to hide the crime, and failure to cooperate with prosecutors (U.S. Sentencing Commission, 2004).

Although in the past business firms would often pay for the legal defense of their employees enmeshed in civil charges and criminal investigations, now firms are encouraged to cooperate with prosecutors to reduce charges against the entire firm for obstructing investigations. These developments mean that, more than ever, managers and employees will have to judge for themselves what constitutes proper legal and ethical conduct.

Although these major instances of failed ethical and legal judgment were not master-minded by information systems departments, financial reporting information systems were instrumental in many of these frauds. In many cases, the perpetrators of these crimes artfully used financial reporting information systems to bury their decisions from public scrutiny in the vain hope they would never be caught. We deal with the issue of control in financial reporting and other information systems in Chapter 10. In this chapter we talk about the ethical dimensions of these and other actions based on the use of information systems.

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, telephone, and radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property.

Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protect the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, What is the ethical and socially responsible course of action?

A Model for Thinking About Ethical, Social, and Political Issues

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure 5-1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed

well-honed rules of behavior, and these are backed by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. But imagine instead of a rock that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. What happens? Ripples, of course.

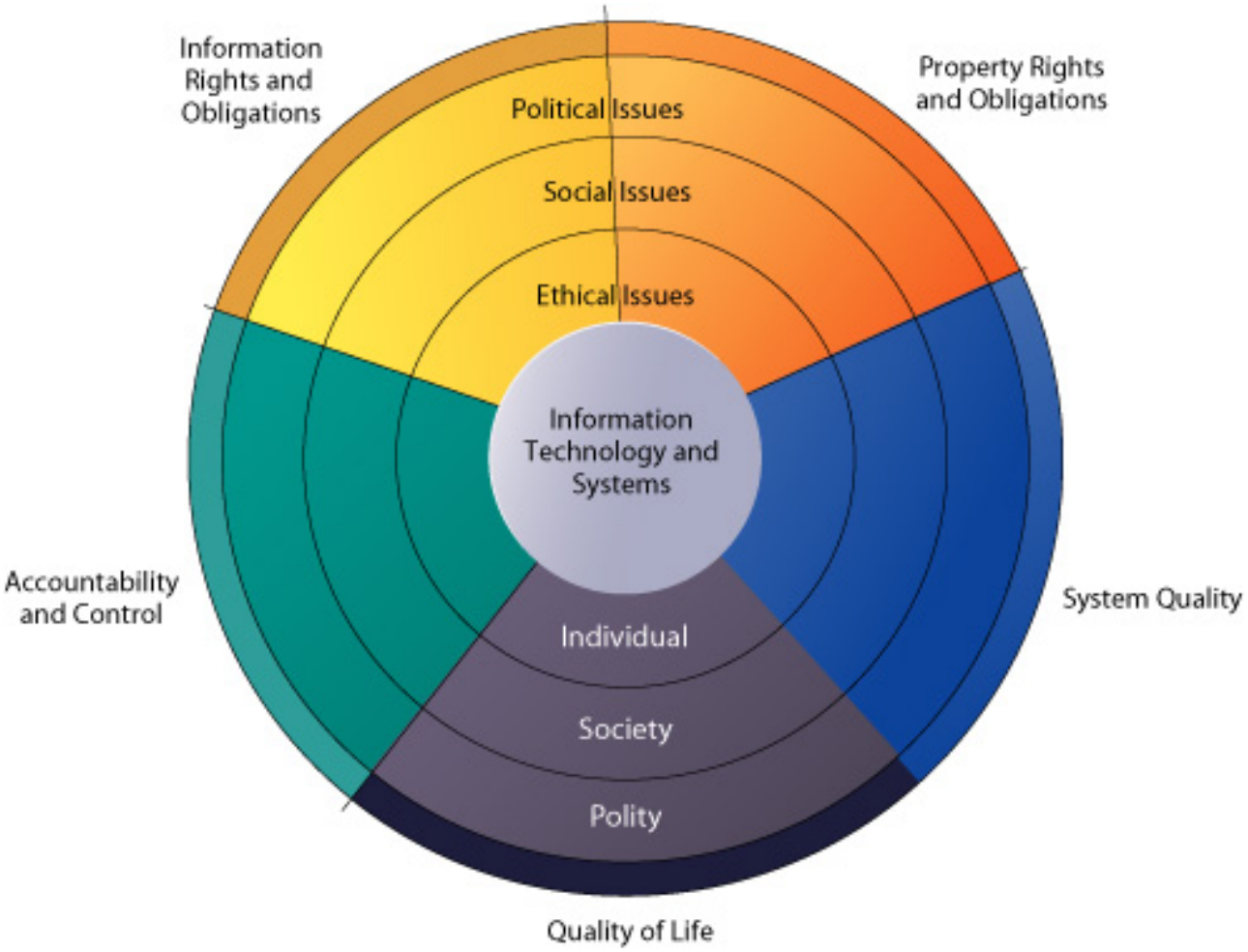


FIGURE 5-1 The relationship between ethical, social, and political issues in an information society

The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Suddenly individual actors are confronted with new situations often not covered by the old rules. Social institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, social responsibility, politically correct attitudes, or approved rules. Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime,

you may have to act. You may be forced to act in a legal gray area.

