant Solutions offering its technology to police departments for free.
3. What are the privacy implications of analyzing licence plate scans?

The scenarios we just considered deal primarily with your personal life. However, electronic surveillance has become a reality in the workplace as well. In general, employees have very limited legal protection against surveillance by employers. The law supports the right of employers to read their employees' email and other electronic documents and to monitor their employees' Internet use. Today, more than three-fourths of organizations routinely monitor their employees' Internet usage. Two-thirds of them also use software to block connections to inappropriate websites, a practice called *URL filtering.* Furthermore, organizations are installing monitoring and filtering software to enhance security by blocking malicious software and to increase productivity by discouraging employees from wasting time.

In one organization, the chief information officer monitored roughly 13,000 employees for three months to determine the type of traffic they engaged in on the network. He then forwarded the data to the CEO and the heads of the human resources and legal departments. These executives were shocked at the questionable websites the employees were visiting, as well as the amount of time they were spending on those sites. The executives quickly decided to implement a URL filtering product.

In general, surveillance is a concern for private individuals regardless of whether it is conducted by corporations, government bodies, or criminals. As a country, Canada (like many nations) is still struggling to define the appropriate balance between personal privacy and electronic surveillance, especially in situations that involve threats to national security.

Personal Information in Databases

Information about individuals is being kept in many databases. Perhaps the most visible locations of such records are credit-reporting agencies. Other institutions that store personal information include banks and financial institutions; cable TV, telephone, and utility companies; employers; mortgage companies; hospitals; schools and universities; retail establishments; government agencies (Canada Revenue Agency, your province, your municipality); and many others.

There are several concerns about the information you provide to these record keepers. Some of the major concerns are as follows:

- Do you know where the records are?
- Are the records accurate?
- Can you change inaccurate data?
- How long will it take to make a change?
- Under what circumstances will the personal data be released?
- How are the data used?
- To whom are the data given or sold?
- How secure are the data against access by unauthorized people?

The Indian government's Aadhaar system is the largest biometric database in the world. IT's About Business 3.4 addresses the uses, advantages, and disadvantages of the system, as well as its privacy implications.

IT's About Business 3.4

India's Aadhaar System

India has vast numbers of anonymous poor citizens. To address this problem, the nation instituted its Unique Identification Project, known as Aadhaar (**https://uidai.gov.in**), which means "the foundation" in several Indian languages. The goal of the project is to issue identification numbers linked to the fingerprints and iris scans of every individual in the country.

Aadhaar was designed to remedy a critical problem that afflicts impoverished Indians. The Indian government has not officially acknowledged the existence of many poor citizens because these individuals do not possess birth certificates and other official documentation. Therefore, they have not been able to access government services to which they are entitled, nor have they been able to open bank accounts. When Aadhaar began, many Indian households were "unbanked," meaning that they had to stash their savings in cash around their homes.

The Indian government also wanted to reduce corruption and streamline the delivery of government services. Prior to Aadhaar, the government experienced problems in managing its welfare programs, and it lost millions of dollars each year as Indian citizens either provided fake names or entered their own names multiple times into the system in order to withdraw more than their fair share of benefits.

Initially, Aadhaar was optional and was used for only certain government subsidies, including those for food and liquefied natural gas for cooking. Further, the program targeted only those people in the greatest need of assistance, particularly rural villagers who lacked official forms of identification. Over time, Aadhaar's mission expanded.

Aadhaar went into operation in September 2010, when officials carrying iris scanners, fingerprint scanners, digital cameras, and laptops began to register the first few villagers as well as slum dwellers in the country's capital city, Delhi. One of the greatest challenges that the project faced was to ensure that each individuals' record in the Aadhaar database matched one and only one person. To perform this task, Aadhaar checks all 10 fingerprints and both irises of each person against those of everyone else in the country. Using the 10 prints and both irises boosted the Aadhaar accuracy rate to 99 percent. However, in a country the size of India, 99 percent accuracy means that 12 million people could have faulty records.

By July 2018, this process had encompassed 1.22 billion people. Aadhaar provides a 12-digit unique identity number to all Indian residents based on their biometric (all 10 fingerprints and both iris scans) and demographic data. In late 2017, the government added facial recognition as an additional biometric to further strengthen Aadhaar.

The biometrics data and the Aadhaar identification number serve as a verifiable, portable, and unique national ID. The Aadhaar project enables millions of Indian citizens to access government services that previously have been out of reach to them.

Today, Aadhaar is the largest biometric database in the world. The program now plays a key role in almost all parts of daily life in India.

Aadhaar became a vehicle to apply data-driven improvements to a wide range of government and private-sector services. The system is now linked to so many activities that it is almost impossible to live in India without enrolling. Participation in Aadhaar has become a requirement for filing taxes, opening bank accounts, receiving school lunch in the state of Uttar Pradesh, purchasing railway tickets online, accessing some public Wi-Fi, participating in the state of Karnataka's universal health care coverage, and benefiting from a wide range of welfare programs.

