

CHAPTER 4

Social, Ethical, and Legal Issues in the Digital Firm

LEARNING OBJECTIVES

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

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

OPENING CASE: TECH DATA HELPS TO FIGHT SOFTWARE PIRACY

This is an interesting, stimulating chapter to present in class. Your students will have a variety of opinions about the ethical issues presented in this chapter. The opening vignette is a good opening for a discussion of the issues around software piracy, and illustrates the impact on businesses. A company, Tech Data, has filled a gap by developing a program that will make businesses aware of whether or not they are buying pirated software. This is useful for companies that do not want to engage in purchasing illegal/pirated software and for the software developers, like Microsoft.

Here are some questions and answers to focus the discussion:

1. **Do you agree that software piracy is a bad thing? Explain your answer.**

Important issues that students should identify are:

- It costs to create software, so people should be compensated for their intellectual contributions
- Software piracy is rampant in developing countries; is piracy different for people who cannot afford to buy software

- If everyone pirated software, would companies be encouraged to produce more (improved) software?
- Why do people think it is okay to pirate software from rich companies, like Microsoft? Does the financial status matter?

2. Apply an ethical analysis to the issue of software piracy.

Students should go through the steps in the ethical analysis, identifying the steps in the textbook, such as:

Identify and Describe the Facts

- piracy affects many players
- it costs money, lost sales, lost taxes, lost jobs
- piracy rates differ in different countries
- companies are coming together to fight piracy

Define the Conflict & the Higher Order Values

- technology allows software to be pirated
- software is protected as intellectual property
- pirating software is theft

Identify the stakeholders

- employees
- government and taxpayers
- pirates

Identify the Options

- companies can use TDC to counteract piracy
- companies can pursue legal action

Identify the potential consequences of your options

- Legal route will probably not work (based on text)
- TDC may cut down on piracy, increase revenues, educate public

3. What are the ethical, social, and political issues raised by software piracy?

- Ethical: piracy hurts many people; it is theft; it contravenes candidate ethical principles (students can discuss any one principle)
- Social: piracy hurts society by impacting tax revenue and costing numerous jobs
- Political: legal issues (piracy is illegal); government will want to create legislation to prevent piracy

4. What is the responsibility of a business such as TechData in reducing or eliminating software piracy?

- TechData is a business making money to prevent piracy. If people didn't pirate then TD would not have a business. Their mandate is to reduce software and in doing so, increase revenues to software companies and to them

4.1

UNDERSTANDING ETHICAL AND SOCIAL ISSUES RELATED TO SYSTEMS

The use of new technology always presents ethical and social questions around the use of technology. Throughout this chapter and throughout the rest of the text, it is imperative that you raise and discuss these issues so that students can see both the positive and negative sides of technology. It is possible, for example, that if more courses and schools had addressed these issues, the current scandals may have been avoided or uncovered sooner. So raise these issues, stress their importance, and point out ways that these issues can affect the students in the long run.

It will help to define ethics as the principles of right and wrong that individuals use to make choices to guide their behaviours. Emphasize that ethical issues raised by the Information Age, and specifically the Internet, are the most explosive to face our society in decades. Because many of these issues are new, it may take many years (and many court battles) before they are resolved.

Ask students to describe some of the ethical dilemmas brought about by the Internet age, such as downloading music, capturing personal information in return for services, watching movies online, spam, etc.

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

Many of these issues not only touch our society as a whole, but also raise lots of questions for organizations, companies, and the workplace in general. We hear arguments for free speech, personal responsibility, and corporate responsibility. There are discussions about the government's role in all this. At the beginning of Chapter 4 the textbook says: "Suddenly individual actors are confronted with new situations often not covered by the old rules. Social institutions cannot respond overnight to these ripples... Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime, you may have to act. You may be forced to act in a legal 'gray area.'"

Figure 4-1 shows the relationship between ethical, social, and political issues in an information society. You could change this diagram somewhat to avoid the impression that the five dimensions are separate. You'd show significant overlap of each area, and most of the diagram would be in shades of gray. The five dimensions we'll discuss are:

information rights and obligations, property rights and obligations, accountability and control, system quality, and the quality of life.

FIVE MORAL DIMENSIONS OF THE INFORMATION AGE

The textbook outlines five moral dimensions that apply in today's business environment. Although these dilemmas have existed in some form or another for years, they are made more important with the technological advances we've seen in the last ten years. This can be discussed with examples.

KEY TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

Information technologies pose problems and threats to established societal rules, and technological advances pose new situations and possible threats to privacy and ethics. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 4-2.

TABLE 4-2 TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

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

Students can also be asked if they are concerned about the amount of data being collected about them. Data from multiple sources can be collected and profiles can be created on an individual. Although students may not be concerned about this per se, they sometimes react when you point out how this profile can be used and the impact it could have on their reputation. The government of Canada's privacy commission website contains an interesting video illustrating the data collected from social networking sites, such as FaceBook http://www.priv.gc.ca/information/social/index_e.cfm

Bottom Line: Technological trends are posing new situations and questions we haven't had to deal with before. As it's your world and your future, you should be concerned and become involved in their resolution.

4.2**ETHICS IN AN INFORMATION SOCIETY**

Did you ever hear the old warning: “Just because you can, doesn’t mean you should?” Well, a lot of things are possible on the Internet nowadays, but that doesn’t mean you should do them.

Ethics is easily managed in small groups because the group itself tends to control the individual’s behaviour. It’s referred to as “self-policing.” The larger the group, the harder it is to manage the actions of individuals. Now stretch that to a huge number of people with many frames of reference and experiences. Responsibility to the group becomes harder to police and accountability for an individual’s actions is harder to enforce.

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Every action causes a reaction. When you’re using the Internet, computers on campus, or your employer’s computer, you should be aware of the following:

- **Responsibility:** Accepting potential costs, duties, and obligations for your decisions.
- **Accountability:** Determining who should take responsibility for decisions and actions.
- **Liability:** Legally placing responsibility with a person or group.
- **Due Process:** ensuring the laws are applied fairly and correctly.

ETHICAL ANALYSIS

It’s safe to say you’ll find yourself in situations where your ethics are challenged. What should you do? Try the following:

- *Identify and describe clearly the facts.*
 - Separate fact from fiction.
- *Define the conflict or dilemma and identify the higher-order values involved.*
 - Remember, no matter how thin you slice it, there’s always two sides.
- *Identify the stakeholders.*
 - Determine who’s really involved.
- *Identify the options that you can reasonably take.*
 - Compromise; it doesn’t always have to be an “either-or” outcome.
- *Identify the potential consequences of your options.*
 - Anticipate the outcome; it will help you devise better solutions.

CANDIDATE ETHICAL PRINCIPLES

Students should study the ethical principles outlined in the text, as they will be incorporated into the discussions throughout the remainder of this chapter.

The principles listed in the text are deeply rooted in cultures around the world. Although they predate the Internet, students can be asked to consider how well they apply to issues raised by the Internet.

- **Golden rule** — do unto others as you would have them do unto you.
- **Immanuel Kant's Categorical Imperative** — if an action is not right for everyone to take, it is not right for anyone.
- **Descartes' rule of change** — if an action cannot be taken repeatedly, it is not right to take at all.
- **Utilitarian Principle** — take the action that achieves the higher or greater value.
- **Risk Aversion Principle** — take the action that produces the least harm or the least potential cost.
- **Ethical "no free lunch" Rule** — assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise.