We can use this model to illustrate the dynamics that connect ethical, social, and political issues. This model is also useful for identifying the main moral dimensions of the information society, which cut across various levels of action—individual, social, and political.

Return to Top

Five Moral Dimensions of the Information Age

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

- *Information rights and obligations.* What information rights do individuals and organizations possess with respect to information about themselves? What can they protect? What obligations do individuals and organizations have concerning this information?
- *Property rights and obligations*. How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?
- *Accountability and control*. Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?
- *System quality*. What standards of data and system quality should we demand to protect individual rights and the safety of society?
- *Quality of life*. What values should be preserved in an information-and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

We explore these moral dimensions in detail in section 5.3.

Return to Top

Key Technology Trends That Raise Ethical Issues

Ethical issues long preceded information technology. Nevertheless, information technology has heightened ethical concerns, taxed existing social arrangements, and made some laws obsolete or severely crippled. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 5-2.

TABLE 5-2 Technology Trends That Raise Ethical Issues

Trend	Impact
Computing power doubles every 18 months	More organizations depend on computer systems for critical operations.
Rapidly declining data storage costs	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.

The doubling of computing power every 18 months has made it possible for most organizations to use information systems for their core production processes. As a result, our dependence on systems and our vulnerability to system errors and poor data quality have increased. Social rules and laws have not yet adjusted to this dependence. Standards for ensuring the accuracy and reliability of information systems (see Chapter 10) are not universally accepted or enforced.

Advances in data storage techniques and rapidly declining storage costs have been responsible for the multiplying databases on individuals—employees, customers, and potential customers—maintained by private and public organizations. These advances in data storage have made the routine violation of individual privacy both cheap and effective. Already massive data storage systems are cheap enough for regional and even local retailing firms to use in identifying customers.

Advances in data analysis techniques for large pools of data are a third technological trend that heightens ethical concerns because companies and government agencies are able to find out much detailed personal information about individuals. With contemporary data management tools (see Chapter 7) companies can assemble and combine the myriad pieces of information about you stored on computers much more easily than in the past.

Think of all the ways you generate computer information about yourself—credit card purchases, telephone calls, magazine subscriptions, video rentals, mail-order purchases, banking records, and local, state, and federal government records (including court and police records). Put together and mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, and your political interests.

Companies with products to sell purchase relevant information from these sources to help them more finely target their marketing campaigns. Chapters 3 and 7 describe how companies can analyze large pools of data from multiple sources to rapidly identify buying patterns of customers and suggest individual responses. The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called profiling.

For example, hundreds of Web sites allow DoubleClick (www.doubleclick.net), an

Internet advertising broker, to track the activities of their visitors in exchange for revenue from advertisements based on visitor information DoubleClick gathers. DoubleClick uses this information to create a profile of each online visitor, adding more detail to the profile as the visitor accesses an associated DoubleClick site. Over time, DoubleClick can create a detailed dossier of a person's spending and computing habits on the Web that can be sold to companies to help them target their Web ads more precisely.

Credit card purchases can make personal information available to market researchers, telemarketers, and direct mail companies. Advances in information technology facilitate the invasion of privacy.

A new data analysis technology called nonobvious relationship awareness (NORA) has given both government and the private sector even more powerful profiling capabilities. NORA can take information about people from many disparate sources, such as employment applications, telephone records, customer listings, and "wanted" lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists (see Figure 5-2).