However, although Aadhaar has become central to life in India, the program is experiencing problems, especially among underserved populations. India has inconsistent Internet service outside its large cities. Consequently, rural towns struggle to go online to authenticate peoples' fingerprints with the central Aadhaar database. In some cases, that situation occurs when elderly or disabled individuals are unable to walk to the distribution sites to verify their identities. In addition, many people who perform manual labour have fingerprints that are too weathered from years of work to scan correctly. As a result, they are denied their food rations. One economist has asserted that millions of people have missed out on government benefits because they could not sign up for Aadhaar for these reasons.

Investigators found that approximately 1 million people in the state of Rajasthan alone were unfairly dropped from government lists for food subsidies because they could not sign up for Aadhaar. In addition, more than 3 million citizens were unable to collect their designated grain allocations. In one district alone, of approximately 2,900 people marked "dead" or "duplicate," 1,350 were actually neither. Nevertheless, they still lost access to their pensions.

There is also evidence of misuse of the Aadhaar program. Consider the following examples:

- 210 government agencies published the full names, addresses, and Aadhaar numbers of welfare beneficiaries.
- The Aadhaar information for 120 million users appears to have been leaked from the telecommunications company Reliance Jio (the company claims that the data were not authentic).
- Bank account and Aadhaar details of more than 100 million people were disclosed through certain open-government portals.
- The government's e-hospital database was hacked to access confidential Aadhaar information.

In addition to these problems, privacy advocates charge that the Aadhaar program faces even larger problems, namely its ubiquity and poor security. Specifically, they contend that when biometric information is used to access a service via Aadhaar—for example, purchasing a new cell phone—the service provider receives that person's demographic data (name, address, phone number), and the government receives the metadata—specifically, the date and time of the transaction, the form of identification used, and the company with which the transaction was carried out.

Aadhaar opponents are particularly concerned about the social stigma attached to some jobs in India; for example, manually cleaning sewers. They worry that Aadhaar will permanently stigmatize these individuals by allowing future employers, schools, banks, and new acquaintances to view their Aadhaar database information and judge them based on their work history. This situation could make social mobility in India even more difficult to achieve.

The Indian government views Aadhaar as an essential solution for a number of societal challenges. In contrast, critics see it as a step toward a surveillance state. In late August 2017, the Supreme Court issued a unanimous decision that found, for the first time, a fundamental right to privacy in the Indian Constitution. Aadhaar's opponents celebrated that decision because they believe that the program conflicts with this newly established right.

Next, the Supreme Court will decide whether Aadhaar violates privacy rights. If the Court finds that Aadhaar does so, then lawmakers will have to rethink the entire program. However, if the Court rules that the program does not violate privacy rights—that is, it determines that Aadhaar is constitutional—then the program will likely continue to grow.

In January 2018, the Indian Supreme Court began hearing crucial cases related to the constitutional validity of Aadhaar. In September 2018, the Court ruled 4:1 that Aadhaar did not violate the right to privacy.

Sources: Compiled from "Face Recognition Feature Set to Ensure Stronger Aadhaar Security: Here's More Detail," *Times of India*, March 13, 2018; "Aadhaar Authentication via Face Recognition from July: How It Will Work," *NDTV*, January 15, 2018; G. Prasad, "Aadhar-PAN Linking Must for Income Tax Return Filing from 1 July: Govt," *LiveMint*, September 30, 2017; M. Rajshekhar, "Aadhaar Shows India's Governance Is Susceptible to Poorly Tested Ideas Pushed by Powerful People," Scoll.in, September 30, 2017; K. Rathee, "Govt Plans to Link Driving Licence with Aadhaar," *Business Standard*, September 16, 2017; N. Kolachalam, "The Privacy Battle over the World's Largest Biometric Database," *The Atlantic*, September 5, 2017; "Right to Privacy a Fundamental Right: 7 Aadhaar Controversies that Raised Concern," *Hindustan Times*, August 24, 2017; T. Johnson, "IIT Kharagpur Graduate Hacked Aadhaar Data through Digital India App," *The Indian Express*, August 4, 2017; "Over 200 Government Sites Reveal Aadhaar Details; No Leakage from UIDAI," *The Economic Times*, July 20, 2017; A. Sethi and S. Bansa, "Aadhaar Gets New Security Features, but This Is Why Your Data Still May Not Be Safe," *Hindustan Times*, July 19, 2017; R. Khera, "The Different Ways in Which Aadhaar Infringes on Privacy," *The Wire*, July 19, 2017; P. Banerjee, "Massive Trove of Reliance Jio User Data Leaked Online," Digit.in, July 9, 2017; A. Srupathi, "How Public Apathy Continues to Keep Manual Scavengers Invisible and in the Margins," *The Wire*, March 18, 2017; "Aadhaar ID Saving Indian Govt about $1 Billion per Annum: World Bank," *The Economic Times*, January 14, 2016; S. Rai, "Why India's Identification Scheme Is Groundbreaking," BBC News, June 5, 2012; E. Hannon, "For India's Undocumented Citizens, an ID at Last," NPR.org, March 1, 2012; **www.uidai.gov.in**, accessed September 30, 2018; M. Surl, "Aadhaar: India Supreme Court Uholds Controversial Biometric Database, CNNWorld, September 26, 2018.

