Ethics and Privacy

CHAPTER OUTLINE	LEARNING OBJECTIVES
3.1 Ethical Issues	**3.1** Describe ethics, 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

MIS Marriott Blocks Guests' Wi-Fi Access

In many ways, technology is disrupting profitable services that hotels previously provided to their guests, causing hotels to lose these sources of revenue. Consider these examples:

- *Phone calls:* Disrupted by smartphones (see Chapter 10) and Voice-Over Internet Protocol (see Chapter 4);
- *Internet access:* Disrupted by personal Wi-Fi hotspots on smartphones and Mi-Fi (see Chapter 10);
- *Premium television:* Netflix (**www.netflix.com**), Hulu (**www.hulu.com**), Amazon Prime (**www.amazon.com/prime**), and customers streaming their own TiVo (**www.tivo.com**) recordings have replaced in-room, on-demand movies and some premium sporting events.
- *Room service:* Disrupted by Seamless (**www.seamless.com**) and Eat24 (**http://eat24.com**), who deliver food to your door.
- *Laundry and dry cleaning pick-up:* Disrupted by Washio (**www.getwashio.com**), Postmates (**http://postmates.com**), and the mobile websites of local cleaners themselves who offer pick-up and delivery.
- *Honor bar:* Disrupted by apps such as Instacart (**www.instacart.com**) that deliver drinks and snacks to your door, possibly for a lower cost than the compact refrigerator in hotel rooms.

To avoid losing revenue, hotels have been forced to devise strategies to compete with these services. Consider hotel chain Marriott (**www.marriott.com**). Wireless connection rates for Marriott start at $14.95 per day. For $19.95, guests receive "enhanced high-speed Internet," which includes video chatting, downloading large files, and streaming video. Rather than pay these expensive charges, many guests use their data allotment from their cell phone providers. Marriott was also charging conference organizers and exhibitors between $250 and $1,000 per access point to use the hotel's Wi-Fi connection.

Marriott attempted to maintain its Internet revenues by blocking Wi-Fi access in its hotels' conference areas. Unfortunately for Marriott, this policy generated more problems than income. In 2013, a conference attendee at the Gaylord Opryland Hotel in Nashville, Tennessee—which is managed by Marriott—discovered that the hotel was jamming Wi-Fi devices in its ballrooms, although it was providing access in the guest rooms. The guest complained to the Federal Communications Commission (FCC; **www.fcc.gov**).

In response, the FCC launched an investigation. In 2014, the agency concluded that Marriott had blocked personal hotspots and was therefore in violation of the Communications Act. The FCC fined the hotel chain $600,000 for these violations. Marriott also had to submit compliance reports to the agency for three years.

Marriott defended its policies by claiming that its objective was to protect its guests from rogue wireless hotspots that could cause degraded service, cyberattacks, and identity theft. The company further contended that the Opryland Hotel's actions were lawful.

In August 2014, Marriott petitioned the FCC to change the Communications Act so the company could continue to block Wi-Fi services in its hotels' conference spaces. The hotel chain asserted this practice

was necessary to prevent attendees from launching cyberattacks on the company's network. Many customers were outraged by the petition, claiming that Marriott's request was an attempt to ban Wi-Fi access in hotel rooms and lobbies as well as in conference rooms.

In December 2014, Microsoft, Google, the Consumer Electronics Association (**www.ce.org**), and others filed comments with the FCC opposing Marriott's Wi-Fi blocking plan. These companies noted that Marriott and other hotels make large amounts of money by charging businesses and individuals expensive rates to connect to the Internet in conference halls and meeting rooms. They contended that these policies were against the public interest, illegal, and malicious. They further charged that the security claims being made by Marriott were misleading. In response to negative publicity, in January 2015, Marriott issued a statement announcing that it would not block Wi-Fi at any hotel for any reason.

Meanwhile, in a strongly worded statement released the same month, the FCC asserted it would aggressively investigate and act upon unlawful intentional interference with Wi-Fi access in any establishment. Several months later, the commission fined Smart City Holdings (**www.smartcity.com**) $750,000 for blocking Wi-Fi access at a number of convention centers served by the company in order to force customers to use the company's own, expensive Wi-Fi options.

Unfortunately, an examination of complaints submitted to the FCC shows that Wi-Fi hotspot blocking is continuing. Since the fall of 2014, the FCC has levied $2.1 million in fines to organizations that have blocked patrons' portable Wi-Fi hotspots. For example, the FCC fined systems integration firm M.C. Dean (**www.mcdean.com**) for blocking consumers' Wi-Fi connections.

Sources: Compiled from B. Brown, "Wi-Fi Hotspot Blocking Persists Despite FCC Crackdown," *Network World*, March 10, 2016; C. Elliott, "The FCC Is Cracking Down on Hotels' Wi-Fi Blocking," *Fortune*, November 4, 2015; A. Lee, "Marriott Ends Its Bid to Kill Your Wi-Fi Hotspot," *ReadWrite*, February 2, 2015; D. Murphy, "Marriott Abandons FCC Petition for Hotel Wi-Fi Blocking," *PC Magazine*, February 1, 2015; M. Moon, "Marriott Is No Longer Fighting for Permission to Block Wi-Fi Hotspots," *Engadget*, January 31, 2015; "FCC to Marriott: Never Try to Block Wi-Fi Again," *CNN Money*, January 27, 2015; B. Brown, "FCC Calls Blocking of Personal Wi-Fi Hotspots 'Disturbing Trend,'" *Network World*, January 27, 2015; "Marriott Hotels Do U-Turn over Wi-Fi Hotspot Blocks," *BBC News*, January 15, 2015; "Marriott: You Win, We Won't Block Wi-Fi," *CNN Money*, January 15, 2015; "Marriott Is Bad, and Should Feel Bad," *The Economist*, January 6, 2015; "Should Hotels Be Allowed to Block Competing Wi-Fi?" *Consumer Traveler*, October 6, 2014; "How This Hotel Made Sure Your Wi-Fi Hotspot Sucked," *ReadWrite*, October 4, 2014; K. Knibbs, "The FCC Fined Marriott $600,000 for Blocking Guests' Wi-Fi," *Gizmodo*, October 3, 2014; www.marriott.com, www.fcc.gov, accessed August 31, 2016.

Questions

1. Discuss the ethicality and legality of Marriott's decision to block Wi-Fi access in conference centers in its hotels.
2. After the FCC found that Marriott had broken the law, did the hotel chain manage the situation correctly? Why or why not? If not, then how should Marriott have handled the situation? That is, what could the hotel chain have done better?
3. Describe the privacy implications of Marriott's trying to force guests to use its Wi-Fi access point.

Introduction

The chapter-opening case about Marriott blocking Wi-Fi access addresses the two major issues you will study in this chapter: ethics and privacy. 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. For example: Are the actions of Marriott ethical? Did Marriott violate the privacy of its guests? The answers to these questions are not straightforward. In fact, IT has made finding answers to these questions even more difficult.

You will encounter numerous ethical and privacy issues in your career, many of which will involve IT in some manner. This chapter provides insights into how to respond to these 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.

For example, suppose your organization decides to adopt social computing technologies (which you will study in Chapter 8) 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.

