Chapter 4

Ethical and Social Issues in Information Systems

After completing this chapter, students should be able to answer the following questions:

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

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

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

How have information systems affected everyday life?
Introduction

It probably goes without saying that the security and ethical issues raised by the Information Age, and specifically the Internet, are the most explosive to face our society in decades. It will be many years and many court battles before socially acceptable policies and practices are in place.

4.1 Understanding Ethical and Social Issues Related to Systems

You may love the idea that a gardening Web site or a mail order catalog gives you information about what grows best in your backyard (literally your backyard). You might even love the idea that you can sign on to Amazon.com, have the Web site greet you by name, and supply you with information about a book or CD by your favorite author or artist. If you're not especially interested in Stephen King or Frank Sinatra, don't worry; Amazon.com knows that and won't bother you with products from those artists.

You are 22 years old, drive a Mazda, like hip-hop music, shop at Macy's at least once a month around the 15th, wear a size 10 dress, live in a small two-bedroom apartment, have friends or relatives who live in Texas, like eating at Red Lobster, go on a skiing trip to Colorado every Spring Break, missed one semester of school last year due to medical problems, and spend lots of time at the ivillage.com Web site chatting with other females your age. Would it surprise you to know that this information and more can all be gleaned from various computer records?

On average, each American is listed in about 60 government and 80 private sector databases. On a typical day, each person's name is passed between computers ten times. A lot of personal information about us has always been available, just not as easily and as readily as today. Massive databases maintained by commercial companies and governments at all levels now allow profiling like that above to be accomplished easier and faster than ever before.

Even though the Internet is about 40 years old and the World Wide Web is close to 15 years old, our society is just beginning to address the ethical issues and dilemmas raised by these technological advances. It's difficult to measure one person's ethics against another person's desire to make money or wreak havoc that's made much easier by the Internet. The U.S. government is just beginning to pass laws against cybercrimes but it's difficult to stay one step ahead of the cybercriminals.

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 5, Laudon 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."

How you act, individually and as groups, in this gray area may well define the future of our society. Though that may sound a bit dramatic, you must understand that you are part of the development of "acceptable usage" of this new medium and will help define the direction in which it goes. Figure 12 depicts the relationship between ethical, social and political issues.

**Figure 12: Relationship between ethical, social, and political issues in an information society**

![Figure 12: Relationship between ethical, social, and political issues in an information society](image)

Source: (Laudon and Laudon, 2010:153)

**Understanding Ethical and Social Issues Related to Systems**
You may love the idea that a gardening Web site or a mail order catalogue gives you information about what grows best in your backyard (literally your backyard). You might even love the idea that you can sign on to Amazon.com, have the Web site greet you by name, and supply you with information about a book or CD by your favourite author or artist.

**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. 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 'grey area.'

How you act, individually and as groups, in this grey area may well define the future of our society. Though that may sound a bit dramatic, you must understand that you are part of the development of "acceptable usage" of this new medium and will help define the direction in which it goes.

**SELF CHECK QUESTION 4.1**

In what ways are ethical, social, and political issues connected? Give some examples. *(Answers at the end of this Section)*

4.2 Ethics in an Information Society

Did you ever hear the old warning: "Just because you can, does not mean you should?" Well, a lot of things are possible on the Internet nowadays, but that does not mean you should do them. Ethics is easily managed in small groups because the group itself tends to control the individual's behaviour. It is 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 are 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

Responsibility, accountability, and liability are all yours when it comes to your actions in cyberspace. Every Internet Service Provider has a "usage policy." even the so-called anonymous e-mailers that hide your real identity. Hotmail is a popular Internet e-mail service that allows you to mask your real identity. You could send out all the, shall we say unethical, threatening, nasty, aberrant, e-mail you like. You think: —Hey, no one will really know who I am. This is cool."

And then here comes the message from Hotmail to cease and desist. Your free e-mail account is cancelled because you violated Hotmail's usage policy. Then your local Internet Service Provider contacts you and tells you are terminated, baby! You violated its usage policy by your actions. By now you are really mad, not to mention embarrassed (at least we hope so). It is true. It happens.
"Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions." Some people seem to absolve themselves of responsibility by putting the onus on the computer - "Hey, the computer messed up," or "Since it was an anonymous username I did not think I'd get caught." It just does not work that way in society – face-to-face or on the Internet. No one can hide behind the technology. Humans control the computers, not the other way around. And if you have received threatening, aberrant e-mails or flames in chat room or discussion groups, and haven't reported them according to the usage policies, you may be as much a part of the problem as the perpetrator!