Questions

1. Discuss the ethics and the legality of India's Aadhaar system.
2. Court decisions in many countries have stated that an individual's privacy must be balanced against the needs of society. Does the Aadhaar system go too far in favour of the needs of society? Why or why not? Support your answer.

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

Every day we see more and more *electronic bulletin boards, newsgroups, electronic discussions* such as chat rooms, and *social networking sites* (discussed in Chapter 9). These sites appear on the Internet, within corporate intranets, and on blogs. A *blog,* short for "weblog," is an informal, personal journal that is frequently updated and is intended for general public reading. How does society keep owners of bulletin boards from disseminating information that may be offensive to readers or simply untrue? This is a difficult problem because it involves the conflict between freedom of speech on the one hand and privacy on the other. This conflict is a fundamental and continuing worldwide ethical issue.

There is no better illustration of the conflict between free speech and privacy than the Internet. Many websites contain anonymous, derogatory information on individuals, who typically have little recourse in the matter. Many organizations use the Internet in examining job applications, including searching on Google and on social networking sites. Consequently, derogatory information contained on the Internet can harm a person's chances of being hired.

Privacy Codes and Policies

Privacy policies or **privacy codes** are an organization's guidelines for protecting the privacy of its customers, clients, and employees. In many corporations, senior management has begun to understand that when they collect vast amounts of personal information, they must protect it. Many organizations also give their customers some voice in how their information is used by providing them with opt-out choices. The **opt-out model** of informed consent permits the company to collect personal information until the customer specifically requests that the data not be collected. You can see an example of this by looking at the global American Express data protection and privacy principles statement (from **www.americanexpress.com**). The statement is organized with numbered steps, with the first step (collection) saying that they only collect the information that is used to conduct normal business operations. The second step (notice

and processing) indicates that they explain in their privacy statement how they collect their data, and that you may object to the way they do so based upon the applicable laws where you live.

Privacy advocates prefer the **opt-in model** of informed consent, which prohibits an organization from collecting any personal information unless the customer specifically authorizes it. Although the opt-out model is a common approach, Canada's privacy commissioner (see **www.priv.gc.ca/**) states that consent should be sought, which is the opt-in model. Canada's anti-spam legislation, Bill C-28, requires that organizations use the opt-in model for the sending of emails. This means that organizations need to have data collection processes so that they can keep records of which customers have agreed to receiving emails, and which ones have not. Details about the requirements of the law are available at **www.fightspam.gc.ca**.

One privacy tool available to consumers is the *Platform for Privacy Preferences* (P3P) (see **www.w3.org/TR/P3P/**). It was developed by the World Wide Web Consortium, a group that creates standards for the Web. P3P automatically communicates privacy policies between an electronic commerce website and visitors to that site. P3P enables visitors to determine the types of personal data that can be extracted by the websites they visit. It also allows visitors to compare a website's privacy policy with the visitors' preferences or with other standards, such as the Canadian Standards Association Model Code for the Protection of Personal Information (see **www.csa.ca/cm/ca/en/privacy-code**) or the European Union Directive on Data Protection.

Canada's privacy legislation is called the Personal Information Protection and Electronic Documents Act (PIPEDA). It became effective January 1, 2004. The legislation applies to businesses and other organizations, such as non-profit organizations. PIPEDA is based upon the principles in the Canadian Standards Association Model Code. As part of the legislation, organizations are required to establish a privacy policy, as well as procedures to ensure that the policy is adhered to.

Table 3.3 provides a sampling of privacy policy guidelines. The last section, "Data Confidentiality," refers to security, which we consider in Chapter 4. All of the good privacy intentions in the world are useless unless they are supported and enforced by effective security measures.

Despite privacy codes and policies, and despite opt-out and opt-in models, guarding whatever is left of your privacy is becoming increasingly difficult. This problem is illustrated in IT's About Business 3.3, 3.4, and 3.5 as well as in the chapter closing case.

TABLE 3.3 Privacy Policy Guidelines: A Sampler

Data Collection
Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.
Data should be adequate, relevant, and not excessive in relation to the business objective.
Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).
Data Accuracy
Sensitive data gathered on individuals should be verified before they are entered into the database.
Data should be kept current, where and when necessary.
The file should be made available so that the individual can ensure that the data are correct.
In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.
Data Confidentiality
Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.
Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.
Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.
Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

IT's About Business 3.5

Facebook and the Cambridge Analytica Data Scandal

In mid-March 2018, *The Guardian* and *The New York Times* published the Facebook-Cambridge Analytica (CA) major data scandal when they revealed that CA had collected the personal information of 87 million Facebook users. The newspapers outlined how the data of these Facebook users were obtained by CA. *The Guardian* referred to the data misuse as a breach but Facebook disagreed. A Facebook executive stated that no systems were infiltrated, and no passwords or information were stolen or hacked.