PROFESSIONAL CODES OF CONDUCT

Most professional organizations have a code of conduct by which they expect their members to abide. Students might be encouraged to visit the following Association for Computing Machinery (ACM) Web site at <http://www.acm.org/constitution/code.html>. Many business students may be familiar with the codes of accounting boards.

SOME REAL-WORLD ETHICAL DILEMMAS

Individuals, companies, and corporations are being forced to deal with these new ethical and social issues in ways never before imagined. Employ the ethical analysis we just discussed to the real-world situations presented here and in the text.

No issue has been harder for organizations to deal with than that of e-mail. Should companies be allowed to read employees' e-mails, especially if they are personal? Should employees be allowed to send personal e-mails to begin with? Should e-mails be used against a person or company in a court of law? If so, how? An example of this issue was the Microsoft versus Department of Justice antitrust trial. Many e-mails written by Microsoft's executives were used against them.

Ask students to discuss what is right? Is it okay for an employee to download the latest picture from any Web site (copyright issues? Appropriate content?) and use it as a screensaver? Is it okay to run a personal commercial Web site from your workplace computer using the company's computer resources? Is it okay to e-mail jokes over the

company's network? Is it okay for the company to use technology to monitor your computer usage every minute you're on the job? Is it okay for the company to use technology to monitor your keystrokes so they can determine how much work you're doing? Is it okay for employees to use the company's computers and networks to access eBay during their lunch break? Should a company be allowed to remove Solitaire from employee computers?

What is the best way for companies and employees to handle these situations? What is the right thing to do?

Another issue is the impact of technology on jobs. Ask students whether a company should go out of business instead of increasing its automation and use of information systems. Ask students if they are willing to pay two to three times more for goods so workers will not lose their jobs. At this point, students are ready to see that it is competitive pressure caused by consumer unwillingness to pay higher prices that is driving the reengineering process. At this point, you can lead a discussion about the ethical ways of reengineering and using information systems.

Also ask students to consider how much information they give away. Then ask your students if giving away so much personal information is necessary. Help your students to see the relationship between the technology they want to use and the loss of privacy. Many students give a good amount of information away on surveys and Web sites, especially social networking sites like FaceBook, without much thought. Lack of confidence in information security, widespread Internet access, and increased malicious attacks by insiders have caused significant information security losses at major U.S. companies, according to an information security survey by Information Week and Ernst & Young LLP. The study found that more than half (54 percent) of the surveys 1320 participants experienced losses due to poor information security and disaster recovery within the last two years (this was before the September 11 attack). If you add computer viruses to the mix, the number rises to 78 percent. Ask students to weigh the tradeoffs of privacy versus information needs. Students, like professors, wear two or more hats. They may say yes to information for marketing purposes, but at the same time want their privacy and their children's privacy protected. Is this an ethical question or a constitutional one? What kinds of rules or ethics do we need to constrain such databases? Apply each of the proposed ethical rules to see if it gives an answer.

Bottom Line: Ethics in an information society holds each person responsible for his or her actions. Each person is accountable for everything he or she does, no matter how anonymous the action may seem. Each person is liable for the consequences his or her actions may inflict on other people and society as a whole.

4.3

THE MORAL DIMENSIONS OF INFORMATION SYSTEMS

This section examines the five moral dimensions (information rights; property rights; accountability, liability, and control; system quality; and the quality of life) by asking you to examine them from a personal standpoint.

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN THE INTERNET AGE

Many of us take our **privacy** and freedom for granted. Students should be aware of how technology is changing and challenging our basic assumptions about these issues.

Although the claim to privacy is protected in many country's constitutions (including that of Canada), there are additional protections such as the Privacy Act of Canada, better known as the Personal Information Protection and Electronic Documents Act (PIPEDA), protects privacy in Canada. It has 10 provisions that include the appointment of a chief privacy officer by every organization in Canada that conducts business transactions. Students should discuss the privacy provisions of PIPEDA, including examples of Canadian companies that may have problems with implementing PIPEDA.

(www.privcom.gc.ca)

Most American and European privacy law is based on a regime called Fair Information Practices (FIP). **Fair Information Practices (FIP)** is a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual.

The European Directive on Data Protection

European countries have much stricter restrictions on gathering data about private individuals, on the Internet or elsewhere. European citizens have the right to deny the initial collection of information. They have the right to know and deny the use of data for purposes other than its original intention. They have the right to inspect and correct any data gathered on them. **Informed consent** can be defined as consent given with knowledge of all the facts needed to make a rational decision.

Working with the European Commission, the U.S. Department of Commerce developed a safe harbour framework for U.S. firms. A **safe harbour** is a private, self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement.

Internet Challenges to Privacy

Under pressure from privacy advocates, and because of government legislation, Web sites now post privacy policies. How do organizations gather the information? By using **cookies**, a part of every browser program. If you have Internet access and have ever

visited a Web site, there is a cookie file on your computer. You can show your students a cookie file if you have access to a computer in class.

Most of the data in the file are unintelligible to you. However, they give information to Web sites about how you prefer the Web site to be configured, who you are, which Web site you came from, what you do while on a site, and other information pertinent to the Web site. You can turn off the cookie option in your browser, but many sites won't let you access their features if you do.

Because the corporate world is demanding better results for the dollars spent on Internet advertising, some Web sites have developed **Web bugs** to help track users and determine what they do and don't do on the Internet. Web bugs are tiny, indistinguishable files embedded within a Web page or within an e-mail message. The bug monitors behaviour of those using the page and combines the information with other data collected to get a more robust picture of how people are using the Web site and how effective the advertising is.

Increasingly, Web sites are using **spyware** in an attempt to gather marketing information about visitors and customers. This type of software is installed directly onto your computer and sends data to the company about your surfing habits. Unfortunately, this software can also cause problems with your computer and send information that can be used in identity theft.

Most e-commerce merchants are pushing for self-regulation and the practice of requiring individuals to “**opt-out**” of data gathering. Opting out allows individuals to tell an organization not to share personal information with any third party. **Opting in** requires individuals to expressly give an organization the right to gather information before any information can be collected. PIPEDA requires individuals to opt-in in Canada.

Technical Solutions

According to the law you must inform someone if you are taping a telephone conversation with them. On the other hand, you can legally record that person's Internet transmissions without any need to inform them you are doing so. This type of disparity exists because our laws have not kept up with emerging technologies. There are some tools that can help you block someone from tracing your Internet activities as the text discusses. However, if you use your company's computers for most of your Web-browsing or e-mail activities, you may want to check with your Information Technology department before you install the tools.

The World Wide Web consortium has developed standards for how privacy policies can be embedded into Web pages and subsequently be compared to a user's privacy wishes through the user's Web browser. The Platform for Privacy Practices (**P3P**) is included in Internet Explorer and allows the user to determine what sites can collect information behind the scenes through the user's cookie files. Because the P3P standards are “machine-readable” the user doesn't have to search each Web site for its privacy policy. The user can let the computers do the comparison and automatically block any site not

conforming to the user's wishes. Still, it only works with Web sites that comply with the P3P standards.

PROPERTY RIGHTS: INTELLECTUAL PROPERTY

Intellectual property issues have been around for hundreds of years. Some of the laws and policies in place to settle disputes about trade secrets, copyrights, and patents have to be rewritten to apply to the Internet. **Intellectual property** is a result of someone's effort at creating a product of value based on their experiences, knowledge, and education. In short, intellectual property is brain power.

Trade secret — any intellectual work or product used for a business purpose that can be classified as belonging to that business, provided it is not based on information in the public domain.