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 behavior. 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. 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 four 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, 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 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, healthcare, 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-defense.

If we combine these five standards, we can develop a general framework for ethics (or ethical decision making). This framework consists of five steps:

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?
   Does this issue involve more than simply legal considerations? If so, then in what way?
2. Get the facts:
   What are the relevant facts of the situation?
   Do I have sufficient information to make a decision?
   Which individuals or groups have an important stake in the outcome?
   Have I consulted all relevant persons and groups?

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)

4. Make a decision and test it:

   Considering all the approaches, which option best addresses the situation?

5. 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?

Now that we have created a general ethical framework, we will 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.

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 many instances, then, 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.

FIN ACCT We have witnessed a large number of extremely poor ethical decisions, not to mention outright criminal behavior, at many organizations. During 2001 and 2002, three highly publicized fiascos occurred at Enron, WorldCom, and Tyco. At each company, executives were convicted of various types of fraud for using illegal accounting practices. These actions led to the passage of the Sarbanes–Oxley Act in 2002. Sarbanes–Oxley requires publicly held companies to implement financial controls and company executives to personally certify financial reports.

Then, the subprime mortgage crisis exposed unethical lending practices throughout the mortgage industry. The crisis also highlighted pervasive weaknesses in the regulation of the U.S. financial industry as well as the global financial system. It ultimately contributed to a deep recession in the global economy. Along these same lines, financier Bernie Madoff was convicted in 2009 of operating a Ponzi scheme and sentenced to 150 years in federal prison. Several of Madoff's employees were also convicted in 2014.

Unfortunately, ethical misbehavior continues. Consider Wells Fargo bank (**www.wellsfargo.com**). In 2016, authorities found that bank employees had created approximately 2 million fake customer checking and credit card accounts without their knowledge. Bank employees had created the accounts under pressure from supervisors to meet daily account quotas. The bank then charged customers at least $1.5 million in fees for the fake accounts. Not only were the bank's victims charged overdraft and maintenance fees, but their credit scores were lowered for not staying current on accounts that they did not even know about.

Wells Fargo fired some 5,300 employees. The bank was also ordered to pay $185 million in fines, which is a very small amount compared with the $5.6 billion that the bank earned in the second quarter of 2016. Furthermore, in October 2016, Wells Fargo CEO John Stumpf stepped down from his position.

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 misuse of information technology at Volkswagen led to a global scandal.

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:

- HRM Should organizations monitor employees' web surfing and e-mail?
- MKT Should organizations sell customer information to other companies?
- HRM 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.

IT's About Business 3.2 illustrates the ethical (and privacy) issues surrounding the European Court of Justice's decision that implemented the "right to be forgotten" in the European Union.

IT's About Business 3.1

Volkswagen and the "Diesel Dupe"

MIS

Beginning in 2009, German car manufacturer Volkswagen (VW; **http://en.volkswagen.com**) launched a global marketing campaign promoting the low emissions of its diesel cars. During this period, global sales of VW diesel cars increased noticeably, and the vehicles won several environmental awards. The low emissions became a critical selling point as consumers and governments became increasingly concerned with pollution and global warming.

On September 18, 2015, the U.S. Environmental Protection Agency (EPA; **www.epa.gov**) sent a notice of violation of the 1970

Clean Air Act to VW. The agency charged that VW had installed software in millions of its diesel cars that could sense when the cars were undergoing emissions testing and then could alter the performance to meet federal standards.

Essentially, Volkswagen had intentionally programmed these diesel engines to activate certain emissions controls only during laboratory emissions testing. During this testing, cars are usually placed on a stationary device called a dynamometer. The programming caused the vehicles' output of pollutants known as nitrogen oxides to meet U.S. emissions standards during laboratory testing. However, during actual driving the software shut down the emissions controls. As a result, the cars provided better performance and fuel economy. However, they also produced up to 40 times more nitrogen oxides. Approximately 11 million cars worldwide, manufactured between model years 2009 and 2015 included this programming, known as a "defeat device."

The case against Volkswagen was solid. Volkswagen fully acknowledged that they had manipulated the vehicle emission tests after being shown the evidence of the defeat device. Both VW CEO Martin Winterkorn and VW America CEO Michael Horn admitted the charges were valid.

The consequences of the scandal, which became known as the "Diesel Dupe," have been severe. The issue wasn't limited to the United States. Authorities in Britain, Canada, Italy, France, Germany, and South Korea are among those investigating the automaker. These countries are questioning whether any of the emissions testing of VW vehicles was legitimate.

The EPA announced that should the allegations be proved, VW could face fines of up to $37,500 per vehicle, for a total of approximately $18 billion. On September 20, 2015, the company officially stopped selling affected diesel vehicles.

Shortly thereafter, VW announced plans to repair up to 11 million vehicles affected by the scandal. It was unclear whether the repairs would include both software and hardware modifications. The recall began in January 2016, with all of the affected cars projected to be fixed by the end of that year. The carmaker earmarked $18 billion to settle the worldwide costs of the recall, fines, and other repercussions. Of this total, $10 billion were for the company's settlement with car owners in the United States. In addition, Volkswagen established an online service in which customers can learn if their car is impacted based on the car's vehicle identification number (VIN).

The timing of the emissions scandal was significant, because the sales of diesel vehicles had already been declining. In Europe, the impact of the scandal could be devastating, perhaps prompting consumers to switch to gasoline-powered cars.

On September 23, 2015, VW CEO Martin Winterkorn resigned, although he denied any personal wrongdoing. It remained unclear which company executives knew what and when they knew it, although the German newspaper *Der Spiegel* reported that at least 30 people in management positions at VW were aware of the deceit for years. VW denied this allegation.

In November 2015, the EPA announced that it was investigating Audi and Porsche for allegedly using defeat devices on their diesel automobiles. The costs of the Diesel Dupe were to blame for VW's first quarterly loss in 15 years as the company suffered a large writedown. In fact, Volkswagen's stock lost up to 40 percent of its value after the scheme was discovered.

Hundreds of class-action lawsuits were filed in the United States on behalf of Volkswagen owners, claiming fraud and breach of contract. The lawsuits claimed that diesel vehicles will be worth less money because they will need to be fixed to conform to pollution regulations, due to expected reductions in horsepower and fuel efficiency. By the end of that month, the resale value of the affected cars in the United States had declined between 5 and 16 percent, based on used car auction prices listed in the Kelley Blue Book (**www.kbb.com**).

In mid-2016, Volkswagen announced it would settle U.S. diesel emissions claims to a maximum of $14.7 billion. The agreement includes paying up to $10.03 billion to purchase cars with the cheating software at their values before the scandal. The car buybacks began in the fall of 2016. However, the U.S. settlement applies to just a portion of the 11 million affected diesel vehicles worldwide. Furthermore, Volkswagen could still be fined up to $45 billion by the U.S. Environmental Protection Agency for violations of the Clean Air Act.

In November 2016, Volkswagen announced an agreement with employees to eliminate some 30,000 jobs around the world. The automaker stated that it needed to save $3.9 billion to help defray the costs attributed to the "diesel dupe."