The Facebook-Cambridge Analytica (CA) scandal involved the collection and subsequent use of personally identifiable information on 87 million Facebook users. The timeline of the incident is useful in understanding what happened.

In April 2010, Facebook deployed software called Open Graph that enabled external developers to contact Facebook users and request permission to access their personal data and to access their Facebook friends' personal data as well. If the user accepted, these developers could access a user's name, gender, location, birthday, education, political preferences, relationship status, religious views, online chat status, and more. With additional permissions, external developers could access a user's private messages.

In 2013, Cambridge University academician, Aleksandr Kogan, and his company Global Science Research developed a personality-quiz app called "This Is Your Digital Life." The app prompted users to answer questions for a psychological profile. Almost 300,000 Facebook users installed Kogan's app on their accounts.

As with any Facebook developer at the time, Kogan could access personal data about those users and their Facebook friends (with appropriate permissions from users themselves). Furthermore, Kogan's app collected that personal information and loaded it into a private database instead of immediately deleting it. Kogan then provided that database, containing information about 87 million Facebook users, to the voter-profiling company Cambridge Analytica. CA used the data to develop 30 million "psychographic" profiles about voters.

In 2014, Facebook changed its rules to limit a developer's access to user data. This change was made to ensure that a third-party could not access a user's friends' data without gaining permission first. However, the rule changes were not retroactive and Kogan did not delete the data thought to have been improperly acquired.

In late 2015, reports suggested that U.S. Senator Ted Cruz's presidential campaign was using psychological data based on research on millions of Facebook users. In response to the reporting, Facebook said that when it learned about the data leaks, it tried to ban Kogan's app and legally pressured both Kogan and CA to remove the data they had improperly collected. Facebook claimed that both Kogan and CA certified that they had deleted the data.

In 2016, Donald Trump's presidential campaign invested heavily in Facebook ads, helped by CA. In August 2018, questions were still being hotly debated about Facebook's role in the 2016 elections. Many questions have focused on Facebook's News Feed and the role it played in magnifying Russian propaganda and other hoaxes. Lawmakers have also criticized the company's lax sale of political advertisements, with some buyers literally paying with Russian rubles. Political ads are not regulated as closely online as they are on television or radio.

After the Facebook-Cambridge Analytica scandal was revealed, Facebook began instituting a series of changes to repair the damage. The company banned Canadian firm, AggregateIQ, and Italian firm, CubeYou, from the Facebook platform following indications that the two companies had improperly accessed user data.

Facebook also restricted who could place political advertisements, or issue ads, on its platform to "authorized advertisers" who have had their identity and location confirmed by the platform. For authorization, advertisers had to provide Facebook with a government-issued ID and a physical mailing address. Furthermore, each issue ad had to be labelled with a marker identifying it as "Political Ad," with information displayed beside the ad that showed who paid for it.

Facebook began working with outside groups to develop criteria for what was considered a political ad. The move intended to prevent or limit "bad actors" who try to interfere with foreign elections, likely in response to the discovery that 470 fake Russian Facebook accounts spent about US $100,000 on roughly 3,000 ads on the platform during the 2016 U.S. presidential election.

In March 2018, the U.S. Federal Trade Commission (FTC; **www.ftc.gov**) announced that it was investigating Facebook for possible violations of the firm's 2011 agreement with the FTC. At that time, the FTC charged that Facebook had deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. The settlement required Facebook to provide consumers with clear and prominent notice and obtain their express consent before their information was shared beyond the privacy settings that the consumers established.

A *single* violation of Facebook's 2011 agreement with the FTC could carry a fine up to US $40,000. Thus, for continuing misuses of consumer data, in July 2019, the FTC approved a fine that was estimated to total about US $5 billion, which at the time of writing (November 2019) was waiting for approval from the U.S. Justice Department.

In March 2018, Cambridge Analytica and its parent company SCL Elections instigated insolvency proceedings and closed. The question is: What happens with the data that the firms had collected?

In July 2018, the UK's Information Commissioner fined Facebook £500,000 for breaking data protection laws following an investigation into the Cambridge Analytica scandal. The investigation found that Facebook had contravened UK law by failing to protect people's data and that the company had also failed to be transparent about how personal data were being used by others. Facebook did have an opportunity to respond before a final decision was made. The scandal took place before the European Union's GDPR (General Data Protection Regulation) came into force on May 25, 2018, or Facebook would have faced a multi-million-dollar fine.

In addition, the United Kingdom announced its intent to bring a criminal prosecution against SCL Elections Ltd., the parent company of Cambridge Analytica, for failing to adequately respond to an enforcement notice issued in May 2018. In an accompanying report, the UK data regulator has made recommendations for how

the government can improve transparency around online campaigning and the political use of personal data.