Copyright — a statutory grant that protects creators of intellectual property against copying by others for any purpose for a minimum of 50 years.

Patent — a legal document that grants the owner an exclusive monopoly on the ideas behind an invention for between 17 and 20 years; designed to ensure that inventors of new machines or methods are rewarded for their labour while making widespread use of their inventions.

Challenges to Intellectual Property Rights

The Internet has made it difficult to protect intellectual property. You may ask students to discuss whether they have ever downloaded music or movies from the Internet, and if it was considered unethical or contravened intellectual property issues. In the US, everything on the Web is considered to be protected under copyright and intellectual property laws unless the Web site specifically states that the content is public domain: the **Digital Millennium Copyright Act (DMCA)** made it a federal offense to violate copyright laws on the Internet, punishable with a fine up to \$250 000.

In Canada, the laws are being constantly challenged. Students can investigate recent advances in legislation and in the response of the music industry and artists. The question is really whether the laws are at all appropriate for the Internet, and whether they can be enforced. How should the music industry respond? Is suing the ISPs the answer? This will be a good in-class discussion.

ACCOUNTABILITY, LIABILITY, AND CONTROL

Many of our laws and court decisions establishing precedents in the area of *accountability*, *liability*, and *control*, were firmly in place long before computers were invented. Many of them date back to the early 1900s, and some simply don't make sense in this day and age.

Computer-Related Liability Problems

As our dependence on the use of computer systems grows, legal courts will have no choice but to develop laws designed to deal with computer-related liability problems. Traditionally, software producers have not been held physically or economically liable for any harm that comes about through the use of their software products.

Students can be asked to discuss other examples that are presented in the textbook.

SYSTEM QUALITY: DATA QUALITY AND SYSTEM ERRORS

As we rely on information systems more, data quality issues are gaining importance. These issues affect you as a consumer and as a user.

Most of us use software that the manufacturer knows has bugs. They usually are nothing more than an aggravation and a frustration. But once in a while, they will affect our use of the computer. Our natural tendency is to let the marketplace control the balance by letting the customer punish or reward the producer. But will that be enough, or will the issue end up in the courts?

When a network server crashes and day-traders miss an important trade, who is responsible for the lost income? The ISP? The financial service company? No one? As more and more companies do business on the Internet, will Internet Service Providers or the companies doing business on the Internet be held accountable for equipment outages that render those businesses unable to process transactions?

Three principal sources of poor system performance are:

- Software bugs and errors
- Hardware or facility failures caused by natural or other causes
- Poor input data quality

How can software companies balance the need to create new software in a timely manner with the enormous cost and time of testing software? What standards for error-checking should be employed?

QUALITY OF LIFE: EQUITY, ACCESS, AND BOUNDARIES

Invariably, when discussing online technology, some students mention their concern about losing the face-to-face contact with other human beings. We hear stories about children who haven't developed normal social skills because they spend all their time in front of a computer. No discussion about the quality of life issues would be complete without mentioning the tales of "online love affairs." Of course, many people lose their jobs and their way of life because of technology. These are all very valid concerns.

Balancing Power: Centre versus Periphery

It was thought that huge centralized mainframe computers would centralize power at corporate headquarters. However, the shift toward highly decentralized computing, coupled with an ideology of empowerment of thousands of workers, and the decentralization of decision making to lower organizational levels have reduced the fears of power centralization in institutions. One must ask themselves if the decentralization of power to the lower-level employees really gives them any more authority to make important decisions.

Rapidity of Change: Reduced Response Time to Competition

Most of us would readily agree that information systems have helped to create much more efficient national and international markets. The flip side of that equation is that the now-more-efficient global marketplace has also reduced the normal social buffers that permitted businesses many years to adjust to competition. In our quest for competitive positioning, are we at risk of developing a “just-in-time society” with “just-in-time jobs” and “just-in-time” workplaces, families, and vacations?

Maintaining Boundaries: Family, Work, and Leisure

One quality-of-life issue that affects more and more people personally is the ability to work from home. Most traditional workers had a “regular day job” 9–5, five days a week, in a typical office setting. If they didn't get their work done today, they would usually wait until they were back in the office tomorrow or Monday. Now because of technology they can work seven days a week, all hours of the day, at home. The impact on personal and family life can be considerable. In many regards, this issue extends to many employees who spend their normal 40–50 hours a week in the office and then stay “wired” in the evenings, on weekends, and even during vacations.

There is an upside to the jobs issue, though. Many parents like telecommuting because they can stay home with, or at least be nearer, their children. More and more people are leaving the big cities and moving to small towns for the quality of life, yet they can still keep their well-paying jobs. Many small companies are able to expand their customer base because of technology, which in turn helps the employees immensely. Completely new businesses are born because of technology.

You can ask students to compare these two points of view.

Dependence and Vulnerability

As a society we have become incredibly dependent on information systems. However, we have also put ourselves in a highly vulnerable position if these systems fail. We have come to treat information systems as commonplace as having a television in our homes, what we most often forget is that there are no regulatory or standard-setting forces in place to regulate them. The absence of standards and the criticality of some system applications will probably call forth demands for national standards and perhaps regulatory oversight.

Computer Crime and Abuse

Computer crime is one area that has been extremely hard for our society and our governments to keep up with the rapid change. Many laws have to be rewritten and many new laws must be implemented to accommodate the changes. **Computer crime and computer abuse** extends to any wrongdoing involving equipment and Internet usage. We spoke earlier about anonymity not being a license for socially unacceptable behaviour.

Spam is junk e-mail sent by an organization or individual to a mass audience of Internet users who have expressed no interest in the product or service being marketed. Spamming has been challenged in the courts by Internet Service Providers (ISP) as an unfair practice. The ISPs say thousands of these e-mails clog their systems, and no one wants them anyway. The spammers argue their right to freedom of speech is violated if they can't send e-mails to anyone they want.

Employment: Trickle-Down Technology and Reengineering Job Loss

Other issues affecting society include job losses and career changes caused by technology. Students can argue the positive or negative effects, but one thing is clear: students will have to continually update skills and knowledge in order to remain competitive in the job market. As companies continue to embrace new technology and new methods of using it, everyone will be responsible for ensuring your skills and education remains current.

Equity and Access: Increasing Racial and Social Class Cleavages

The **digital divide** exists between urban and rural communities in North America, and between ethnic and racial groups, as well as between the rich and the poor. In addition, there is a digital divide between developed and developing countries. Students can discuss who should take responsibility for lessening the divide.

Health Risks: RSI, CVS, and Technostress

Managers should be acutely aware of the health issues caused by computer usage, especially **repetitive stress injury (RSI)**. Why? Because these health issues cost businesses huge amounts of money each year in medical treatment claims and lost productivity. **Carpal tunnel syndrome**, a subset of RSI, is the most serious health issue plaguing businesses. **Computer vision syndrome (CVS)** is increasing as people continually use computer screens and handheld devices that strain eyesight.

It doesn't take much to avoid the problems associated with computer usage. Ergonomics, the study of the relationship between humans and machines, has helped determine that it's cheaper to purchase equipment that reduces the health risks associated with computers, such as different keyboards, monitors that reduce eye strain, and desks that allow proper body positions.

A recent malady is **technostress**. Managers should encourage their employees to take frequent breaks from their computers and to recognize and understand the dangers of isolation from humans.

How has all this technology affected you? Ask students to think about this.