Perhaps the most significant element of the VW scandal is that the workaround to improve emissions during testing was coded into the software that controlled the vehicles' emissions. Cheating that occurs within the software can be difficult to pick up. The significance of the software cheating could have ramifications in other situations, as similar software is being used in everything from voting machines to electric power distribution. As software becomes more pervasive, these technologies need to be more trustworthy and transparent.

Sources: Compiled from C. Rauwald, "VW Said to Cut 30,000 Jobs, Save $3.9 Billion in Labor Pact," *Bloomberg.com*, November 18, 2016; K. Mehrotra and M. Fisk, "VW Buybacks to Begin under $14.7 Billion Diesel-Cheat Accord," *Bloomberg*, October 25, 2016; H. Tabuchi and J. Ewing, "Volkswagen to Pay $14.7 Billion to Settle Diesel Claims in U.S.," *New York Times*, June 27, 2016; D. Francis, "Analysis: Volkswagen's Emissions Cheat Headache Just Got Worse," *Chicago Tribune*, May 17, 2016; G. Smith and R. Parloff, "Hoaxwagen," *Fortune*, March 7, 2016; R. Hotten, "Volkswagen: The Scandal Explained," *BBC News*, December 10, 2015; T. Pollard, "Volkswagen's Emissions 'Cheat' Software Scandal: An Explainer," *Car magazine*, November 25, 2015; "VW Emissions Scandal: U.S. Regulators Find More Cars with Cheat Tests," *BBC News*, November 3, 2015; N. Bomey, "House Slams 'Arrogance' of VW; CEO Says No Buyback Planned," *USA Today*, October 9, 2015; M. Spector and A. Harder, "Volkswagen U.S. CEO Says He Didn't Know in 2014 of Emissions Defeat Devices," *Wall Street Journal*, October 9, 2015; D. Ivory and K. Bradsher, "Regulators Investigating 2nd VW Emissions Program on Emissions," *New York Times*, October 8, 2015; K. Johnson and J. Willhite, "Emissions Scandal Puts Volkswagen CFO in the Hot Seat," *Wall Street Journal*, September 28, 2015; B. Schneier, "VW Scandal Could Just Be the Beginning," *CNN*, September 28, 2015; T. Claburn, "Volkswagen's New CEO Brings Software Know-How," *InformationWeek*, September 26, 2015; T. Claburn, "Volkswagen: 11 Million Cars Used Deceptive Emissions Software," *InformationWeek*, September 22, 2015; J. Ewing and C. Davenport, "Volkswagen to Stop Sales of Diesel Cars Involved in Recall," *New York Times*, September 20, 2015; W. Boston, A. Harder, and M. Spector, "Volkswagen Halts U.S. Sales of Certain Diesel Cars," *Wall Street Journal*, September 20, 2015; http://en.volkswagen.com, accessed October 31, 2016.

Questions

1. **Describe the role that information technology played in Volkswagen's Diesel Dupe.**
2. **The fundamental tenets of ethics include responsibility, accountability, and liability. Discuss each of these tenets as it applies to the Volkswagen scandal.**

IT's About Business 3.2

Do You Have the Right to Be Forgotten?

MIS

In 1998, a lawyer in Spain undergoing financial trouble had to put a piece of property he owned up for auction. This was reported in a Spanish newspaper, *La Vanguardia.* Soon after, the lawyer cleared his debts, but the newspaper article was still accessible online when someone searched his name on Google.

The lawyer in 2010 insisted that the newspaper take down the online articles and that Google delete the links to them. The Spanish Data Protection Agency (**www.agpd.es**) turned down his request for the newspaper to remove the articles, but it allowed his request that Google not link to them. In 2014, the Spanish agency's decisions were upheld by the European Court of Justice, the superior court for countries of the European Union. The Court of Justice decision went even further, protecting the rights of everyone in member countries to have Google take down links to any information about them that was deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed."

In effect, then, the European Union's highest court had ruled that citizens have a "right to be forgotten" on the web and can therefore force Google and other search engines to remove outdated or "irrelevant" links about their personal histories from search results. The "right to be forgotten" is the right for individuals to request that information about them be taken offline after it's no longer relevant. Specifically, individuals can ask Google to remove links to news articles, court judgments, and other documents in search results for their name. The court's decision empowers individuals to ask Google or other search operators to take down links to web pages that are published by third parties, such as newspapers, that contain information relating to them. The decision does not require that the article or the website be removed or altered by the original publisher. Rather, the link to this content must be removed.

Subsequent to the courts' decision, requests to remove embarrassing and negative links exploded. By September 2015, roughly 250,000 requests had been submitted. In one instance, a former politician seeking reelection requested the removal of links to articles about his poor behavior while in office. In another scenario, a physician sought to erase negative online reviews.

Not surprisingly, the "right to be forgotten" has created a great deal of controversy. Privacy advocates defend the decision as a reclamation of privacy rights. Opponents contend that, were this policy to be implemented, people's search results would come to resemble official biographies that record only the facts that individuals want other people to know. That situation could be dangerous. Opponents further argue that the court decision fails to identify which criteria the search engines should use to decide which requests to honor. The ruling also does not require that embarrassing material—revealing photographs, court documents, or gossip—be erased from the Internet, just from search results.

While the European Court of Justice decision was clear on granting the "right to be forgotten" to all citizens, it was unclear exactly how that would happen. The ruling called for a balance between the privacy rights of individuals and the rights of the public to information. But the decision by Europe's highest court is binding on the courts in member states, which must interpret it as best they can. Consequently, privacy and the "right to be forgotten" could vary from one country to another, potentially generating a great deal of confusion and uncertainty.

As of September 2016, it was not clear how search engines such as Google needed to comply with the EU ruling. Google has a page that allows users to request that certain links be deleted, based on copyright and similar claims. In March 2016, Google announced that it would apply the right to be forgotten to all European Union searches.

Google has implemented a two-part system for complying with the court's decision. The first part launched software to remove links. This software enables Google to use its existing system to delete copyrighted and trademarked items.

In the second part, Google developed an administrative system to collect and respond to requests to remove links. Internet users in all of the EU countries covered by the decision can fill out a form in one of 25 languages through the local Google site in that country. (The form is not available through the main Google.com homepage based in the United States.) People fill in their name and the links they want removed, and must also explain why they feel the information is objectionable, such as that it is no longer relevant or is out of date. If Google agrees with the petitioner, it notifies the webmaster of the sites in question and allows those sites to state their reasons for keeping the link.

Each request for link deletion is reviewed by a team of lawyers, paralegals, and other experts put together by Google. The reviewers are mainly looking at whether the petitioner is a public or private figure, if the information is from a reliable news organization or government agency, if the petitioner themselves originally published the item, and whether the link relates to political speech or criminal charges.

Meanwhile, another dispute has arisen concerning the scope of the court's ruling. Specifically, France's data regulators determined that it is not sufficient for Google to remove a result from its European search pages (Google.fr, Google.de, etc.). Instead, the company must remove links worldwide by deleting them from its "Google.com" version as well. In response, Google informed the French regulators in September 2015 that it would not implement "right to be forgotten" requests on a worldwide basis. The company argued that although the right to be forgotten is the law in Europe, it is not the law globally. Furthermore, content that is illegal in one country can still be legal in other countries.