In August 2018, lawyers for a group of UK residents whose Facebook data was collected by CA filed a class-action suit against Facebook, which resulted in a fine of £500,000, the maximum fine under the privacy legislation then in force in the United Kingdom.

Since 2007, Facebook has changed its rules about how much data apps can access. However, over that time, how many developers followed Facebook's rules? How many acted like Kogan did, storing the data and creating their own private databases? Where are those data now, and who has them? If all those private user data are as powerful as Cambridge Analytica has said they were, what have they been used to do?

Sources: Compiled from I. Lapowsky, "UK Group Threatens to Sue Facebook over Cambridge Analytica," *Wired*, July 31, 2018; M. Burgess and J. Temperton, "Facebook Broke Data Law and Faces £500,000 Fine over Cambridge Analytica Scandal," *Wired*, July 10, 2018; "Former Cambridge Analytica Employee Says 'There Were More' Apps that Collected User Data," CBS News, June 27, 2018; C. Stokel-Walker, "What Will Happen to Cambridge Analytica's Data Now It Has Closed?" *Wired*, May 4, 2018; A. Hern, "Far More than 87M Facebook Users Had Data Compromised, MPs Told," *The Guardian*, April 17, 2018; A. Schomer, "Facebook Moves to Impress Regulators," *Business Insider*, April 10, 2018; S. Meredith, "Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal," CNBC, April 10, 2018; W. Ashford, "Facebook Data Scandal a Game Changer, Says ICO," *Computer Weekly*, April 9, 2018; J. Sanders, "If Your Organization Advertises on Facebook, Beware of These New Limitation," *TechRepublic*, April 9, 2018; O. Solon, "Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data," *The Guardian*, April 4, 2018; W. Ashford, "Facebook Braces for New Regulation for Cambridge Analytica Deal," *Computer Weekly*, March 23, 2018; T. Romm and C. Timberg, "FTC Opens Investigation into Facebook after Cambridge Analytica Scrapes Millions of Users' Personal Information," *The Washington Post*, March 20, 2018; R. Meyer, "The Cambridge Analytica Scandal, in 3 Paragraphs," *The Atlantic*, March 20, 2018; M. Giles, "The Cambridge Analytica Affair Reveals Facebook's 'Transparency Paradox'," *MIT Technology Review*, March 20, 2018; B. Tau and D. Seetharaman, "Data Blowback Pummels Facebook," *The Wall Street Journal*, March 20, 2018; K. Granville, Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *The New York Times*, March 19, 2018; M. Rosenberg, N. Confessore, and C. Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *The New York Times*, March 17, 2018; H. Davies, "Ted Cruz Campaign Using Firm that Harvested Data on Millions of Unwitting Facebook Users," *The Guardian*, December 11, 2015; Facebook, **www.facebook.com**, accessed September 16, 2018; C. Kang, "F.T.C. Approves Facebook Fine of about $5 Billion," *The New York Times*, July 12, 2019; J. Vincent, "UK Data Watchdog Fines Facebook Maximum Legal Amount for Cambridge Analytica Data Scandal," **www.theverge.com**, October 25, 2018, accessed August 11, 2019.

Questions

1. Discuss the legality and the ethics of Facebook in the Facebook-Cambridge Analytica incident.
2. Discuss the legality and the ethics of Cambridge Analytica in the Facebook-Cambridge Analytica incident.
3. Describe how each of the fundamental tenets of ethics (responsibility, accountability, and liability) applies to Facebook and then to Cambridge Analytica in this incident.

International Aspects of Privacy

As the number of online users has increased globally, governments throughout the world have enacted a large number of inconsistent privacy and security laws. This highly complex global legal framework is creating regulatory problems for companies. Approximately 50 countries have some form of data protection laws. Many of these laws conflict with those of other countries, or they require specific security measures. Other countries have no privacy laws at all.

The absence of consistent or uniform standards for privacy and security obstructs the flow of information among countries *(transborder data flows)*. The European Union (EU), for one, has taken steps to not only overcome this problem but also to protect the rights of individuals. The EU data protection laws, like the Canadian ones, are stricter than the U.S. laws, and therefore, could create problems for U.S.-based multinational corporations, which could face lawsuits for privacy violations.

On May 25, 2018, the *General Data Protection Regulation* (GDPR), the world's strongest data protection laws, went into effect in the European Union. The GDPR replaces the 1995 data protection directive.

The GDPR modernizes laws that protect the personal information of individuals because previous data protection laws across Europe could not keep pace with rapid technological changes. The GDPR changes how businesses and public sector organizations manage the information of their customers. The regulation also increases the rights of individuals and gives them more control over their own information.

The GDPR covers both personal data and sensitive personal data. *Personal data* includes information that can be used to identify a person, such as a name, address, Internet Protocol address, and many other pieces of information. *Sensitive personal data* encompass genetic data, racial information, information about religious and political views, sexual orientation, trade union membership, among others.