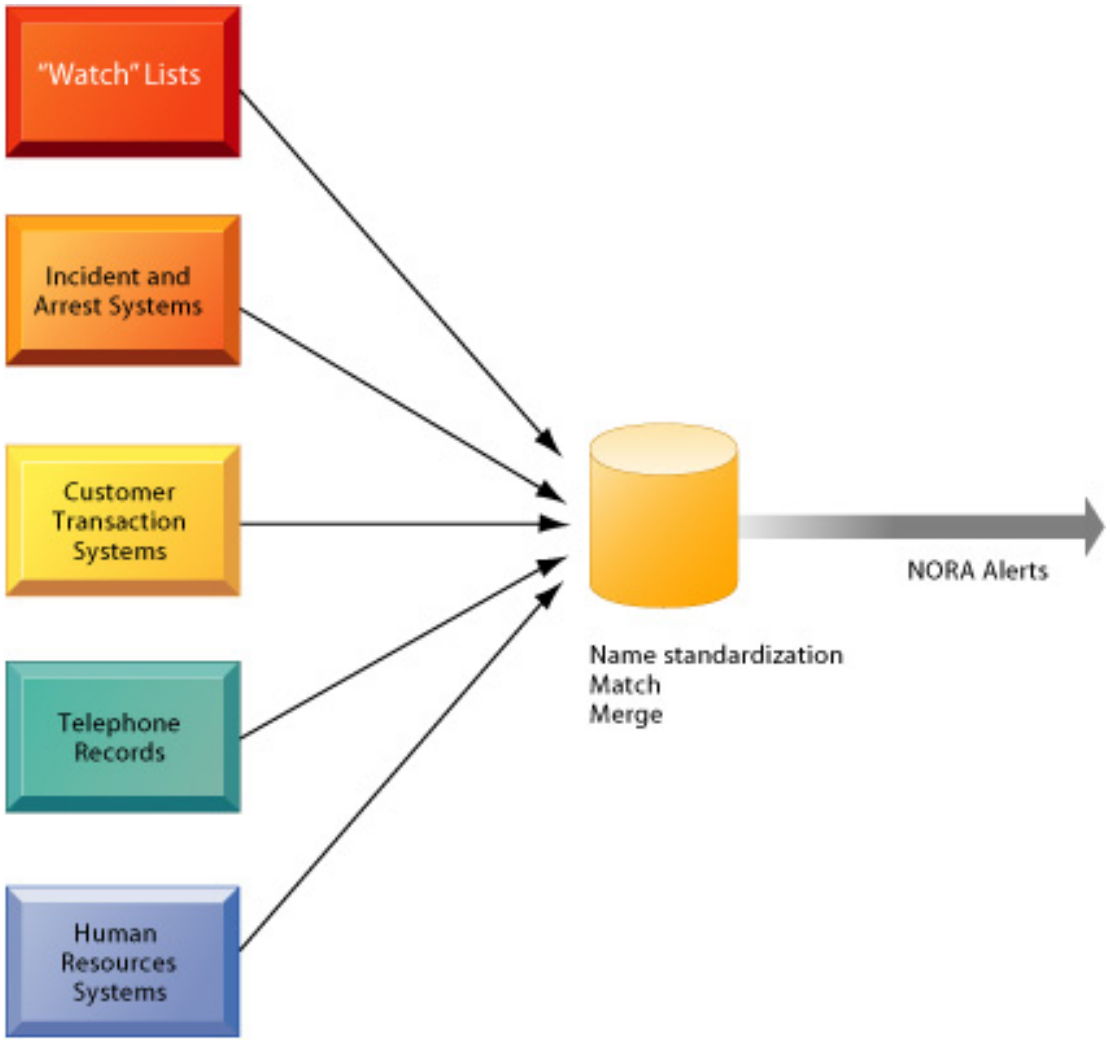


FIGURE 5-2 Nonobvious Relationship Awareness (NORA)
NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool for homeland security but does have privacy implications because it can provide such a detailed picture of the activities and associations of a single individual (Barrett and Gallagher, 2004).

Last, advances in networking, including the Internet, promise to reduce greatly the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely using small desktop machines, permitting an invasion of privacy on a scale and with a precision heretofore unimaginable. If computing and networking technologies continue to advance at the same pace as in the past, by 2023 large organizations will be able to devote the equivalent of a contemporary desktop personal computer to monitoring each of the 350 million individuals who will then be living in the United States (Farmer and Mann, 2003).

The development of global digital superhighway communication networks widely available to individuals and businesses poses many ethical and social concerns. Who will account for the flow of information over these networks? Will you be able to trace information collected about you? What will these networks do to the traditional relationships between family, work, and leisure? How will traditional job designs be altered when millions of “employees” become subcontractors using mobile offices for which they themselves must pay?

In the next section we consider some ethical principles and analytical techniques for dealing with these kinds of ethical and social concerns.

Return to Top

ETHICS IN AN INFORMATION SOCIETY

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

Basic Concepts: Responsibility, Accountability, and Liability

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. Responsibility is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make. Accountability is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. Liability extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. Due process is a related feature of law-governed societies and is a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them. First, as discussed in Chapter 3, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behaviors. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

Return to Top

Ethical Analysis

When confronted with a situation that seems to present ethical issues, how

should you analyze it? The following five-step process should help.

1. *Identify and describe clearly the facts.* Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.

2. *Define the conflict or dilemma and identify the higher-order values involved.* Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-ending case study illustrates two competing values: the need to protect citizens from terrorist acts and the need to protect individual privacy.

3. *Identify the stakeholders.* Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions (Smith, 2003). Find out the identity of these groups and what they want. This will be useful later when designing a solution.

4. *Identify the options that you can reasonably take.* You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.

5. *Identify the potential consequences of your options.* Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, “What if I choose this option consistently over time?”