Bottom Line: If it sounds too good to be true, it is. If it's illegal or immoral or unethical outside the computing arena, it's probably illegal, immoral, and unethical in the computing arena. If you are aware of a problem or are a victim of unethical, illegal actions, and you don't do something about it, you're part of the problem. It's your new world – use it wisely.

WINDOW ON ORGANIZATIONS WHAT SHOULD WE DO ABOUT CYBERBULLYING?

TO THINK ABOUT QUESTIONS

- 1. What are some of the technologies and communication methods used by cyberbullies? Why are they so effective?**

Cyberbullies use a variety of Internet technologies that make it easier to find and affect their victims. Some of these technologies include social networking sites, e-mail, instant messaging, and cell phone cameras. The technologies are effective because policing the Internet is a daunting task. Cyberbullies have immediate audiences that span a wide range of other technology users. The technologies help cyberbullies get their message out, either to the victim or others, more quickly and easily than non-Internet technologies. The Internet allows cyberbullies to take on other personas that are hard to trace and allows them to be faceless.

- 2. What measures have been taken by school districts and governments to combat cyberbullying? How helpful are they? Can you think of any other ways to effectively control cyberbullying?**

The local school system to which Megan Meier (cyberbully victim that committed suicide) belonged had already identified cyberbullying as a serious problem. The school held a series of assemblies, meetings, and workshops to train students, parents, faculty, and administrators how to recognize and respond to the problem. Even with these measures, cyberbullying continued. Other schools are trying to make changes locally to avoid situations like Meier's. Some schools have created 'safe rooms' in schools where problems like online harassment can be addressed in a relaxed atmosphere. Other schools provide counselors to speak with students. Parents are encouraged to take a more active role in their children's Internet activities. Some states have passed laws against cyberbullying.

How helpful are these measures? The success of all these measures varies. Cyberbullying is likely to remain a widespread problem. Bullies have been around for a much longer time than the Internet, and they are unlikely to relinquish their

newfound abilities to insult, hurt, and embarrass that social networks and other new methods of communication provide.

Other ways to help combat the problem include making it easier to report cyberbullying incidences and encourage victims and others to report instances of the problem.

3. Should there be stronger laws outlawing cyberbullying? Why or why not?

Student answers to this question will vary depending on personal opinions and preferences.

It would probably be helpful to pass stronger laws with stiffer penalties. However, as with other Internet-related laws, it has taken time to migrate rules and laws to technology-driven activities and violations.

4. Does a social networking site catering to teens such as Facebook or MySpace represent an ethical dilemma? Why or why not?

Student answers will vary. Most teens, the target audience of Facebook and MySpace.com and other social networking sites, are not fully aware of the ethical analysis process. Their reactions are based on more immediate satisfactions. The Candidate Ethical Principles outlined in the chapter should be taught at an earlier age by parents, schools, and social organizations. Social networking sites could also display them more prominently than they do now – which is never. Most users don't read user agreements so including the principles there is least effective. Sites could use banner-type advertising or splash the Principles throughout the sites in an eye-catching, pleasing way. See also re privacy on Facebook http://www.priv.gc.ca/information/social/index_e.cfm

MIS IN ACTION

Visit MySpace.com and click on Safety Tips. Explore the features for parents & educators, for teens, more resources, and safety tips and settings. Describe what capabilities and tools are available to educate users about cyberbullying and to combat this practice. Compare this with Facebook: go to www.facebook.com and click on Help, Help Center, then Safety. How effective is this Web site in dealing with cyberbullying?

(Most of the material in these answers was copied directly from the MySpace Web site, November 2008.)

Parents & educators: Cyberbullying411.com has provided the following tips to educate yourself and your family about cyberbullying and how to address it in the real world. In general, cyberbullying is bullying or harassment that happens online. Much of it is similar to what teenagers experience offline in schools, homes, or the

community, but has the additional aspect of the Internet. Cyberbullying occurs in many different places online, including through instant messaging, on social networking sites, via e-mail, and in chat rooms. The most common place cyberbullying occurs is over instant messenger, but it also can occur via other new technologies such as text messaging on mobile phones and personal digital assistants (PDAs).

For parents it's important to educate yourself about cyberbullying. Talk to your kids about the things they do, the things they see, and the people they talk to online and offline. Talk to other parents about Internet safety and behaviour; just because you and your teens know what's up doesn't mean all parents do. Internet behaviour should be an ongoing conversation within the home:

- Talk about Internet safety. Kids want to know that you "get it."
- Discuss appropriate online etiquette. For example, tell them that if they wouldn't say something to the person's face because it's too mean, it's probably not okay to say it online. Make sure your teens know appropriate online behaviour and how to end a conversation they don't like.
- Just as you ask your kids about where they go and who they're with after school, ask them which Web sites they visit and who they chat with online.
- Assure your teens that if they tell you about something that happened online, you will work with them to resolve the issue without taking away their Internet privileges.

Teens: Cyberbullying411.com has provided the following tips to educate yourself and your friends about cyberbullying and how to address it in the real world. In general, cyberbullying is bullying or harassment that happens online. Much of it is similar to what you might have experienced offline in schools, homes, or the community, but has the additional aspect of the Internet. Cyberbullying can take the form of a message on e-mail or IM or a social networking site from someone who is threatening to hurt you or beat you up. It could be a profile made by someone pretending to be you. Or, someone hacking into your profile and writing comments pretending they're from you.

Cyberbullying occurs in many different places online, including instant messaging, social networking sites, e-mail, and chat rooms. The most commonplace bullying occurs online is over instant messenger, but it also can occur via other new technologies. If you are being cyberbullied or threatened online in any way, there are things you can do to stop it:

- **Ignore the person.** Sometimes the easiest thing to do is to ignore the person and go on about your business.
- **Block or delete the person.** If it is happening on Instant Messaging or some other place online that requires a 'buddy list,' you can block certain users based upon their username, or delete them if they are in your buddy list. You can also block e-mails that are coming from specific e-mail addresses.

- **Log-off** if the harassment is bothering you.
- **Change your information.** If someone has phished your profile, change your password. If someone repeatedly sends you messages (like, 'add me to your buddy list' over and over), consider changing your username or e-mail address.
- If there is a profile that was created about you without you knowing, **contact MySpace and click on "Imposter Profile"** to have the profile or language taken down.
- If you are upset about what is being said, **talk to someone you trust.** Don't feel like you're alone.

When to talk to adults: Many times, teens are able to take care of the cyberbullying on their own. But sometimes it gets out of hand, and it's helpful to talk to an adult about what is going on. If you feel scared or overwhelmed, maybe even trapped, it's definitely time to talk to an adult.

If you don't feel comfortable speaking with a parent, seek out other adults or authorities like a teacher, coach, school counselor, a youth group leader, or other adult family member such as an aunt or uncle.

More resources: includes links to ParentCare software downloads, MySpace Guides, additional software downloads, Internet safety experts, books, and safety organizations.

Safety tips and settings: MySpace makes it easy to express yourself, connect with friends and make new ones, but who you let into your space, how you interact with them, and how you present yourself online are important things to think about when using social networking sites. Here are some common sense guidelines that you should follow when using MySpace:

- **Don't forget that your profile and MySpace forums are public spaces.** Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen names, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day or a picture of you in front of your office or school.
- **People aren't always who they say they are.** Be careful about adding strangers to your friends list. It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- **Harassment, hate speech and inappropriate content should be reported.** If you feel someone's behaviour is inappropriate, react. Report it to MySpace or the authorities.
- **Don't post anything that would embarrass you later.** It's easy to think that only our friends are looking at our MySpace page, but the truth is that

everyone can see it. Think twice before posting a photo or information you wouldn't want your parents, potential employers, colleges or boss to see!