Google launched its Google forget program in the United States without fanfare. Users may go to **http://myactivity.google.com** to view the history of their web searches, YouTube viewing, and other activities they have done on Google platforms.

Sources: Compiled from E. Schuman, "Google Quietly Brings Forgetting to the U.S." *Computerworld,* July 13, 2016; C. Lecher, "Google Will Apply the 'Right to Be Forgotten' to All EU Searches Next Week," *The Verge,* March 4, 2016; M. Stern, "UK Orders Google to Censor Links to Articles about 'Right to Be Forgotten,' Removals," *Slate,* August 21, 2015; F. Manjoo, "'Right to Be Forgotten' Online Could Spread," *New York Times*, August 5, 2015; A. Hern, "Google Says Non to French Demand to Expand Right to Be Forgotten Worldwide," *The Guardian,* July 30, 2015; J. Roberts, "The Right to Be Forgotten from Google? Forget It, Says U.S. Crowd," *Fortune,* March 12, 2015; H. Maycotte, "America's 'Right to Be Forgotten' Fight Heats Up," *Forbes,* September 30, 2014; J. Toobin, "The Solace of Oblivion," *The New Yorker,* September 29, 2014; "Internet Privacy: Do Users Have a 'Right to be Forgotten'?" *The Week,* May 30, 2014; "Google's Legal Blow: What the 'Right to Be Forgotten' Means," *Wall Street Journal,* May 13, 2014; D. Lee, "What Is

the 'Right to Be Forgotten'?" *BBC News*, May 13, 2014; T. Claburn, "Google Ordered to 'Forget,'" *InformationWeek*, May 13, 2014; www.google.com, accessed September 7, 2016.

Questions

1. Describe the advantages to individuals of the "right to be forgotten" policy. Provide examples to support your answer.
2. What are the potential long-term disadvantages of the "right to be forgotten" policy? Provide examples to support your answer.
3. Describe the ethicality and legality of the "right to be forgotten" policy.
4. What are the privacy implications of the "right to be forgotten" policy?

TABLE 3.1 **A Framework for Ethical Issues** (Mason, R.O., "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), pp. 5–12.)

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, fidelity, 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 3.1 lists representative questions and issues for each of these categories. Online Ethics Cases also presents 14 scenarios that raise ethical issues. These scenarios will provide a context for you to consider situations that involve ethical or unethical behavior.

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 the U.S. states and by the federal government, either by statute or in common law.

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, such as LexisNexis (**www.lexisnexis.com**), ChoicePoint (**www.choicepoint.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; financial data; and police, criminal, and motor vehicle records. They 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 them to companies that want to know their customers better, a process called *customer intimacy.*

Electronic Surveillance

According to the American Civil Liberties Union (ACLU), tracking people's activities with the aid of information technology has become a major privacy-related problem. The ACLU notes that this monitoring, or **electronic surveillance**, is rapidly increasing, particularly with the emergence of new technologies. Electronic surveillance is conducted by employers, the government, and other institutions.

Americans 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 now everywhere. 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 license 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 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 10, smartphones can now record video, take pictures, send and receive e-mail, 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. 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 behavior. One marketing analyst has predicted that your experience in every store will soon be customized.

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. He or she could then quickly profile you (find out information about where you live, your employment, etc.) 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 his or her own. One privacy attorney 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 500 feet. However, to regulate small, low-flying drones, the Federal Aviation Administration (FAA; www.faa.gov) has assumed authority all the way down to the ground.

Consider this example. You see a drone flying about 100 feet above your backyard and you suspect that it is spying on you. Who is flying it? Whom are you going to sue? And if you do sue, how are you going to prove that the drone was spying on you?

In the fall of 2016, it was not clear which government agencies, if any, were responsible for addressing drone-related privacy concerns. The FAA has declined to make rules. The Federal Trade Commission (FTC; www.ftc.gov), the U.S. government's primary consumer privacy agency, is still exploring the drone privacy issue. IT's About Business 3.3 illustrates another type of surveillance technology employed by law enforcement agencies.

HRM 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' e-mail 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.

IT's About Business 3.3

The StingRay

MIS

The Federal Communications Commission (FCC; **www.fcc.gov**) has authorized the Harris Corporation (**www.harris.com**), a defense contractor, to sell a surveillance device that tracks cell phones. The StingRay, the size of a suitcase, functions as a cell tower, emitting signals that can dupe phones up to one mile away into sending identifying data. The device can also harvest information from texts, calls, e-mails, and other phone activity. Harris routinely rejects requests to talk about the StingRay.

The StingRays are popular among local law enforcement agencies, costing them millions of dollars. Agencies have spent part of the more than $35 billion in grants from the Department of Homeland Security (DHS; **www.dhs.gov**) earmarked for cities, counties, and states to fight terrorism and prepare for emergencies and disasters. Money for the StingRay also comes from federal drug enforcement grants and nonprofit organizations that have collected donations for local police departments.

The American Civil Liberties Union (ACLU; **www.aclu.org**) claims that cell phone surveillance equipment is owned by at least 51 police forces in 21 states, while other local law enforcement agencies borrow the equipment from federal agencies such as the Federal Bureau of Investigation (FBI; **www.fbi.gov**) and the Drug Enforcement Administration (DEA; **www.dea.gov**).

The StingRay technology is a closely guarded secret. The FBI says it must be kept confidential or else criminals and terrorists could try to get around it. As a result, law enforcement agencies must sign a confidentiality agreement before buying a StingRay. There is controversy that the nondisclosure agreements make government practices less transparent. Legal experts claim that these agreements bring up important privacy and constitutional issues.

Because the StingRay can monitor all cell phones within range, civil rights groups say that it violates the privacy of innocent people, not just potential criminals who are being targeted. Furthermore, until 2015, police officers could use the StingRay without informing anyone or having to obtain approval from judges, as they would have to do to obtain phone records.

The secrecy over StingRay has led to unintended consequences. For example, reporters have uncovered cases in which the police used a StingRay as part of their routine police work, including locating petty criminals, and then did not reveal the cell phone surveillance tactic to the suspects, their lawyers, or even the judges hearing the cases.

The use of StingRays has stirred up a hornet's nest regarding procedural issues in the justice system. Suspects usually have the right to know what evidence was collected against them and to file complaints about the legality of the method used to gather that evidence. While police have used StingRays against those suspected of everything from petty crimes to murder, records show that that evidence has been routinely hidden or obscured from the suspects in court. In fact, many such suspects were never even prosecuted. About one-third of cases involving evidence from StingRays are thrown out, even those involving stolen cell phones. Only half of those who were prosecuted are convicted. Even though state law requires that defense attorneys be informed about electronic surveillance, many say they weren't told that a StingRay was involved.

In September 2015, the U.S. Department of Justice (DOJ; **www.doj.gov**) mandated that federal agencies had to obtain search warrants to use StingRays. To enhance privacy protections, the policy requires that data gathered through a StingRay be deleted when the cell phone is found. Furthermore, all data must be deleted at least once per day. The directive also forbids federal agencies from using StingRays during criminal investigations to gather data from communication, such as e-mails, texts, contact information, and photos. Significantly, the ACLU notes that the policy applies only to federal agencies and not the many state and local police departments that have bought StingRays with federal money. In that sense, the ACLU argues, the policy is too limited.