CANDIDATE ETHICAL PRINCIPLES

Once your analysis is complete, what ethical principles or rules should you use to make a decision? What higher-order values should inform your judgment? Although you are the only one who can decide which among many ethical principles you will follow, and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history.

1. Do unto others as you would have them do unto you (the Golden Rule). Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.

2. If an action is not right for everyone to take, it is not right for anyone (Immanuel Kant's Categorical Imperative). Ask yourself, "If everyone did this, could the organization, or society, survive?"

3. If an action cannot be taken repeatedly, it is not right to take at all (Descartes' rule of change). This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if repeated would bring unacceptable changes in the long run. In the vernacular, it might be stated as "once started down a slippery path you may not be able to stop."

4. Take the action that achieves the higher or greater value (the Utilitarian Principle). This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.

- Take the action that produces the least harm, or the least potential cost (Risk Aversion Principle). Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid these high-failure-cost actions, paying greater attention obviously to high-failure-cost potential of moderate to high probability.
- Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the ethical "no free lunch" rule.) If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work.

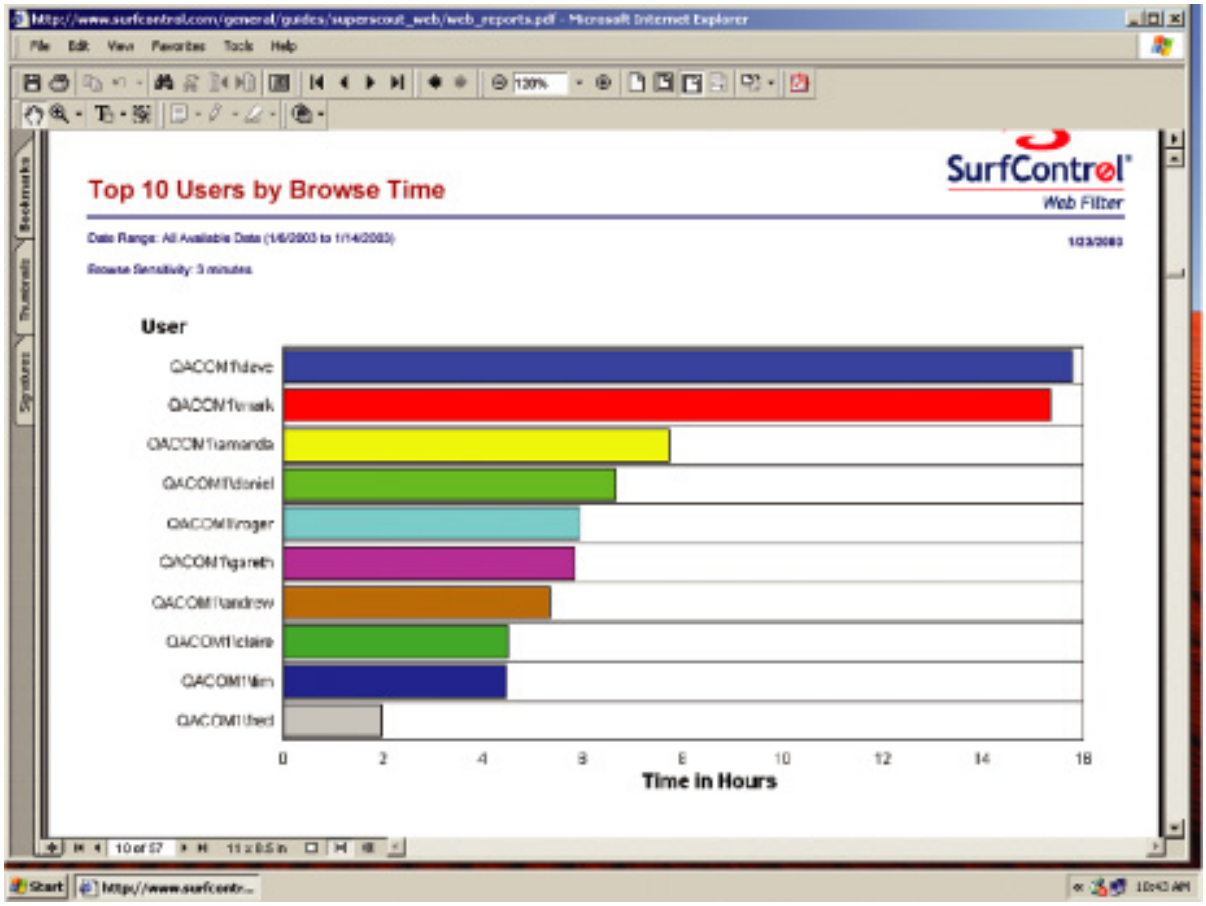
Although these ethical rules cannot always be guides to action, actions that do not easily pass these rules deserve some very close attention and a great deal of caution. The appearance of unethical behavior may do as much harm to you and your company as actual unethical behavior.