- **Don't say you're over 18 if you're not. Don't say you're younger than 18 if you're not.** If MySpace customer service determines you are under 13 and pretend to be older, we will delete your profile. If customer service determines you are over 18 and pretend to be a teenager to contact underage users, we will delete your profile.

For Facebook, see government of Canada :

http://www.priv.gc.ca/information/social/index_e.cfm

WINDOW ON MANAGEMENT:

Flexible Scheduling at Wal-Mart: Good or Bad for Employees?

Case Study Questions:

1. **What is the ethical dilemma facing Wal-Mart in this case? Do Wal-Mart's associates also face an ethical dilemma? If so, what is it?**

Wal-Mart is trying to automate a process that was largely left to people who could make decisions based on personal judgments. The new Kronos system tracks business data within each store and uses the data to schedule employee work hours. The work schedules compiled by the system are more favorable to the company's profit margin at each store than to the employees. That impacts the quality of life for employees. Wal-Mart must accept responsibility of the potential conflicts its new system may cause employees.

Employees also face an ethical dilemma under the new Kronos system. It may decrease the stability of their jobs and perhaps create financial hardships. The new system generates schedules that are irregular and unpredictable. That makes it more difficult for employees to schedule their own personal needs and those of their family. The ethical dilemma they face is whether to cheat on their "personal availability" forms to try to create a schedule that's favorable to themselves and their families. Language on the form instructs associates that "Limiting your personal availability may restrict the number of hours you are scheduled." That causes conflict for employees—if they cheat on the form they may suffer less hours and less income; if they don't cheat, they may suffer from irregular schedules.

2. **What ethical principles apply to this case? How do they apply?**

Both sides, Wal-Mart and its employees, should be guided by the Candidate Ethical principle of "Do unto others as you would have them do unto you." Would Wal-Mart want its employees to treat customers as callously as the employees feel they have

been? Do the employees want Wal-Mart cheating against them like many of them might on their availability slips?

Employees must consider Immanuel Kant's Categorical Imperative. If every employee cheated on their availability slip, could the organization survive and thrive?

Wal-Mart must consider Descartes' rule of change. While the new scheduling system may bring only small changes now, what happens if the corporation continues making similar small changes to the detriment of its employees? What will those incremental changes do to the employees' morale in the long run?

3. What are the potential effects of computerized scheduling on employee morale? What are the consequences of these effects for Wal-Mart?

Obviously, employee morale is and will continue suffering. Experienced associates with high pay rates have expressed concern that the system enables managers to pressure them into quitting. If employees are unwilling to work nights and weekends, some justifiably so, managers can replace them with lower cost employees. Managers can avoid paying overtime or full-time wages by cutting back the hours of associates who are approaching the thresholds that cause extra benefits to kick in. Most importantly, associates are almost always people who need all the work they can get.

The consequences of poor morale in the workforce will most likely show up in customer relations. The employees most likely impacted by the new Kronus system are the very ones that most likely are on the front lines of customer touch points—the cashiers and customer assistants. Poor treatment of the customer will drive them away from the stores.

MIS IN ACTION

Visit the Web site at www.WakeUpWalMart.com and then answer the following questions:

1. What are this group's major points of contention with Wal-Mart?

It contends that, as the largest retailer in the world, Wal-Mart is a giant company with giant responsibility to all Americans to set the standard for customers (1.4 million), workers and communities, and to help build a better America. The Web site states that "America's largest employer must reflect America's values."

The site contends that the American public must force Wal-Mart to adopt policies that serve the public, its employees, and communities before it serves its shareholders. The site encourages the public to hold Wal-Mart accountable through various campaigns and actions. It takes an "us-versus-them" approach, painting Wal-Mart as the bad guy and the American public as the good guys.

2. How well does the Web site serve their cause? Does the site help their cause or hurt it?

The site lists over 400,000 supporters of its campaign. That's a fairly sizeable number. On the other hand, it's only a fraction of the number of employees and customers that Wal-Mart has. The site is well laid out and contains a lot of interesting information that refutes many of Wal-Mart's own claims of fairness to employees and customers.

Most of the numbers and facts cited on the Web site are backed up by sources. That's important to help maintain credibility and remove the criticism that it's "just gossip or ranting." In that regard, the site probably helps their cause a great deal.

3. What other approach could the organization take to bring about change?

"WakeUpWalMart.com, a union-backed group that has waged an aggressive campaign against Wal-Mart, the nation's largest retailer, will today name several Democratic political strategists as its new leaders and introduce a fresh round of ads. The group, which has attacked the wages, health benefits and labour practices of the nonunionized Wal-Mart, is expected to appoint Meghan Scott, who worked on John Edwards's presidential campaign, as its deputy campaign manager, giving her day-to-day control. Ms. Scott previously oversaw communications for the American Association for Justice, formerly the Association of Trial Lawyers of America. WakeUpWalMart, started in 2005 by the United Food and Commercial Workers union, lost its founding leaders months ago when they left to work on Mr. Edwards's latest presidential campaign. But Ms. Scott pledged that the group was "not backing off."

"We are going to fight to ensure that Wal-Mart becomes a responsible organization," she said.

Beginning today, the group will run commercials in 26 television markets suggesting that Wal-Mart's health coverage is unaffordable, forcing states to devote resources to the company's workers." (The New York Times Online, August 16, 2007, Democratic Advisers Take Posts in Group Opposing Wal-Mart, Michael Barbaro)

Using Wal-Mart's Web site and Google for research, answer the following questions:

4. How does Wal-Mart address the issues raised by organizations such as WakeUpWalMart.com?

Wal-Mart uses aggressive advertising campaigns to promote itself as "family friendly" by showing how much money it helps save families. It promotes itself as environmentally friendly and business friendly. Its Web site contains articles about the company's charitable contributions. It promotes its support of employment diversity. Wal-Mart's Web site also contains information about how a community benefits from having a local Wal-Mart store.

5. Are the company's methods effective?

Apparently Wal-Mart's efforts are effective. The company continues to attract huge numbers of job applications. It continues to post healthy profits. It's continually expanding the number of stores around the nation and around the world.

6. If you were a public relations expert advising Wal-Mart, what suggestions would you make for handling criticism?

Regarding the new Kronos scheduling system, Wal-Mart should work to make the employees part of the solution by encouraging them to take the less-than-desirable shifts, possibly by paying a small per-hour premium. Certainly, the company should not use the new Kronos system to punish employees, especially when it's first implemented. Wal-Mart should show proof to its employees that the system is not being used to replace workers with less-expensive employees

SUMMARY

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

Information technology has raised new possibilities for behaviour for which laws and rules of acceptable conduct have not yet been developed. Information technology is introducing changes that create new ethical issues for societies to debate and resolve. Increasing computer power, storage, and networking capabilities—including the Internet—can expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information can be communicated, copied, and manipulated in online environments are challenging traditional rules of right and wrong behaviour. Ethical, social, and political issues are closely related. Ethical issues confront individuals who must choose a course of action, often in a situation in which two or more ethical principles are in conflict (a dilemma). Social issues spring from ethical issues as societies develop expectations in individuals about the correct course of action. Political issues spring from social conflict and are mainly concerned with using laws that prescribe behaviour to create situations in which individuals behave correctly.