The GDPR applies to *data controllers*, which are the organizations that have relationships with data subjects, and *data processors*, which are organizations that work for data controllers

and process personal data on the controllers' behalf. The GDPR defines a *natural person* as a living human being and a *data subject* as a human being whose data an organization has or processes.

The GDPR states that data controllers and data processors should keep minimal data on each data subject, secure them properly, ensure that they are accurate, and retain the data for just as long as they are needed. The GDPR also covers individuals' rights, which include:

- The right to know what organizations are doing with their data.
- The right to ask, at any time, for copies of all the data that organizations have about them.
- The right to know an organization's justification why it has their data and how long it is planning to keep them.
- The right to have their data corrected, if needed.
- The right to have their data deleted. This provision is called the "right to be forgotten."

The GDPR provides the ability for regulators to fine businesses that do not comply with the regulation. Specifically, regulators can fine an organization if it:

- does not correctly process an individual's data;
- experiences a security breach; and
- is required to have, but does not have, a data protection officer.

The transfer of data into and out of a nation without the knowledge of either the authorities or the individuals involved raises a number of privacy issues. Whose laws have jurisdiction when records are stored in a different country for reprocessing or retransmission purposes? For example, if data are transmitted by a Polish company through a Canadian satellite to a British corporation, which country's privacy laws control the data, and at what points in the transmission? Questions like these will become more complicated and frequent as time goes on. Governments must make an effort to develop laws and standards to cope with rapidly changing information technologies to solve some of these privacy issues.

Privacy legislation anywhere shares the goal of privacy protection for its citizens. Canada's PIPEDA privacy legislation discusses and requires the use of 10 principles:

1. accountability,
2. identifying purposes,
3. consent,
4. limiting collection,
5. limiting use, disclosure, and retention,
6. accuracy,
7. safeguards,
8. openness,
9. individual access, and
10. challenging compliance.

The following list of benefits of high-quality information privacy is from a business perspective:

- To protect the organization's public image or brand images;
- To maintain or enhance trust and promote continued consumer confidence in the organization and promote goodwill;
- To achieve a competitive advantage in the marketplace by maintaining high quality, accurate customer information;
- To meet legal requirements of industry associations or organizations (such as of e-payment and credit card processors); and

- To efficiently manage personal information, reducing administration or data handling costs and avoiding additional financial costs, such as the need to modify information systems to meet legal requirements.

Before You Go On . . .

1. Describe the issue of privacy as it is affected by IT.
2. Discuss how privacy issues can impact transborder data flows.

What's In IT For Me?

For the Accounting Major

Public companies, their accountants, and their auditors have significant ethical responsibilities. Accountants now are being held professionally and personally responsible for increasing the transparency of transactions and assuring compliance with Canadian privacy principles.

For the Finance Major

As a result of global regulatory requirements, financial managers must follow strict ethical guidelines. They are responsible for full, fair, accurate, timely, and understandable disclosure in all financial reports and documents that their companies submit to regulatory agencies. Furthermore, financial managers are responsible for compliance with all applicable governmental laws, rules, and regulations.

For the Marketing Major

Marketing professionals have new opportunities to collect data on their customers; for example, through business-to-consumer electronic commerce (discussed in Chapter 7). Business ethics clearly mandate that these data should be used only within the company and should not be sold to anyone else. Marketers do not want to be sued for invasion of privacy over data collected for the marketing database.

Customers expect their data to be properly secured. However, profit-motivated criminals want that data. Therefore, marketing managers must analyze the risks of their operations. Failure to protect corporate and customer data will cause significant public relations problems and outrage customers. Customer relationship management (discussed in Chapter 11) operations and tracking customers' online buying habits can expose unencrypted data to misuse or result in privacy violations.

For the Production/Operations Management Major

POM professionals decide whether to outsource (or offshore) manufacturing operations. In some cases, these operations are sent overseas to countries that do not have strict labour laws. This situation raises serious ethical questions. For example: Is it ethical to hire employees in countries with poor working conditions in order to reduce labour costs?

For the Human Resource Management Major

Ethics is critically important to HR managers. HR policies explain the appropriate use of information technologies in the workplace. Questions such as the following can arise: Can employees use the Internet, email, or chat systems for personal purposes while at work? Is it ethical to monitor employees? If so, how? How much? How often? HR managers must formulate and enforce such policies while at the same time, maintaining trusting relationships between employees and management.

For the MIS Major

Ethics might be more important for MIS personnel than for anyone else in the organization because these individuals have control of the information assets. They also have control over a huge amount of the employees' personal information. As a result, the MIS function must be held to the highest ethical standards.

Summary

1. Define ethics and explain its three fundamental tenets and the four categories of ethical issues related to information technology.

Ethics refers to the principles of right and wrong that individuals use to make choices that guide their behaviour.