Return to Top

Professional Codes of Conduct

When groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect. Professional codes of conduct are promulgated by associations of professionals such as the American Medical Association (AMA), the American Bar Association (ABA), the Association of Information Technology Professionals (AITP), and the Association of Computing Machinery (ACM). These professional groups take responsibility for the partial regulation of their professions by

determining entrance qualifications and competence. Codes of ethics are promises by professions to regulate themselves in the general interest of society. For example, avoiding harm to others, honoring property rights (including intellectual property), and respecting privacy are among the General Moral Imperatives of the ACM's Code of Ethics and Professional Conduct (ACM, 1993).



SurfControl offers tools for tracking Web and e-mail activity and for filtering unauthorized e-mail and Web site content. The benefits of monitoring employee e-mail and Internet use should be balanced with the need to respect employee privacy.

Return to Top

Some Real-World Ethical Dilemmas

Information systems have created new ethical dilemmas in which one set of interests is pitted against another. For example, many of the large telephone companies in the United States are using information technology to reduce the sizes of their workforces. Voice recognition software reduces the need for human operators by enabling computers to recognize a customer's responses to a series of computerized questions. Many companies monitor what their

employees are doing on the Internet to prevent them from wasting company resources on nonbusiness activities (see the Chapter 8 Window on Management).

In each instance, you can find competing values at work, with groups lined on either side of a debate. A company may argue, for example, that it has a right to use information systems to increase productivity and reduce the size of its workforce to lower costs and stay in business. Employees displaced by information systems may argue that employers have some responsibility for their welfare. Business owners might feel obligated to monitor employee e-mail and Internet use to minimize drains on productivity (Jackson, Dawson, and Wilson, 2003; Urbaczewski and Jessup, 2002). Employees might believe they should be able to use the Internet for short personal tasks in place of the telephone. A close analysis of the facts can sometimes produce compromised solutions that give each side “half a loaf.” Try to apply some of the principles of ethical analysis described to each of these cases. What is the right thing to do?

Return to Top

THE MORAL DIMENSIONS OF INFORMATION SYSTEMS

In this section, we take a closer look at the five moral dimensions of information systems first described in Figure 5-1. In each dimension we identify the ethical, social, and political levels of analysis and use real-world examples to illustrate the values involved, the stakeholders, and the options chosen.

Information Rights: Privacy and Freedom in the Internet Age

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance (Ball, 2001). Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

The claim to privacy is protected in the U.S., Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. In the United States, the claim to privacy is protected primarily by First Amendment guarantees of freedom of speech and association, Fourth Amendment protections against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process.

Table 5-3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information. At present, most U.S. federal privacy laws apply only to the federal government and regulate very few areas of the private sector.

TABLE 5-3 Federal Privacy Laws in the United States

GENERAL FEDERAL PRIVACY LAWS
Freedom of Information Act of 1966 as Amended (5 USC 552)
Privacy Act of 1974 as Amended (5 USC 552a)
Electronic Communications Privacy Act of 1986
Computer Matching and Privacy Protection Act of 1988
Computer Security Act of 1987
Federal Managers Financial Integrity Act of 1982
PRIVACY LAWS AFFECTING PRIVATE INSTITUTIONS
Fair Credit Reporting Act of 1970
Family Educational Rights and Privacy Act of 1974
Right to Financial Privacy Act of 1978
Privacy Protection Act of 1980
Cable Communications Policy Act of 1984
Electronic Communications Privacy Act of 1986
Video Privacy Protection Act of 1988
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Children's Online Privacy Protection Act of 1998 (COPPA)
Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999

Most American and European privacy law is based on a regime called Fair Information Practices (FIP) first set forth in a report written in 1973 by a federal government advisory committee (U.S. Department of Health, Education, and Welfare, 1973). Fair Information Practices (FIP) 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. The individual has an interest in engaging in a transaction, and the record keeper—usually a business or government agency—requires information about the individual to support the transaction. Once information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, the Federal Trade Commission (FTC) restated and extended the original FIP to provide guidelines for protecting online privacy. Table 5-4 describes the FTC's Fair Information Practices principles.

TABLE 5-4 Federal Trade Commission Fair Information Practices Principles

1.	*Notice/Awareness (core principle)*: Web sites must disclose their information practices before collecting data. Includes identification of collector; uses of data; other recipients of data; nature of collection (active/inactive); voluntary or required status; consequences of refusal; and steps taken to protect confidentiality, integrity, and quality of the data.
2.	*Choice/Consent (core principle)*: There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
3.	*Access/Participation:* Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
4.	*Security:* Data collectors must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
5.	*Enforcement:* There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulations.