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

The moral dimensions of information systems centre around information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life. Six ethical principles are available to judge conduct. These principles are derived independently from several cultural, religious, and intellectual traditions and include the Golden Rule, Immanuel Kant's Categorical Imperative, Descartes' rule of change, the Utilitarian Principle, the Risk Aversion Principle, and the ethical "no free lunch" rule. These principles should be used in conjunction with

an ethical analysis to guide decision making. The ethical analysis involves identifying the facts, values, stakeholders, options, and consequences of actions. Once completed, you can consider which ethical principle to apply to a situation to arrive at a judgment.

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

Contemporary information systems technology, including Internet technology, challenges traditional regimens for protecting individual privacy and intellectual property. Data storage and data analysis technology enables companies to easily gather personal data about individuals from many different sources and analyze these data to create detailed electronic profiles about individuals and their behaviours. Data flowing over the Internet can be monitored at many points. The activities of Web site visitors can be closely tracked using cookies and other Web monitoring tools. Not all Web sites have strong privacy protection policies, and they do not always allow for informed consent regarding the use of personal information. The online industry prefers self-regulation to the U.S. government tightening privacy protection legislation.

Traditional copyright laws are insufficient to protect against software piracy because digital material can be copied so easily. Internet technology also makes intellectual property even more difficult to protect because digital material can be copied easily and transmitted to many different locations simultaneously over the Net. Web pages can be constructed easily using pieces of content from other Web sites without permission.

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

Although computer systems have been sources of efficiency and wealth, they have some negative impacts. Errors in large computer systems are impossible to eradicate totally. Computer errors can cause serious harm to individuals and organizations, and existing laws and social practices are often unable to establish liability and accountability for these problems. Less serious errors are often attributable to poor data quality, which can cause disruptions and losses for business. Jobs can be lost when computers replace workers or tasks become unnecessary in reengineered business processes. The ability to own and use a computer may be exacerbating socioeconomic disparities among different racial groups and social classes. Widespread use of computers increases opportunities for computer crime and computer abuse. Computers can also create health problems, such as repetitive stress injury, computer vision syndrome, and technostress.

KEY TERMS

The following alphabetical list identifies the key terms discussed in this chapter.

Accountability — the mechanism for assessing responsibility for decisions made and actions taken.

Carpal tunnel syndrome — type of repetitive stress disorder (RSI) in which pressure on the median nerve through the wrist's bony carpal tunnel structure produces pain.

Computer abuse — the commission of acts involving a computer that may not be illegal but are considered unethical.

Computer crime — the commission of illegal acts through the use of a computer or against a computer system.

Computer vision syndrome (CVS) — eyestrain condition related to computer display screen use; symptoms include headaches, blurred vision, and dry and irritated eyes.

Cookies — tiny file deposited on a computer hard drive when an individual visits certain Web sites. Used to identify the visitor and track visits to the Web site.

Copyright — a statutory grant that protects creators of intellectual property against copying by others for any purpose for a minimum of 50 years.

Descartes' rule of change — a principle that states that if an action cannot be taken repeatedly, it is not right to be taken at any time.

Digital divide — large disparities in access to computers and the Internet among different social groups and different locations.

Digital Millennium Copyright Act (DMCA) — legislation that adjusts copyright laws to the Internet Age by making it illegal to make, distribute, or use devices that circumvent technology-based protections of copyrighted materials.

Due process — a process in which laws are well known and understood that there is an ability to appear to higher authorities to ensure that laws are applied correctly.

Ethical "no free lunch" rule — assumption that all tangible and intangible objects are owned by someone else, unless there is a specific declaration otherwise, and that the creator wants compensation for this work.

Ethics — principles of right and wrong that can be used by individuals acting as free moral agents to make choices to guide their behaviour.

Fair Information Practices (FIP) — a set of principles originally set forth in 1973 that governs the collection and use of information about individuals and that forms the basis of most United States and European privacy laws.

Golden Rule — putting yourself into the place of others, and thinking of yourself as the object of the decision.

Immanuel Kant's Categorical Imperative — a principle that states that if an action is not right for everyone to take, it is not right for anyone.

Information rights — the rights that individuals and organizations have with respect to information that pertains to them.

Informed consent — consent given with knowledge of all the facts needed to make a rational decision.

Intellectual property — intangible property created by individuals or corporations that is subject to protections under trade secret, copyright, and patent law.

Liability — the existence of laws that permit individuals to recover the damages done to them by other actors, systems, or organizations.

Nonobvious relationship awareness (NORA) — technology that can find obscure hidden connections between people or other entities by analyzing information from many different sources to correlate relationships.

Opt-in — model of informed consent prohibiting an organization from collecting any personal information unless the individual specifically takes action to approve information collection and use.

Opt-out — model of informed consent permitting the collection of personal information until the consumer specifically requests that the data not be collected.

P3P — industry standard designed to give users more control over personal information gathered on Web sites they visit. Stands for Platform for Privacy Preferences Project.

Patent — a legal document that grants the owner an exclusive monopoly on the ideas behind an invention for 17-20 years; designed to ensure that inventors of new machines or methods are rewarded for their labour while making widespread use of their inventions.

Privacy — the claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or the state.

Profiling — the use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals.

Repetitive stress injury (RSI) — occupational disease that occurs when muscle groups are forced through repetitive actions with high-impact loads or thousands of repetitions with low-impact loads.

Responsibility — accepting the potential costs, duties, and obligations for the decisions one makes.

Risk Aversion Principle — principle that one should take the action that produces the least harm or incurs the least cost.

Safe harbour — private self-regulating policy and enforcement mechanism that meets the objectives of government regulations but does not involve government regulation or enforcement.

Spam — unsolicited commercial e-mail.

Spyware —technology that aids in gathering information about a person or organization without its knowledge.

Technostress — stress induced by computer use; symptoms include aggravation, hostility toward humans, impatience, and enervation.

Trade secret — any intellectual work or product used for a business purpose that can be classified as belonging to that business, provided it is not based on information in the public domain.

Utilitarian Principle — principle that assumes one can put values in rank order and understand the consequences of various courses of action.

Web bugs — tiny graphic files embedded in e-mail messages and Web pages that are designed to monitor online Internet user behaviour.

REVIEW QUESTIONS

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

Explain how ethical, social, and political issues are connected and give some examples.

Figure 4-1 can be used to answer this question. Information technology has raised new possibilities for behaviour for which laws and rules of acceptable conduct have not yet been developed. The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. Ethical, social, and political issues are closely related. Ethical issues confront individuals who must choose a course of action, often in a situation in which two or more ethical principles are in conflict (a dilemma). Social issues spring from ethical issues as societies develop expectations in individuals about the correct course of action. Political issues spring from social

conflict and are mainly concerned with using laws that prescribe behaviour to create situations in which individuals behave correctly.

In giving examples, students can identify issues surrounding the five moral dimensions of the information age. These include: information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life.

List and describe the key technological trends that heighten ethical concerns.

Table 4-2 summarizes the four key technological trends responsible for heightening ethical concerns. These trends include:

- Computing power doubles every 18 months
- Data storage costs rapidly declining
- Data analysis advances
- Networking advances and the Internet

Increasing computer power, storage, and networking capabilities including the Internet can expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information can be communicated, copied, and manipulated in online environments are challenging traditional rules of right and wrong behaviour.

Differentiate between responsibility, accountability, and liability?