**THINK POINT**

Think of instances where you have witnessed unethical behaviour regarding the use of technology in your organisation.

**Candidate Ethical Principles**

It is safe to say you will find yourself in situations where your ethics are challenged. What should you do? Try the following:
- Separate fact from fiction.
- Remember, no matter how thin you slice it, there's always two sides.
- Determine who's really involved.
- Compromise; it does not always have to be an "either-or" outcome.
- Anticipate the outcome; it will help you devise better solutions.

You should study the ethical principles outlined in the text, as we will be incorporating them into the discussions throughout the remainder of this chapter.

**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, and how? A recent example of this issue is the Microsoft versus Department of Justice antitrust trial. Many e-mails written by Microsoft's executives have been used against them. E-mails are not as anonymous as people think – "Sending an e-mail message is more like sending a postcard than sending a sealed envelope."(CNN Headline News, April 28, 1996).

So in your opinion, what is right? Is it okay for an employee to download the latest picture from Playgirl's Web site 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 discriminatory jokes over the company’s network that would not be allowed over the water.
Is it okay to send e-mail telling everyone that the boss is a jerk, then get mad when the company fires you?

Is it okay for the company to use technology to monitor your computer usage every minute you are on the job? Is it okay for the company to use technology to monitor your keystrokes so they can determine how much work you are doing? Is it okay for you to use the company's computers and networks to surf Macy's Web site and order the latest fashions during your lunch break? Should a company be allowed to remove Solitaire from employee computers?

What if Ester is using her computer to surf gardening Web sites three hours a day while you have to do her work? What if Joe and Sipho play the newest Internet game during their coffee break every morning and afternoon, which bogs down the entire company's network?

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

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. You should be aware of how technology is changing and challenging our basic assumptions about these issues.

SELF CHECK QUESTION 4.2

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

(Answers at the end of this Section)

Internet Challenges to Privacy

Technical Solutions

According to South African law you must inform someone if you are taping a telephone conversation with him or her. 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.

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 copyrights, patents, and trade secrets, 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 brainpower.

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 Web site does not need to carry the copyright symbol © in order for it to be protected. Copyright laws and intellectual property rights cannot be violated on the Internet any more than they can in other mediums. While this is not a law class, you should be aware of the fine line between acceptable and legal usage of materials and the illegal theft of materials. When it comes to copyright material, the underlying ideas are not protected, just the publication of the material. On the other hand, a **patent** grants a monopoly on the underlying concepts and ideas. Before you use anything, especially any material on the World Wide Web, make sure you are using it legally and ethically.

Get past the idea that because everything on the Web is free, easy, and available 24-hours a day, it must therefore be okay to use it however you want. The question you should be asking yourself is, "Is it ethically right and legal?"

The **Business Software Alliance (BSA)** is an organization working to prevent software piracy and the illegal use of copyrighted material around the world. And do not think the problem is limited to the 17-year old computer wizard locked in his bedroom. This crime can be committed by anyone, as this news clip shows:

*Seventeen high-tech professionals were indicted on federal charges for participating in an Internet piracy ring that hijacked software worth more than $1 million. The government said 12 of those indicted are members of an underground organization while the five others are employees of Intel Corp. The individuals indicted were charged with conspiracy to infringe on copyrights, which carries a maximum sentence of five years in prison, a $250,000 fine and restitution.* (AP Newswire, May 5, 2000)

Perhaps the most notorious copyright infringement and intellectual property case in 2000 and 2001 involved the music industry. MP3, one of the most popular methods of illegally downloading music from Web sites, lost a court battle waged by the music industry. MP3 was forced to pay millions of dollars to the industry for lost revenues. The rock group Metallic sued Napster.com because it was allowing people to trade copyrighted material illegally. Napster.com lost that battle and is now trying to help the music industry devise a method of charging for downloaded music. So before you copy your favourite sound clip, remember you are actually stealing someone else’s property as surely as if you walked into that person’s home and took the CD.

**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 1900’s, and some simply do not make sense in this day and age. That is what we were referring to in the opening paragraphs of this lecture when we talked about new
Management Information Systems

questions for organizations, companies, and the workplace in general. No issue makes this subject more important than the Internet laws our government has tried, and still tries, to pass.

**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 abuse** extends to any wrongdoing involving equipment and Internet usage. We spoke earlier about anonymity not being a license for socially unacceptable behaviour. You should remember that everything you do on a network or the Internet is recorded and can be tracked. Many people committing computer crimes and abuse have been caught and prosecuted.