In response to the objections of the ACLU and the DOJ, federal officials stated that StingRays allow them to monitor dangerous criminals. For example, FBI Director James Comey asserted that the agency uses StingRay to find killers, kidnappers, drug dealers, missing children, and pedophiles.

In one unsettling example, when the Indian government bought such devices, government officials began monitoring the calls of opposition-party politicians. One intelligence official told an Indian newspaper that they could keep tabs on anyone. By 2010, top government officials admitted that India's entire cellular network was breached. One privacy advocate noted that India gives us a look at what will happen in America once these devices become ubiquitous.

Another problem with such surveillance devices is that they are becoming cheaper and easier to manufacture, enabling the technology to be in the hands of the public. Ultimately, it could be someone you know who hacks into your smartphone.

A market has developed for countermeasures to these devices. For example, the SnoopSnitch is an inexpensive, open source Android app that sweeps mobile data, looking for fake cellular sites. A more expensive countermeasure is the $3,500, highly secure CryptoPhone by ESD America (**http://esdamerica.com**).

Sources: Compiled from R. Kolker, "The Democratization of Surveillance," *Bloomberg BusinessWeek,* March 14–20, 2016; R. Brandom, "The Dragnet," *The Verge,* January 13, 2016; W. Ashford, "U.S. Cracks Down on Mobile Phone Tracking by Federal Agencies," *Computer Weekly,* September 4, 2015; N. Woolf, "2,000 Cases May Be Overturned Because Police Used Secret StingRay Surveillance," *The Guardian,* September 4, 2015; K. Zetter, "The Feds Need a Warrant to Spy with StingRays from Now On," *Wired,* September 3, 2015; B. Heath, "Police Secretly Track Cellphones to Locate Even Petty Criminals," *USA Today,* August 25, 2015; C. Farivar, "In Rare Move, Silicon Valley County Gov't Kills Stingray Acquisition," *Ars Technica,* May 7, 2015; J. Fenton, "Baltimore Judge Allows Police Use of StingRay Phone Tracking in Murder Case," *The Baltimore Sun,* April 20, 2015; K. Klonick, "Stingrays: Not Just for Feds!" *Slate,* November 10, 2014; P. Robison, "Another Privacy Concern: Police Spying on Cell Phones," *Bloomberg BusinessWeek,* October 16, 2014; M. Richtel, "A Police Gadget Tracks Phones? Shhh! It's Secret," *New York Times,* March 16, 2015; K. Zetter, "Florida Cops' Secret Weapon: Warrantless Cellphone Tracking," *Wired,* March 3, 2014; R. Gallagher, "Meet the Machines that Steal Your Phone's Data," *Ars Technica,* September 25, 2013; www.esdamerica.com, accessed October 30, 2016.

Questions

1. As technology advances, what are the implications for electronic surveillance?
2. Discuss the legality and ethicality of the police using StingRays for ordinary crime.
3. Discuss the legality and ethicality of federal law enforcement agencies using StingRays to find terrorists.
4. Are your answers to Questions 2 and 3 different? Explain your reasoning.

In one organization, the chief information officer (CIO) 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 chief executive officer (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 nation, the United States 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

Modern institutions store information about individuals 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 (Internal Revenue Service, your state, 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?

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 8). 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 ethical issue in the United States and throughout the world.

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. The vast majority of U.S. firms 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.

New information technologies can also present serious privacy concerns. IT's About Business 3.4 shows how life and automobile insurance companies use technology to track individual policy holders.

IT's About Business 3.4

Tracking Data Impacts Life and Automobile Insurance

MIS

Life Insurance. Only 4 in 10 households in the United States own individual life insurance policies, the lowest rate in the past half-century. As a result, John Hancock (**www.johnhancock.com**) is offering a new type of life insurance program, which the insurer hopes will increase sales.

MKT Life insurance policies are typically underwritten using a person's medical status at the time they apply for the policy. In this way, life insurance is a onetime process, unlike health insurance, which requires ongoing medical information to adjust premiums annually.

In its new program, John Hancock will price policies continuously for participating consumers. These customers must agree to continually share their medical data with Hancock. The insurer operates the program in conjunction with Vitality (**www.thevitalitygroup.com**), a global wellness company.

Similar programs launched by Vitality in other countries, including Australia, South Africa, and Singapore, have shown impressive results: Policyholders are motivated to improve their fitness to bring down their life insurance premiums. In a 2014 study, Vitality found that participants who had not been exercising but who underwent a fitness regime for three years saw a 13 percent drop in their health risk factors. Those who were active before the study but increased their fitness activities cut these factors by 22 percent over the three years.

Holders of the John Hancock life insurance policy through Vitality earn points for various fitness activities that are expected to increase their longevity. The more points they earn, the bigger the discount they receive on their premiums. Participants get a free Fitbit monitor and they may choose to upload their data to the insurance company. Policyholders receive 1,000 points for being a nonsmoker; 1,000 points for each reading in the "normal" range of cholesterol, glucose, and blood sugar; 3,120 points over a year for working out three times a week at a standard rate or twice a week at an advanced rate; and 400 points for getting a flu shot. Ten percent of earned points can be carried over to the next year.

All participants begin the program by paying a premium at the "gold" rate, which requires 7,000 points per year. The gold-level premium is reduced by about 9 percent over the regular premium. If over the course of the program a participant can't maintain gold status, their annual premium could go up by as much as 1.6 percent. If a participant achieves platinum status, which requires 10,000 points a year, the premium goes down by about 0.3 percent per year.

The program does yield concerns about the security of consumers' health information and whether it could be used in detrimental ways. For example:

- Would an insurance company penalize a policyholder whose Fitbit data shows they have symptoms of stress?
- What if insurance underwriters make mistakes or wrong assumptions in analyzing Fitbit data?
- What happens when insurance companies break the consumer protection rules in the Health Insurance Portability and Accountability Act (HIPAA)? Will they be fined and if so, how much?

Hancock's program also raises privacy concerns. Hancock responds by stating that consumers are not obliged to send the company any data that they are not comfortable with, although they will not accumulate points for data that they do not share.

And one final interesting question: For most life insurance policyholders, the older they are, the higher their risk. Therefore, why would anyone want to continuously price their policies when they could enjoy level premiums over the years (depending on the policy they purchased)?

Automobile Insurance. If you have a clean driving record, you may be overpaying for car insurance. That's because auto insurance companies base premiums on statistical averages for characteristics such as age, sex, marital status, location, and the type and age of the car. Some drivers get a discount based on how long they have gone accident-free.

Technology now enables drivers to get discounts on their auto insurance rates based on how they really drive, rather than on statistics. The strategy, called usage-based insurance, lets auto insurers monitor your driving in return for a yearly discount on your insurance premium, depending on your driving habits. You can opt in or out of the program.