The FTC's FIP are being used as guidelines to drive changes in privacy legislation. In July 1998, the U.S. Congress passed the Children's Online Privacy Protection Act (COPPA), requiring Web sites to obtain parental permission before collecting information on children under the age of 13. (This law is in danger of being overturned.) The FTC has recommended additional legislation to protect online consumer privacy in advertising networks that collect records of consumer Web activity to develop detailed profiles that are then used by other companies to target online ads. Other proposed Internet privacy legislation focuses on protecting the online use of personal identification numbers such as Social Security numbers, protecting personal information collected on the Internet that deals with individuals not covered by the Children's Online Privacy Protection Act of 1998, and limiting the use of data mining for homeland security (see the chapter-ending case study).

Privacy protections have also been added to recent laws deregulating financial services and safeguarding the maintenance and transmission of health information about individuals. The Gramm-Leach-Bliley Act of 1999, which repeals earlier restrictions on affiliations among banks, securities firms, and insurance companies, includes some privacy protection for consumers of financial services. All financial institutions are required to disclose their policies and practices for protecting the privacy of nonpublic personal information and to allow customers to opt out of information-sharing arrangements with nonaffiliated third parties.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which took effect on April 14, 2003, includes privacy protection for medical records. The law gives patients access to their personal medical records maintained by health care providers, hospitals, and health insurers and the right to authorize how protected information about themselves can be used or disclosed. Doctors, hospitals, and other health care providers must limit the disclosure of personal information about patients to the minimum necessary to achieve a given purpose.

THE EUROPEAN DIRECTIVE ON DATA PROTECTION

In Europe, privacy protection is much more stringent than in the United States. Unlike the United States, European countries do not allow businesses to use personally identifiable

information without consumers' prior consent. On October 25, 1998, the European Commission's Directive on Data Protection went into effect, broadening privacy protection in the European Union (EU) nations. The directive requires companies to inform people when they collect information about them and disclose how it will be stored and used. Customers must provide their informed consent before any company can legally use data about them, and they have the right to access that information, correct it, and request that no further data be collected. Informed consent can be defined as consent given with knowledge of all the facts needed to make a rational decision. EU member nations must translate these principles into their own laws and cannot transfer personal data to countries such as the United States that do not have similar privacy protection regulations.

Working with the European Commission, the U.S. Department of Commerce developed a safe harbor framework for U.S. firms. A safe harbor is a private self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement. U.S. businesses would be allowed to use personal data from EU countries if they develop privacy protection policies that meet EU standards. Enforcement would occur in the United States, using self-policing, regulation, and government enforcement of fair trade statutes.

INTERNET CHALLENGES TO PRIVACY

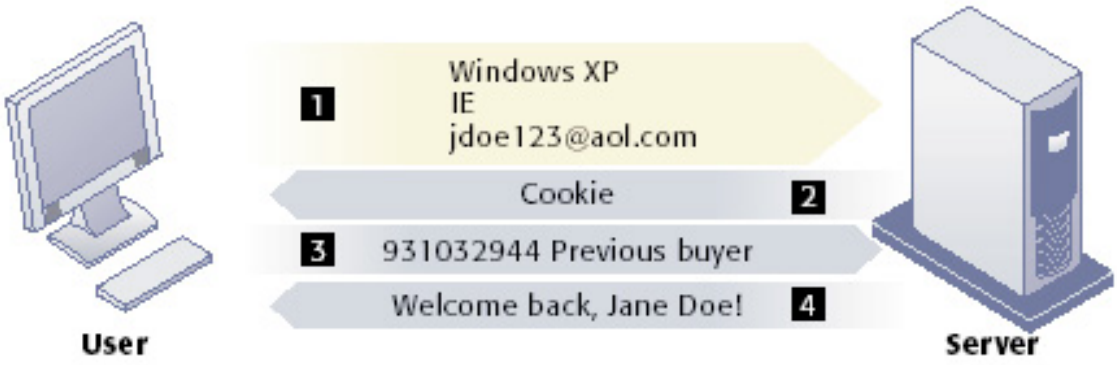
Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

It is possible to record many online activities, including which online newsgroups or files a person has accessed, which Web sites and Web pages he or she has visited, and what items that person has inspected or purchased over the Web. Much of this monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. Tools to monitor visits to the World Wide Web have become popular because they help organizations determine who is visiting their Web sites and how to better target their offerings. (Some firms also monitor the Internet usage of their employees to see how they are using company network resources.) Web retailers now have access to software that lets them "watch" the online shopping behavior of individuals and groups while they are visiting a Web site and making purchases. The commercial demand for this personal information is virtually insatiable.

Web sites can learn the identities of their visitors if the visitors voluntarily register at the site to purchase a product or service or to obtain a free service, such as information. Web sites can also capture information about visitors without their knowledge using cookie technology.

Cookies are tiny files deposited on a computer hard drive when a user visits certain Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize its contents for each visitor's interests. For example, if you purchase

a book on the Amazon.com Web site and return later from the same browser, the site will welcome you by name and recommend other books of interest based on your past purchases. DoubleClick, introduced earlier in this chapter, uses cookies to build its dossiers with details of online purchases and to examine the behavior of Web site visitors. Figure 5-3 illustrates how cookies work.