Fundamental tenets of ethics include responsibility, accountability, and liability. Responsibility means that you accept the consequences of your decisions and actions. Accountability refers to determining who is responsible for actions that were taken. Liability is a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

The major ethical issues related to IT are privacy, accuracy, property (including intellectual property), and access to information. Privacy may be violated when data are held in databases or transmitted over networks. Privacy policies that address issues of data collection, data accuracy, and data confidentiality can help organizations avoid legal problems.

Privacy is the right to be left alone and to be free of unreasonable personal intrusions. Threats to privacy include advances in information technologies, electronic surveillance, personal information in databases, Internet bulletin boards, newsgroups, and social networking sites. The privacy threat in Internet bulletin boards, newsgroups, and social networking sites is that you might post too much personal information that many unknown people can see.

2. Discuss at least one potential threat to the privacy of the data stored in each of three places that store personal data.

Chapter Glossary

accountability A tenet of ethics that refers to determining who is responsible for actions that were taken.

code of ethics A collection of principles intended to guide decision making by members of an organization.

digital dossier An electronic description of an individual and their habits.

electronic surveillance Tracking people's activities with the aid of computers.

ethics The principles of right and wrong that individuals use to make choices to guide their behaviours.

information privacy The right to determine when, and to what extent, personal information can be gathered by or communicated to others.

liability A legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

opt-in model A model of informed consent in which a business is prohibited from collecting any personal information unless the customer specifically authorizes it.

opt-out model A model of informed consent that permits a company to collect personal information until the customer specifically requests that the data not be collected.

privacy The right to be left alone and to be free of unreasonable personal intrusions.

privacy policies (or privacy codes) An organization's guidelines for protecting the privacy of customers, clients, and employees.

profiling The process of forming a digital dossier.

responsibility A tenet of ethics in which you accept the consequences of your decisions and actions.

Discussion Questions

1. In 2008, the Massachusetts Bay Transportation Authority (MBTA) obtained a temporary restraining order barring three Massachusetts Institute of Technology (MIT) students from publicly displaying what they claimed to be a way to get "free subway rides for life." Specifically, the 10-day injunction prohibited the students from revealing vulnerabilities of the MBTA's fare card. The students were scheduled to present their findings in Las Vegas at the DEFCON computer hacking conference. Were the students' actions legal? Were their actions ethical? Discuss your answer from the students' perspective and then from the perspective of the MBTA.

2. Frank Abagnale, the criminal played by Leonardo DiCaprio in the motion picture *Catch Me If You Can*, ended up in prison. After he left prison, however, he worked as a consultant to many companies on matters of fraud.

a. Why do these companies hire the perpetrators (if caught) as consultants? Is this a good idea?

b. You are the CEO of a company. Discuss the ethical implications of hiring Frank Abagnale as a consultant.

3. Access various search engines to find information relating to the use of drones (unmanned aerial vehicles) for electronic surveillance purposes in Canada.

a. Take the position favouring the use of drones for electronic surveillance.

b. Take the position against the use of drones for electronic surveillance.

4. Research the Volkswagen "Diesel Dupe." The fundamental tenets of ethics include responsibility, accountability, and liability. Discuss each of these tenets as it applies to the Volkswagen scandal.

5. Research the Ashley Madison breach.

a. Discuss the legality and the ethics of the Ashley Madison website.

b. Discuss the legality and the ethics of the actions of the hackers who stole data from the Ashley Madison website.

c. Discuss the legality and the ethics of the actions of people who copied the Ashley Madison data from the Dark Web and then made the data available on the open Web.

d. Discuss the legality and the ethics of the reporters who used stolen data in their stories.

e. Are there differences in your answers to the first four questions? If so, then describe them. How do you account for the differences?

Problem-Solving Activities

1. An information security manager routinely monitored Web surfing among the company's employees. The manager discovered that many employees were visiting the "sinful six" websites. (*Note:* The "sinful six" are websites with material related to pornography, gambling, hate, illegal activities, tastelessness, and violence.) The manager then prepared a list of the employees and their surfing histories and gave the list to management. Some managers punished their employees. Some employees, in turn, objected to the monitoring, claiming that they and other employees should have a right to privacy.
   a. Is monitoring of Web surfing by managers ethical? (It is legal.) Support your answer.
   b. Is employee Web surfing on the "sinful six" ethical? Support your answer.
   c. Is the security manager's submission of the list of abusers to management ethical? Why or why not?
   d. Is punishing the abusers ethical? Why or why not? If yes, then what types of punishment are acceptable?
   e. What should the company do in this situation? (*Note:* There are a variety of possibilities here.)
2. Access the Computer Ethics Institute's website at **www.cpsr.org/issues/ethics/cei**. The site offers the "Ten Commandments of Computer Ethics." Study these and decide whether any others should be added.
3. Access the Association for Computing Machinery's code of ethics for its members (see **www.acm.org/code-of-ethics**). Discuss the major points of this code. Is this code complete? Why or why not? Support your answer.
4. In 2008 a web site called HYPERLINK "**http://www.eightmaps.com**" **www.eightmaps.com** arose which held the names, addresses and maps of individuals who made donations to support a proposal in the U.S. called Proposition 8 that supported gay marriage. The map was a "mashup" that used Google maps and publicly available donor lists. What if someone used publicly available donor lists to create maps to homes of people who supported gun laws or abortion? Is the use of data in this way unethical or illegal? Support your answer.
5. The Electronic Frontier Foundation (**www.eff.org**) has a mission of protecting rights and promoting freedom in the "electronic frontier." Review the organization's suggestions about how to protect your online privacy and summarize what you can do to protect yourself.
6. Access your university's guidelines for ethical computer and Internet use. Are there limitations as to the types of websites that you can visit and the types of material you can view? Are you allowed to change the programs on the lab computers? Are you allowed to download software from the lab computers for your personal use? Are there rules governing the personal use of computers and email?
7. Access **www.albion.com/netiquette/corerules.html**. What do you think of this code of ethics? Should it be expanded? Is it too general?
8. Access **www.cookiecentral.com** and **www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives**. Do these sites provide information that helps you protect your privacy? If so, then explain how.
9. Do you believe that a university should be allowed to monitor email sent and received on university computers? Why or why not? Support your answer.