The technology works like this. Drivers insert a device into the vehicle's diagnostic ports. The tool collects information from the onboard computer, such as the time of day, mileage, speed, and acceleration and braking rates. The tool then transmits these data to the auto insurance company through a cellular network.

State Farm (**www.statefarm.com**; Drive Safe), Progressive (**www.progressive.com**; Snapshot), and Allstate (**www.allstate.com**; Drive Wise) all offer usage-based automobile insurance. Let's take a closer look at Progressive's Snapshot product.

As with the other companies, Progressive drivers plug the device into their cars' data ports. Drivers can earn a discount if their data show a good driving record after 30 days. The tracking lasts six months, after which drivers return the tool back to the company. They can be eligible to receive a discount of up to 30 percent from then on. Progressive does not increase premiums based on any data it collects. Participation in the program is free.

Progressive's usage-based insurance program has been used by more than 1.4 million people, and about one-third continued with it. Of those who continued, about two-thirds qualified for a discount, usually from 10 percent to 15 percent. The program currently provides approximately 10 percent of the company's revenue.

As of the fall of 2016, none of the three auto insurers was collecting GPS data, so drivers' locations remained private. Furthermore, the three companies were not raising rates on drivers whose data turned out to be poor.

Privacy is a major worry with these programs. There is a fear that data may be fed to people outside the insurance company or that the data may be used for purposes other than originally intended. For example, auto insurers may have little interest in a driver's location at a certain time on a certain day, but if insurers start to collect and store that data, it may some day be subpoenaed by lawyers. Another privacy concern is that the auto insurers will provide driver information to a central industry database. In that case, drivers would have a "driver score" similar to the credit score that FICO (**www.myfico.com**) maintains. Therefore, when drivers look

to purchase automobile insurance, their driver scores will impact the premium cost.

Sources: Compiled from "Usage-Based Insurance and Telematics," *National Association of Insurance Commissioners*, June 6, 2016; "Usage-Based Auto Insurance, Slow at First, Picking Up Speed," *Insurance Journal*, May 12, 2016; R. Bloink and W. Byrnes, "Life Insurance Carriers Offer Premium Cuts for Individual Wellness Policies," *ThinkAdvisor*, January 6, 2016; "Automotive Usage-Based Insurance (UBI) Market Report 2015–2025 Insurance Telematics and the Connected Car—Reportlinker Review," *PR Newswire*, October 7, 2015; C. Tuohy, "Health Data Leads to Floating Premiums in Some Life Policies," *InsuranceNewsNet*, July 10, 2015; A. Dart, "The Case for Connected Wearables in Life Insurance," *CSC*, July 3, 2015; M. Mapp, "John Hancock's Bargain: Give Us More Data, You Pay Less in Rates," *CNBC*, April 19, 2015; T. Bernard, "Giving Out Private Data for Discount in Insurance," *New York Times*, April 8, 2015; K. Calamur, "John Hancock Hopes You'll Trade Activity Data for Insurance Discounts," *NPR.org*, April 8, 2015; R. Lieber, "Lower Your Car Insurance Bill, at the Price of Some Privacy," *New York Times*, August 15, 2014; A. Tanner, "Data Monitoring Saves Some People on Car Insurance, But Some Will Pay More," *Forbes*, August 14, 2013; C. Woodyard and J. O'Donnell, "Your Car May Be Invading Your Privacy," *USA Today*, March 24, 2013; J. Anderson, "Data-Tracking Technology Can Help Lower Your Car Insurance," *Kiplinger*, September 30, 2011; www.johnhancock.com, www.thevitalitygroup.com, accessed September 1, 2016.

Questions

1. Describe the advantages of continuous life insurance underwriting and usage-based automobile insurance to the consumer.
2. Describe the advantages of continuous life insurance underwriting and usage-based automobile insurance to the company.
3. Would you be willing to participate in continuous life insurance? Why or why not?
4. Would you be willing to participate in usage-based automobile insurance? Why or why not?
5. Are your answers to Questions 3 and 4 different? If so, why?

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. 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.

One privacy tool available to consumers is the *Platform for Privacy Preferences* (P3P), a protocol that 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 sites they visit. It also allows visitors to compare a site's privacy policy to the visitors' preferences or to other standards, such as the Federal Trade Commission's (FTC) Fair Information Practices Standard or the European Directive on Data Protection.

Table 3.2 provides a sampling of privacy policy guidelines. The last section, "Data Confidentiality," refers to security, which we consider in Chapter 7. 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 3.5.

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 overcome this problem. In 1998, the European Community Commission (ECC) issued guidelines to all of its member countries regarding the rights of individuals

TABLE 3.2 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.

to access information about themselves. The EU data protection laws are stricter than the U.S. laws and therefore could create problems for the U.S.-based multinational corporations, which could face lawsuits for privacy violations.

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 U.S. satellite to a British corporation, which country's privacy laws control the data, and at what points in the transmission?

IT's About Business 3.5

The Ashley Madison Breach

MIS

The Problem

Launched in 2001, Ashley Madison (**www.ashleymadison.com**) is an online dating and social network service based in Canada. Unlike most dating services, Ashley Madison marketed specifically to people who are married or in a committed relationship but are seeking an outside relationship. In mid-2015, the site claimed 39 million members in 53 countries, and it generated an estimated $115 million in annual revenue.

Significantly, Ashley Madison purportedly allowed users to hide their account profiles for free. Users who wanted to delete their accounts had to pay a $19 fee. Ashley Madison assured its users that its "full delete option" removed all relevant data from the site: user profiles, all messages sent and received, site usage history, personally identifiable information, and photos.

On July 15, 2015, Ashley Madison was hacked by a group called "The Impact Team." The hackers claimed to have stolen personal information about the site's users, and it threatened to release names, addresses, search histories, and credit card numbers if the site did not immediately cease operations. The Impact Team claimed their demand was caused by Ashley Madison's failure to delete users' personal information following their invoiced requests to do so.

When Ashley Madison ignored the demand, The Impact Team launched its first data release on August 18, followed by a second release three days later. The second batch of data included Ashley Madison CEO Noel Biderman's personal e-mails.

The data, which first appeared on the Dark Web, were copied and made public on the open web. The Dark Web is the World Wide Web content that exists on networks that require encryption, specific software, or authorization to access. The Dark Web is not indexed by search engines, and it can be accessed only through

a browser called Tor (**www.torproject.org**). The Dark Web is an anonymous platform used to hide the activities of individuals such as dissidents in authoritarian regimes, cybercriminals, child pornographers, and drug traffickers.

Ashley Madison's Attempts at a Solution

Immediately following The Impact Team's announcement, CEO Biderman admitted the breach and asserted that the company was "working diligently and feverishly" to try to stop the spread of the leaked data. Ashley Madison released the following statement: "We are actively monitoring and investigating this situation to determine the validity of any information posted online. . . . We will continue to put forth substantial efforts into removing any information unlawfully released to the public, as well as continuing to operate our business." The company also delivered copyright takedown notices under the 1998 Digital Millennium Copyright Act (DMCA) to many sites, alleging that they were violating "intellectual property in the data." Many of the sites obeyed these notices.