- Responsibility is a key element of ethical actions. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make.
- Accountability is a feature of systems and social institutions. It means that mechanisms are in place to determine who took responsible action, who is responsible.
- Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations.

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

Identify and describe the five steps in an ethical analysis

The five steps in ethical analysis include:

- Identify and describe clearly the facts.
- Define the conflict or dilemma and identify the higher-order values involved.
- Identify the stakeholders.
- Identify the options that you can reasonably take.
- Identify the potential consequences of your options.

Identify and describe six ethical principles.

Six ethical principles are available to judge conduct. These principles are derived independently from several cultural, religious, and intellectual traditions and include:

- **Golden Rule.** Do unto others as you would have them do unto you
- **Immanuel Kant's Categorical Imperative.** If an action is not right for everyone to take, it is not right for anyone
- **Descartes' rule of change.** If an action cannot be taken repeatedly, it is not right to take at all
- **Utilitarian Principle.** Take the action that achieves the higher or greater value
- **Risk Aversion Principle.** Take the action that produces the least harm or the least potential cost
- **"No free lunch" rule.** Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise.

These principles should be used in conjunction with an ethical analysis to guide decision making. The ethical analysis involves identifying the facts, values, stakeholders, options, and consequences of actions. Once completed, you can consider which ethical principle to apply to a situation to arrive at a judgment.

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

Define privacy and fair information practices.

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

Fair information practices are a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual.

Explain how the Internet challenges the protection of individual privacy and intellectual property.

Contemporary information systems technology, including Internet technologies, challenges traditional regimens for protecting individual privacy and intellectual property. Data storage and data analysis technology enables companies to easily gather personal data about individuals from many different sources and analyze these data to create detailed electronic profiles about individuals and their behaviours. Data flowing over the Internet can be monitored at many points. The activities of Web site visitors can be closely tracked using cookies and other Web monitoring tools. Not all Web sites have strong privacy protection policies, and they do not always allow for informed consent regarding the use of personal information.

Explain how informed consent, legislation, industry self-regulation, and technology tools help protect the individual privacy of Internet users.

Informed consent means that the Web site visitor knowingly permits the collection of his/her data during his/her visit to the company's Web site. In Canada, individuals must opt-in to allow their information to be shared by organizations (legislated by PIPEDA). The federal legislation that applies to private sector organizations is mirrored by public sector legislation at most provincial levels, and at the federal level. Industry must comply with PIPEDA legislation that dictates the level of responsibility for privacy and protection of data. Some industries' professional organizations, such as accountants, engineers, and information systems professionals, have adopted codes of ethics to help regulate what their professionals do. Businesses have taken some steps, including publishing statements about how their information will be used.

Technology tools can be used on individual computers to protect against viruses, spyware, and block certain sites. Technical solutions also enable e-mail encryption, anonymous emailing and surfing, and cookie rejection. Of particular interest is the P3P standard that allows the user to have more control over personal information that is gathered on the Web sites visited.

List and define three different regimes that protect intellectual property rights?

Intellectual property is subject to a variety of protections under three different legal traditions:

- Trade secrets
- Copyright
- Patent law

Traditional copyright laws are insufficient to protect against software piracy because digital material can be copied so easily. Internet technology also makes intellectual property even more difficult to protect because digital material can be copied easily and transmitted to many different locations simultaneously over the Internet. Web pages can be constructed easily using pieces of content from other Web sites without permission.

5. How have information systems affected everyday life?

Explain why it is so difficult to hold software services liable for failure or injury.

Software is like a book in that it stores and displays information. Courts are wary of holding software authors liable for booklike software. In general, it is very difficult (if not impossible) to hold software producers liable for their software products when those products are considered like books are, regardless of the physical or economic harm that results. However, as people become more dependent on services essentially based on software the chances are excellent that liability law will extend its reach to include software when the software merely provides an information service.

List and describe the principal causes of system quality problems?

Three principle sources of poor system performance are:

- Software bugs and errors
- Hardware or facility failures caused by natural or other causes
- Poor input data quality

Name and describe four quality of life impacts of computers and information systems.

Four quality of life impacts of computers and information systems include:

- Jobs can be lost when computers replace workers or tasks become unnecessary in reengineered business processes
- Ability to own and use a computer may be exacerbating socioeconomic disparities among different racial groups and social classes
- Widespread use of computers increases opportunities for computer crime and computer abuse
- Computers can create health problems, such as repetitive stress injury, computer vision syndrome, and technostress

Define and describe technostress and repetitive stress injury (RSI) and explain their relationship to information technology.

Technostress is defined as stress induced by computer use; symptoms include aggravation, hostility toward humans, impatience, and fatigue.

Repetitive stress injury (RSI) is avoidable. Three management actions that could reduce RSI injuries include:

- Designing workstations for a neutral wrist position, using proper monitor stands, and footrests all contribute to proper posture and reduced RSI.
- Using ergonomically designed devices such as keyboards and mice are also options.
- Promoting and supporting frequent rest breaks and rotation of employees to different jobs.

DISCUSSION QUESTIONS

1. Should producers of software-based services, such as ATMs, be held liable for economic injuries suffered when their systems fail?

If a system fails, it is foreseeable that the producers of the software-based services could potentially be held liable for economic injuries. This could even extend to systems that have been managed poorly and implemented unsuccessfully. They, too, have the potential to impact the company's bottom line and subject producers of software-based services to liability. While the general rule is that they cannot be held

liable for matters beyond their knowledge or control, this defense may not be available in some software guideline compliance programs. Thus, producers of software-based services need to be aware of and involved in the software compliance program. In addition, software vendors may face liability if they fail to advise licensees of latent problems in their software.

Software compliance is also an issue to be considered in due diligence conducted by any company involved, directly or indirectly, in investing or making loans to businesses with computer systems. Financial advisors, in particular, may be held liable even if they are unaware that a company is not in compliance when making financial recommendations. In connection with mergers or acquisitions of companies using date-sensitive software (as almost all are), software compliance is also a factor in due diligence. Basically, software compliance raises technical, contractual, and managerial issues. For a complete solution, the strategies for responding to them must be handled on a coordinated basis.

2. Should companies be responsible for unemployment caused by their information systems? Why or why not?

Answers for this question will vary, as will student discussion of the ethics of various issues in information systems, including social responsibility, environmental protection, privacy, individual rights, occupational safety and health, product liability, equality of opportunity, and the morality of capitalism.

This question provides an excellent opportunity for students to discuss American economist, Milton Friedman's (Nobel Prize for economics, 1976, currently, senior research fellow at the Hoover Institution at Stanford University) famous statement that a business's objective is to "maximize shareholder wealth."

Ask your students to discuss the following questions. What is the corporation? Do corporations, and more particularly the managers who represent them, have any responsibilities beyond seeking to maximize shareholder wealth? Is the term "business ethics" an oxymoron? What is the source of moral truth? These and other related questions provide the "grist" for the answer to this question.

1. Do you believe that practicing good ethics pays off? Why or why not?

Students can argue either side of the issue. Some important points to consider are whether it matters if you are caught. How do legal repercussions differ from ethical repercussions? Which are worse?

2. What do you believe the role of government should be in policing the practice of good ethics by businesses and other organizations?

Again, students' answers will differ but they should review PIPEDA and discuss how it will be used by businesses. You should be willing to discuss whether government should have a hand in business, at all.