Chapter Closing Case

Case 3.2 Accessing Patient Data through Electronic Medical Records

When a patient is admitted to a hospital emergency room, the physician may have never seen them before, and must diagnose their problem quickly. If the physician knew the patient's medical history, then the examination and subsequent diagnosis would be faster, possibly less expensive, and more accurate.

To address this problem, the Government of Canada created Canada Health Infoway (**www.infoway-inforoute.ca**), with the objective of helping the provinces and territories perform a "digital makeover" of their health records management systems to improve health while reducing costs. In its first decade, Infoway spent more than $2 billion on the project. Infoway's goal is to provide a database with the records of each patient treated in every hospital and doctor's office across Canada. The database would then allow physicians to track patients' visits across the country.

This is now a reality in Canada. Doctors across the country now use electronic medical records, or EMRs, to access patient information online. Doctors can look up when a patient was last seen, which specialist they saw (audiologist, respirologist, cardiologist, or others), what tests were performed with their results, what medications were prescribed with dosage, and any confirmed future appointments.

Medical data are private, confidential data. The website of the Office of the Privacy Commissioner of Canada (**www.priv.gc.ca**) explains that (effective January 2018) there were three provinces that had privacy laws that are considered similar enough to PIPEDA to be used in its stead: Alberta, British Columbia, and Quebec. In addition, there were four provinces that had health-related privacy laws that could be used: Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia. For other provinces, privacy and the privacy of health data would be covered by PIPEDA, our federal privacy legislation.

Sadly, there are many leaks and unauthorized accesses to private medical data. For example, Nova Scotia's then-privacy commissioner Catherine Tully reported in June 2019 that there were 865 privacy breaches during the period from April 1, 2018 to March 31, 2019.

E-Health Saskatchewan was proactive in monitoring the privacy of the victims of the Humboldt Broncos junior hockey team bus crash of April 2018. Within days of the crash, the e-health agency started tracking accesses to the health records of the team members. Several doctors and an office manager were charged with inappropriately accessing the team's medical records during April and May 2018.

It is not only doctors and medical clinics that are gathering electronic health information. For example, the use of smartphones, tablets, and personal technology such as Fitbit and glucose monitors provide the ability to collect vast amounts of data about an individual's quality of health (such as biometric data, or food and drug intake). Such large amounts of data, what experts have come to call "Big Data," can be analyzed in order to obtain valuable information that can then be turned into actions. For example, analyzing data from wearable technologies could help predict the type of health care problems a population will experience in the future.

One source of data used for medical and pharmaceutical research is anonymized health data. IQVIA Biotech (**www.iqviabiotech.com**) is a company that markets EMR software. When physicians and clinics have given permission, the company strips names and other personal information from data that have been provided and sells the data to the pharmaceutical industry. Such anonymized data are not covered by privacy legislation.

Sources: Compiled from Z. Khayat, "Time to Reinvent Health-Care for the Digital Age," *Toronto Star*, January 19, 2016; J. Chilibeck, "Group Still Backs Electronic Medical Records," *Telegraph-Journal*, February 9, 2015; A. Rankin, "At Least 865 Privacy Breaches of Nova Scotia Medical Records in the Past Year: Watchdog," *The Chronicle Herald*, June 5, 2019; The Canadian Press, "Doctors Snooped on Humboldt Broncos' Records, Privacy Commissioner Finds," CBCNews.ca, February 11, 2019; S. Spithoff, "Medical-Record Software Companies Are Selling Your Health Data," *Toronto Star*, February 20, 2019.

Questions

1. Discuss the ethics and the legality of selling anonymized health data.
2. Discuss the ethics and the legality of a doctor accessing the EMR of a famous sports team member.
3. How does a privacy policy help health care providers protect the privacy of EMR data?