Ashley Madison subsequently announced that it had secured its site. It labeled the hack an act of "cyberterrorism," and it apologized to its users. The company offered $500,000 (Canadian) to anyone with information that results in the identification of the hackers. Finally, the site announced that in the future it would delete user information free of charge, thus eliminating the $19 fee.

The Results

Both the site and its users experienced further damage from the attack. For example, spammers quickly began to extort people whose information was made public. One group, for example, sent e-mails to Ashley Madison users demanding one bitcoin (approximately $225) or their information would be revealed. The group gave the users one week before it exposed them. In addition to extortion, victims of the breach risk identity theft as well.

Extortion attempts resulting from the Ashley Madison breach continue. A group with a Ukrainian top-level Internet domain announced that on May 1, 2017 it would create a website called "Cheaters Gallery." The website promises to expose people who were caught in the breach unless they pay approximately $500 in bitcoins.

While the moral and ethical outrage surrounding the Ashley Madison hack has received most of the headlines, industry analysts maintain that the real issues are the assault on consumer privacy and the inability of businesses to protect their customers' data. Analysts further predict that in the future, businesses will likely be held far more accountable for data security than they have been in the past.

From a different perspective, private investigation firm Trustify (**www.trustify.info**) capitalized on the Ashley Madison breach by launching a service just after the attack that lets users search the data dump from the hackers. Trustify advertised its services to suspicious partners who were alarmed by a name that was released.

In July 2016, the U.S. Federal Trade Commission (**www.ftc.gov**) announced an inquiry into Ashley Madison's business practices. The new executive team at the company has announced several initiatives aimed at restoring the firm's reputation. First, the site has announced a new slogan: "Find Your Moment" rather than its previous slogan of "Life Is Short, Have an Affair." Second, the company states that it has deleted all fembots from its website, which are programs that enticed men by pretending to be women. Third, Ashley Madison now has a free feature to delete all user data from its website. Executives state that this option does now work.

By the fall of 2016, more than $1 billion in lawsuits had been filed against Ashley Madison, and CEO Biderman had stepped down. According to the official press release, the senior management team currently in place would continue to lead the company.

In December 2016, Ashley Madison agreed to a $1.7 million settlement with several U.S. states and the federal government. The company still faces the prospect of a class action lawsuit by irate customers.

Sources: Compiled from J. Pagliery, "Ashley Madison Agrees to $1.7 Million Settlement," *CNN*, December 14, 2016; N. Bomey, "Ashley Madison's New Slogan: 'Find Your Moment,' Not 'Have an Affair,'" *USA Today,* July 12, 2016; M. McPhate, "Ashley Madison Faces F.T.C. Inquiry Amid Rebranding," *New York Times,* July 5, 2016; R. Hackett, "CEO of Ashley Madison Parent Company Stepping Down," *Fortune,* August 28, 2015; R. King, "IBM Advises Companies to Keep Networks Free from Dark Web," *Wall Street Journal,* August 26, 2015; M. Slater-Robins, "Here's What Ashley Madison's $19 'Full Delete' Feature Actually Removes," *Business Insider UK,* August 26, 2015; W. Ashford, "Avid Life Media Offers Reward for Information on Ashley Madison Hack as Writs Loom," *Computer Weekly,* August 25, 2015; B. Krebs, "Who Hacked Ashley Madison?" *Krebs on Security,* August 26, 2015; L. Loeb, "Ashley Madison Fallout: Investigations, Lawsuits, Lessons," *InformationWeek,* August 26, 2015; A. Blake, "Ashley Madison Hack Could Cost Dating Site More than $1 Billion as Lawsuits Mount," *The Washington Times,* August 25, 2015; J. Greenberg, "Private Investigator Startup Exploits Ashley Madison Hack," *Wired,* August 25, 2015; B. Cole, "Will Data Privacy Finally Come to the Fore, Post Ashley Madison Hack?" *TechTarget,* August 21, 2015; H. King, "Ashley Madison Tries to Stop the Spread of Its Leaked Data," *CNN Money,* August 21, 2015; L. Segall, "Ashley Madison Users Now Facing Extortion," *CNN Money,* August 21, 2015; "Ashley Madison Probes Veracity of Data Leaked by Hackers," *CNBC,* August 19, 2015; C. Welch, "Ashley Madison's $19 'Full Delete' Option Made the Company Millions," *The Verge,* August 19, 2015; 765 xc, "Hackers Expose First Ashley Madison Users," *CBS News,* July 22, 2015; B. Krebs, "Online Cheating Site Ashley Madison Hacked," *Krebs on Security,* July 19, 2015; www.ashleymadison.com, accessed August 29, 2016.

Questions

1. **Discuss the legality and the ethicality of the Ashley Madison website.**
2. **Discuss the legality and the ethicality of the actions of the hackers who attacked the Ashley Madison website.**
3. **Discuss the legality and ethicality 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.**
4. **Discuss the legality and ethicality of the reporters who used hacked (stolen) information in their stories.**
5. **Discuss the legality and ethicality of the actions of Trustify.**
6. **Are there differences in your answers to the first five questions? If so, then describe them. How do you account for them?**
7. **What are the implications of the Ashley Madison breach for general privacy concerns regarding digital data?**

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.

The United States and the European Union share the goal of privacy protection for their citizens, but the United States takes a different approach. To bridge the different privacy approaches, the U.S. Department of Commerce, in consultation with the European Union, developed a "safe harbor" framework to regulate the way U.S. companies export and handle the personal data (e.g., names and addresses) of European citizens. See **www.export.gov/safeharbor** and **http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm**.

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?

ACCT 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 Generally Accepted Accounting Principles (GAAP). In fact, regulatory agencies, such as the SEC and the Public Company Accounting Oversight Board (PCAOB), require accounting departments to adhere to strict ethical principles.

FIN For the Finance Major

As a result of global regulatory requirements and the passage of Sarbanes–Oxley, 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 the Securities and Exchange Commission (SEC) and in all other public financial reports. Furthermore, financial managers are responsible for compliance with all applicable governmental laws, rules, and regulations.

MKT 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 9). 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 12) operations and tracking customers' online buying habits can expose unencrypted data to misuse or result in privacy violations.

POM 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 labor 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 labor costs?

HRM 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, e-mail, 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.

MIS 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. Describe ethics, 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 behavior.

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.

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

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.

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 his or her 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 behaviors.

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 codes See **privacy policies**.

privacy policies (also known as 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 (UAVs)) for electronic surveillance purposes in the United States.

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

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

Problem-Solving Activities

1. An information security manager routinely monitored web surfing among her company's employees. She 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.) She 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 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 rules 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/constitution/code.html**). Discuss the major points of this code. Is this code complete? Why or why not? Support your answer.
4. Access **www.eightmaps.com**. Is the use of data on this website illegal? Unethical? 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 e-mail?
7. Access **http://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.epubliceye.com**. 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 e-mail sent and received on university computers? Why or why not? Support your answer.