COLLABORATION AND TEAMWORK: DEVELOPING A CORPORATE ETHICS CODE

With three or four of your classmates, develop a corporate ethics code on privacy that addresses both employee privacy and the privacy of customers and users of the corporate Web site. Be sure to consider e-mail privacy and employer monitoring of worksites, as well as corporate use of information about employees concerning their off-the-job behaviour (e.g., lifestyle, marital arrangements, and so forth). If possible, use electronic presentation software to present your ethics code to the class.

Answers will vary by individual groups, but should reflect the concepts presented in this chapter. The purpose of the exercise is to cause students to struggle with difficult, but vital, issues of privacy. They should view these issues not only as personal (privacy for themselves and their families) but also for our society, and for the world in general.

Students should both understand that rights do not end when they walk through the door of their job, and they should also gain an appreciation of the complexities of these issues. In writing the code, students must remember to include the accountability and control dimension.

LEARNING TRACK MODULE

- 1. *Developing a Corporate Code of Ethics for Information Systems.*** This Learning Track Module describes the outline for a corporate code of ethics in information systems. What should be in a code of ethics? What ethical dimensions should be included? The Learning Track Module is available at the MyMISLab.
- 2. *Creating a Web Page.***

HANDS-ON MIS: PROJECTS

MANAGEMENT DECISION PROBLEMS

1. USADATA'S WEBSITE

2. INSURANCE COMPANY

ACHIEVING OPERATIONAL EXCELLENCE: CREATING A SIMPLE BLOG

Software skills: Blog page creation

Business skills: Blog and Web page design

This exercise will not turn students into Web site developers, but it will give them a feel for its basic functions. Students are asked to create a simple blog using software at Blogger.com. Each student's solution will differ, depending on the content and design they have chosen. The MyMISLab includes instructions for completing this project. Please see the file named Ch04_Web_Page_Instructions.pdf in the Chapter 4 folder.

Have students discuss the different software that they used. Also, what problems or challenges did they encounter? What strategies did they employ to overcome them? Have them assess the blogs they created and how a company selling products or services could use them. Here are some helpful criteria:

Authority: Who is the author? Are his or her credentials stated? How knowledgeable is he or she? Who is the sponsor of the site? Is there an organization affiliated with the site or its author? Can you find out more about their purposes and intent?

Accuracy: Is the material free of error (typos, spelling, grammar, etc.)? Are the sources for factual information in the material clearly identified?

Objectivity: Is any bias present? To what extent is the material meant to persuade? Is this clearly stated? Is the page an advertisement or some other kind of promotional material? Would any surrounding advertising influence the materials contents or results? Is the advertising clearly separate from the resource contents?

Coverage: Who is the intended audience?

Currency: When was the site last updated? Does it rely on the most current available information? If not, is the reason clearly stated and justified?

IMPROVING DECISION MAKING: USING INTERNET NEWSGROUPS FOR ONLINE MARKET RESEARCH

Software skills: Web browser software and Internet newsgroups

Business skills: Using Internet newsgroups to identify potential customers

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

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

Answers will vary considerably depending on how deeply students go into the Google site. They should notice however, that the site contains a list of "Sponsored Links," and this could be an alternative to marketing their boots. Of course, there would be a fee, but they will pay for advertising eventually, and they would be attracting people directly interested in hiking boots.

CASE STUDY: SHOULD GOOGLE ORGANIZE YOUR MEDICAL RECORDS?

1. **What concepts in the chapter are illustrated in this case? Who are the stakeholders in this case?**

Chapter concepts illustrated in this case include:

- Responsibility – accepting the potential costs, duties, and obligations for decisions. Google must assume the bulk of responsibility for securing the data and ensuring it's used only for authorized purposes.

- **Accountability** – a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action. Again, Google must ensure accountability of its systems and those responsible for creating and maintaining the system.
- **Liability** – a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. Federal and state governments must pass and enforce laws protecting medical data and its uses. Google must assume liability for the system.

Of the five moral dimensions discussed in the chapter, at least three play a major role in the proposed system:

- Information rights and obligations
- Accountability and control
- System quality

Stakeholders in this case include patients and health-care consumers, doctors and other medical professionals, insurance companies, health-care related businesses like pharmaceutical companies, governments, and storage providers like Google, Microsoft and Revolution Health Group.

2. What are the problems with Canada's current medical recordkeeping system? How would electronic medical records alleviate these problems?

Current records are paper-based, making effective communications and access difficult. The current system for recording and storing medical information makes it difficult, if not impossible, to systematically examine and share the data. It's also very expensive and time-consuming to maintain paper-based medical records.

Google's proposed electronic medical record system would allow consumers to enter their basic medical data into an online repository and invite doctors to send relevant information to Google electronically. One feature of the system will include a 'health profile' for medications, conditions, and allergies, reminder messages for prescription refills or doctor visits, directories for nearby doctors, and personalized health advice. The application will also be able to accept information from many different recordkeeping technologies currently in use by hospitals and other institutions. The intent of the system is to make patients' records easily accessible, especially in emergencies, and more complete and to streamline recordkeeping.

3. What management, organization, and technology factors are most critical to the creation and development of electronic medical records?

Management: Electronic recordkeeping promises to reduce costs associated with maintaining health data. However, the upfront costs of implementation are daunting, especially to doctors who maintain their own practices. Managers would have to ensure data was not used for profiling patients or use the data to deny medical

procedures. Managers would also have to ensure data was not misused for purposes other than what is intended.

Organization: The new system promises to make data more organized and easier to retrieve. Organizations must ensure that data is not used for profiling and not used in the data analysis technology called nonobvious relationship awareness. Government, private, and non-profit organizations must pass new laws, similar to the HIPAA law, that provides adequate protection of consumer health data. That would help reassure patients and make them more likely to use the system.

Technology: New systems must be able to mesh with other versions of medical record-keeping applications. The software must be created around universal standards making implementation easier and more efficient. Above all else, technology must be created to prevent security breaches. Systems must be available one hundred percent of the time, especially to obtain medical information for emergency patients.

All three factors must work together to prevent privacy invasions and ensure medical data is not misused or abused.

4. What are the pros and cons of electronic patient records? Do you think the concerns over digitizing our medical records are valid? Why or why not?

Pros of electronic patient records include more efficient access and dissemination of medical data, especially in emergencies. The costs of gathering, storing, and disseminating medical data promise to be lower with electronic health records. Electronic health records stand to provide much-needed organization and efficiency to the healthcare industry. Proponents of electronic health records argue that computer technology, once fully implemented, would enhance security rather than threaten it.

Cons of electronic patient records, first and foremost, include privacy concerns over how the data will be captured, stored, and used. Security breaches already occur with some medical data systems and Google's proposed system is subject to the same threats. People are worried that sensitive information legitimately accessible via electronic health records might lead to their losing health insurance or job opportunities.

5. Should people entrust Google with their electronic medical records? Why or why not?

Student answers will vary according to how they view privacy, access to medical data, and lower costs. Some elements students should consider include:

- Google's reassurances that its security is iron-tight and that businesses and individuals should have confidence in its ability to store and protect data.

- Because Google hasn't provided much detail about its security practices, other business people maintain their concerns, "Businesses are hoping Google will pick the right tools to secure the infrastructure, but they have no assurances and no say in what it will pick."

6. If you were in charge of designing an electronic medical recordkeeping system, what are some features you would include? What are features you would avoid?

Answers will vary based on students' exposure to security systems and electronic recordkeeping systems. Some features that should be included are security, universal standards for gathering, storing, and disseminating data, and universal standards for transmission technologies. Some features to avoid may include unrestricted access to data and unencrypted transmissions.