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

FIGURE 5-3 How cookies identify Web visitors

Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

Web sites using cookie technology cannot directly obtain visitors' names and addresses. However, if a person has registered at a site, that information can be combined with cookie data to identify the visitor. Web site owners can also combine the data they have gathered from cookies and other Web site monitoring tools with personal data from other sources such as offline data collected from surveys or paper catalog purchases to develop very detailed profiles of their visitors.

There are now even more subtle and surreptitious tools for surveillance of Internet users. Marketers use Web bugs as another tool to monitor online behavior. Web bugs are tiny graphic files embedded in e-mail messages and Web pages that are designed to monitor who is reading the e-mail message or Web page and transmit that information to another computer. Other spyware can secretly install itself on an Internet user's computer by piggybacking on larger applications. Once installed, the spyware calls out to Web sites to send banner ads and other

unsolicited material to the user, and it can also report the user's movements on the Internet to other computers. You will learn more about Web bugs, spyware, and other intrusive software in Chapter 10.

Google has been using tools to scan the contents of messages received by users of its free Web-based e-mail service called Gmail. Ads that users see when they read their e-mail are related to the subjects of these messages. Google's service offers users 1 gigabyte of storage space—far more than any of its competitors—but privacy advocates find the practice offensive (Hansell, 2004).

The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other marketing purposes without obtaining the informed consent of the individual whose information is being used. U.S. e-commerce sites are largely content to publish statements on their Web sites informing visitors about how their information will be used. Some have added opt-out selection boxes to these information policy statements. An opt-out model of informed consent permits the collection of personal information until the consumer specifically requests that the data not be collected. Privacy advocates would like to see wider use of an opt-in model of informed consent in which a business is prohibited from collecting any personal information unless the consumer specifically takes action to approve information collection and use.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. In 1998, the online industry formed the Online Privacy Alliance to encourage self-regulation to develop a set of privacy guidelines for its members. The group promotes the use of online seals, such as that of TRUSTe, certifying Web sites adhering to certain privacy principles. Members of the advertising network industry, including DoubleClick, Atlas DMT, ValueClick, and 24/7 Real Media, have created an additional industry association called the Network Advertising Initiative (NAI) to develop its own privacy policies to help consumers opt out of advertising network programs and provide consumers redress from abuses.

In general, however, most Internet businesses do little to protect the privacy of their customers, and consumers do not do as much as they should to protect themselves. Many companies with Web sites do not have privacy policies. Of the companies that do post privacy polices on their Web sites, about half do not monitor their sites to ensure they adhere to these policies. The vast majority of online customers claim they are concerned about online privacy, but less than half read the privacy statements on Web sites (Laudon and Traver, 2004).

Internet Connection

The Internet Connection for this chapter will direct you to a series of Web sites where you can learn about the privacy issues raised by the Internet and the Web. You can complete an exercise to analyze the privacy implications of existing technologies for tracking Web site visitors.

TECHNICAL SOLUTIONS

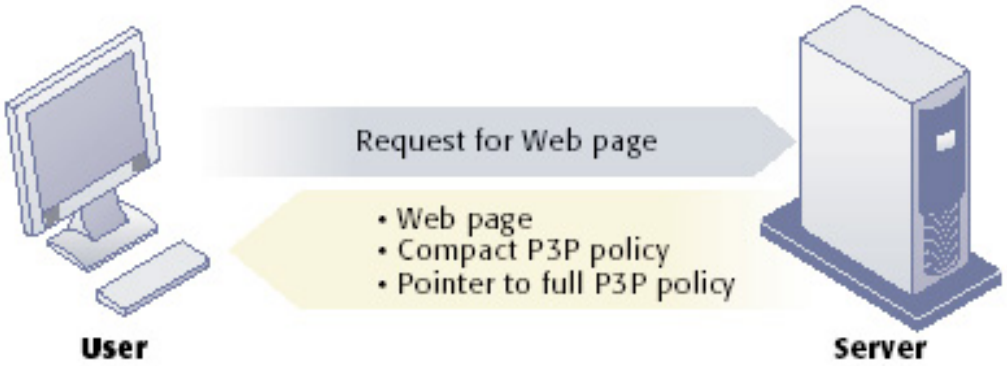
In addition to legislation, new technologies are available to protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware.

There are now tools to help users determine the kind of personal data that can be extracted by Web sites. The Platform for Privacy Preferences, known as P3P, enables automatic communication of privacy policies between an e-commerce site and its visitors. P3P provides a standard for communicating a Web site's privacy policy to Internet users and for comparing that policy to the user's preferences or to other standards such as the FTC's new FIP guidelines or the European Directive on Data Protection. Users can use P3P to select the level of privacy they wish to maintain when interacting with the Web site.