Chapter Closing Case

The Facebook Experiments

MIS

The Problem

Facebook (**www.facebook.com**) has long conducted digital experiments on various aspects of its website. For example, just before the 2012 election, the company conducted an experiment on the News Feeds of nearly 2 million users so that they would see more "hard news" shared by their friends. In the experiment, news articles that Facebook users' friends had posted appeared higher in their News feeds. Facebook claimed that the news stories being shared were general in nature and not political. The stories originated from a list of 100 top media outlets from the *New York Times* to Fox News. Industry analysts claim that the change may have boosted voter turnout by as much as 3 percent.

Next, Facebook decided to conduct a different kind of experiment that analyzed human emotions. The social network has observed that people's friends often produce more News Feed content than they can read. As a result, Facebook filters that content with algorithms to show users the most relevant and engaging content. For one week in 2012, Facebook changed the algorithms it uses to determine which status updates appeared in the News Feed of 689,000 randomly selected users (about 1 of every 2,500 Facebook users). In this experiment, the algorithm filtered content based on its emotional content. Specifically, it identified a post as "positive" or "negative" if it used at least one word previously identified by Facebook as positive or negative. In essence, Facebook altered the regular news feeds of those users, showing one set of users happy, positive posts while displaying dreary, negative posts to another set.

Previous studies had found that the largely positive content that Facebook tends to feature has made users feel bitter and resentful. The rationale for this finding is that users become jealous over the success of other people, and they feel they are not "keeping up." Those studies, therefore, predicted that reducing the positive content in users' feeds might actually make users less unhappy. Clearly, Facebook would want to determine what types of feeds will make users spend more time on its site rather than leave the site in disgust or despair. Consequently, Facebook designed its experiment to investigate the theory that seeing friends' positive content makes users sad.

The researchers—one from Facebook and two from academia—conducted two experiments, with a total of four groups of users. In the first experiment, they reduced the positive content of News Feeds; in the second experiment, they reduced the negative content. In both experiments, these treatment conditions were compared with control groups in which News Feeds were randomly filtered without regard to positive or negative content.

The results were interesting. When users received more positive content in their News Feed, a slightly larger percentage of words in their status updates were positive, and a smaller percentage were negative. When positivity was reduced, the opposite pattern occurred. The researchers concluded that the emotions expressed by friends, through online social networks, elicited similar emotions from users. Interestingly, the results of this experiment did *not* support the hypothesis that seeing friends' positive content made users sad.

Significantly, Facebook had not explicitly informed the participants that they were being studied. In fact, few users were aware of this fact until the study was published in a paper titled "Experimental evidence of massive-scale emotional contagion through social networks" in the prominent scientific journal *Proceedings of the National Academy of Sciences.* At that point, many people became upset that Facebook had secretly performed a digital experiment on its users. The only warning that Facebook had issued was buried in the social network's one-click user agreement. Facebook's Data Use Policy states that Facebook "may use the information we receive about you . . . for internal operations, including troubleshooting, data analysis, testing, research, and service improvement." This policy led to charges that the experiment violated laws designed to protect human research subjects.

Some lawyers urged legal action against Facebook over its experiment. While acknowledging the potential benefits of digital research, they asserted that online research such as the Facebook experiment should be held to some of the same standards required of government-sponsored clinical trials. What makes the Facebook experiment unethical, in their opinion, was that the company did not explicitly seek subjects' approval at the time of the study.

Some industry analysts challenged this contention, arguing that clinical research requirements should not be imposed on Facebook. They placed Facebook's experiment in the context of manipulative advertising—on the web and elsewhere—and news outlets that select stories and write headlines in a way that is designed to exploit emotional responses by their readers.

On July 3, 2014, the privacy group Electronic Privacy Information Center (EPIC; **www.epic.org**) filed a formal complaint with the Federal Trade Commission (FTC; **www.ftc.gov**) claiming that Facebook had broken the law when it conducted the experiment without the participants' knowledge or consent. EPIC alleged that Facebook had deceived its users by secretly conducting a psychological experiment on their emotions.

Facebook's Response

Facebook Chief Operating Officer Sheryl Sandberg defended the experiment on the grounds that it was a part of ongoing research that companies perform to test different products. She conceded, however, that the experiment had been poorly communicated, and she formally apologized. The lead author of the Facebook experiment also stated, "I can understand why some people have concerns about it (the study), and my co-authors and I are very sorry for the way the (academic) paper described the research and any anxiety it caused."

For its part, Facebook conceded that the experiment should have been "done differently," and it announced a new set of guidelines for how the social network will approach future research studies. Specifically, research that relates to content that "may be considered deeply personal" will go through an enhanced review process before it can begin.

The Results

At Facebook, the experiments continue. In May 2015, the social network launched an experiment called Instant Articles in partnership with nine major international newspapers. This new feature allowed Facebook to host articles from various news publications directly on its platform, an option that the social network claims will generate a richer multimedia experience and faster page-loading times.

The following month Facebook began experimenting with its Trending sidebar, which groups news and hashtags into five categories among which users can toggle: all news, politics, science and technology, sports, and entertainment. Facebook maintained that the objective is to help users discover which topics they may be interested in. This experiment could be part of Facebook's new effort to become a one-stop news distributor, an approach that would encourage users to remain on the site for as long as possible.

A 2016 report asserts that Facebook's list of top trending topics is not quite objective. For example, one source stated that Facebook's news curators routinely excluded trending stories from conservative media sites from the trending section. Facebook strongly denied the claim.

Sources: Compiled from S. Gunaratna, "Report: Facebook Manipulates What's 'Trending,'" *CBS News*, May 10, 2016; J. Matias, "Were All Those Rainbow Profile Photos Another Facebook Study?" *The Atlantic,* June 28, 2015; J. Vaughn, "Facebook Experiment Points to Data Ethics Hurdles in Digital Research," *SearchDataManagement,* November 14, 2014; G. Smith, "Facebook Conducted Another Secret Experiment on Users," *The Huffington Post,* November 3, 2014; J. O'Toole, "Facebook: We're Still Experimenting on Users, But Now It's Less Creepy," *CNN Money,* October 2, 2014; D. Rushe, "Facebook Sorry—Almost—for Secret Psychological Experiment on Users," *The Guardian,* October 2, 2014; R. Meyer, "Facebook's Mood Manipulation Experiment Might Have Been Illegal," *The Atlantic*, September 24, 2014; "The Facebook Experiment: What It Means for You," *Forbes*, August 4, 2014; A. Ma, "Facebook Is Experimenting with How You Read the News," *The Huffington Post*, June 30, 2014; "Facebook Emotion Experiment Sparks Criticism," *BBC News*, June 30, 2014; M. Meyer, "Everything You Need to Know about Facebook's Controversial Emotion Experiment," *Wired*, June 30, 2014; R. Albergotti, "Furor Erupts over Facebook's Experiment on Users," *Wall Street Journal*, June 30, 2014; V. Goel, "Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry," *the New York Times*, June 29, 2014; www.facebook.com, accessed September 3, 2016.

Questions

1. Discuss the ethicality and legality of Facebook's experiment with human emotions.
2. Was Facebook's response to criticism concerning that experiment adequate? Why or why not?
3. Consider the experiments that Facebook conducted in May and June 2015. Is there a difference between these two experiments and Facebook's experiment with human emotions? Why or why not?
4. Should the law require companies to inform their users every time they conduct experiments? Why or why not?