**Other Issues**
As managers, you should be acutely aware of the health issues caused by computer usage, especially **repetitive stress injury (RSI)**. Why? Because these health issues costs 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** is increasing as people continually use computer screens and handheld devices that strain eyesight.

It does not 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 is 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.

Too much of a good thing can be bad. You have heard of road rage, the anger people experience when driving. We are now experiencing road rage on the Information Superhighway, and it is called **techno stress**. Managers should encourage their employees to take frequent breaks from their computers and to recognize and understand the dangers of isolation from humans. We may be a wired nation, but we still need the human touch.

How has all this technology affected you? Think about it. Ultimately, there is a positive and a negative side to everything. How you handle it determines how it affects you.

**Management Actions: A Corporate Code of Ethics**
Many firms have not established a Code of Ethics or Employee Conduct for Computing in today's workplace.

Some corporations are confused about what to include and how to approach this new dilemma. Businesses and their managers should recognize:

- The information rights to privacy and freedom
- The property rights to individual ideas and efforts
- The accountability, liability and control issues involved in using technology
- The system quality requirements of businesses and individuals
- The quality of life impact of technology
Companies can no longer ignore the necessity of establishing rules for technology usage. The issue won't go away and will only continue to grow. If you work for a company that does not have a policy, you should encourage it to establish one immediately. If you are a manager in a company, you should get busy and establish a policy for your employees – it is the only fair thing to do.

**THINK POINT**

Does your organisation have a code of ethics? If not, what are some of the rules that you would include regarding the use of technology?

**CASE STUDY**

Read the —Should Google Organize your Medical Records?! Case Study from Page 184 of the text book and answer the questions that follow

*(Answers at the end of this Section)*
SUGGESTED ANSWERS TO SELF-CHECK QUESTIONS

4.1 In what ways are ethical, social, and political issues connected? Give some examples

Ethics refers to principles of right and wrong that individuals use to guide their behavior. Individuals act within a social environment that, in turn, exists within a political environment. Ethical dilemmas are problems that affect society and often are addressed in the political arena. For example, new computer technology makes it easier to gain private information about individuals, creating an ethical dilemma for the potential user of that information (whether or not to invade the privacy of the individual). Society will respond by demanding new laws to regulate the use of data. Students will be able to give a range of examples of this connection.

4.2 Name and describe four “quality of life” impacts of computers and information systems

The textbook describes nine "quality of life" impacts of computers and information systems. These include balancing power, rapidity of change, maintaining boundaries, dependency and vulnerability, computer crime and abuse, computer forensics, employment, equity and access, and health risks.

Balancing power describes the shift toward highly decentralized computing, coupled with an ideology of "empowerment" of thousands of workers and decentralization of decision making to lower organizational levels. The problem is that the lower-level worker involvement in decision making tends to be trivial. Key policy decisions are as centralized as in the past.

The rapidity of change impact suggests that information systems have increased the efficiency of the global marketplace. As a result, businesses no longer have many years to adjust to competition. Businesses can now be wiped out very rapidly, and along with them, jobs. The maintaining boundaries impact suggests that portable computers and telecommuting have created the condition where people can take their work anywhere with them and do it at any time. As a result, workers find that their work is cutting into family time, vacations, and leisure, weakening the traditional institutions of family and friends and blurring the line between public and private life.

The dependency and vulnerability impact suggests that businesses, governments, schools, and private associations are becoming more dependent on information systems, and so they are highly vulnerable to the failure of those systems.

The computer crime and abuse impact suggests that computers have created new opportunities for committing crimes and have themselves become the target of crimes. Computer forensics is the newest field and deals with recovering, storing, and handling data from computers as well as finding information in electronic data and presenting the information to a court.

The employment impact suggests that redesigning business processes could potentially cause millions of middle-level managers and clerical workers to lose their jobs. Worse, if reengineering actually works as claimed, these workers will not find similar employment because the demand...
for their skills will decline. The equity and access impact suggests that access to computer and information resources is not equitably distributed throughout society. Access is distributed inequitably along racial, economic, and social class lines (as are many other information resources). Poor children attending poor school districts are less likely to use computers at school. Children from wealthy homes are five times more likely to use PCs for schoolwork than poor children. Whites are three times more likely to use computers at home for schoolwork than African-Americans. Potentially, we could create a society of information haves and have-nots, further increasing the social cleavages in our society.

Health risks have been attributed to computers and information technologies. For instance, business now spends $20 billion a year to compensate and treat victims of computer-related occupational diseases. Those illnesses include RSI (repetitive stress injury), CVS (computer vision syndrome), and techno stress.

ANSWERS - CASE STUDY

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 America’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.