Web sites are starting to post their privacy policies for visitors to review. The TRUSTe seal designates Web sites that have agreed to adhere to TRUSTe's established privacy principles of disclosure, choice, access, and security.

The P3P standard allows Web sites to publish privacy policies in a form that computers can understand. Once it is codified according to P3P rules, the privacy policy becomes part of the software for individual Web pages (see Figure 5-4).

Users of recent versions of Microsoft Internet Explorer Web browsing software can access and read the P3P site's privacy policy and a list of all cookies coming from the site. Internet Explorer enables users to adjust their computers to screen out all cookies or let in selected cookies based on specific levels of privacy. For example, the "medium" level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy.



1. The user with P3P Web browsing software requests a Web page.
2. The Web server returns the Web page along with a compact version of the Web site's policy and a pointer to the full P3P policy. If the Web site is not P3P compliant, no P3P data are returned.
3. The user's Web browsing software compares the response from the Web site with the user's privacy preferences. If the Web site does not have a P3P policy or the policy does not match the privacy levels established by the user, it warns the user or rejects the cookies from the Web site. Otherwise, the Web page loads normally.

FIGURE 5-4 The P3P standard

P3P enables Web sites to translate their privacy policies into a standard format that can be read by the user's Web browser software. The user's Web browser software evaluates the Web site's privacy policy to determine whether it is compatible with the user's privacy preferences.

However, P3P only works with Web sites of members of the World Wide Web Consortium who have translated their Web site privacy policies into P3P format. The technology will display cookies from Web sites that are not part of the consortium, but users will not be able to obtain sender information or privacy statements. Many users may also need to be educated about interpreting company privacy statements and P3P levels of privacy.

ETHICAL ISSUES

The ethical privacy issue in this information age is as follows: Under what conditions should I (you) invade the privacy of others? What legitimates intruding into others' lives through unobtrusive surveillance, through market research, or by whatever means? Do we have to inform people that we are eavesdropping? Do we have to inform people that we are using credit history information for employment

screening purposes?

SOCIAL ISSUES

The social issue of privacy concerns the development of expectations of privacy, or privacy norms, as well as public attitudes. In what areas of life should we as a society encourage people to think they are in private territory as opposed to public view? For instance, should we as a society encourage people to develop expectations of privacy when using electronic mail, cellular telephones, bulletin boards, the postal system, the workplace, or the street? Should expectations of privacy be extended to criminal conspirators?

POLITICAL ISSUES

The political issue of privacy concerns the development of statutes that govern the relations between record keepers and individuals. Should we permit the FBI to monitor e-mail at will to apprehend suspected criminals and terrorists (see the chapter-ending case study). To what extent should e-commerce sites and other businesses be allowed to maintain personal data about individuals?

Return to Top

Property Rights: Intellectual Property

Contemporary information systems have severely challenged existing law and social practices that protect private intellectual property. Intellectual property is considered to be intangible property created by individuals or corporations. Information technology has made it difficult to protect intellectual property because computerized information can be so easily copied or distributed on networks. Intellectual property is subject to a variety of protections under three different legal traditions: trade secret, copyright, and patent law.

TRADE SECRETS

Any intellectual work product—a formula, device, pattern, or compilation of data—used for a business purpose can be classified as a trade secret, provided it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly.

Software that contains novel or unique elements, procedures, or compilations can be included as a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make this claim, the creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

The limitation of trade secret protection is that although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software

is widely distributed.

COPYRIGHT

Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death. For corporate-owned works, copyright protection lasts for 95 years after their initial creation. Congress has extended copyright protection to books, periodicals, lectures, dramas, musical compositions, maps, drawings, artwork of any kind, and motion pictures. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

In the mid-1960s, the Copyright Office began registering software programs, and in 1980 Congress passed the Computer Software Copyright Act, which clearly provides protection for software program code and for copies of the original sold in commerce, and sets forth the rights of the purchaser to use the software while the creator retains legal title.

Copyright protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that the underlying ideas behind a work are not protected, only their manifestation in a work. A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright.

"Look and feel" copyright infringement lawsuits are precisely about the distinction between an idea and its expression. For instance, in the early 1990s Apple Computer sued Microsoft Corporation and Hewlett-Packard for infringement of the expression of Apple's Macintosh interface, claiming that the defendants copied the expression of overlapping windows. The defendants countered that the idea of overlapping windows can be expressed only in a single way and, therefore, was not protectable under the merger doctrine of copyright law. When ideas and their expression merge, the expression cannot be copyrighted.

In general, courts appear to be following the reasoning of a 1989 case—*Brown Bag Software v. Symantec Corp.*—in which the court dissected the elements of software alleged to be infringing. The court found that similar concept, function, general functional features (e.g., drop-down menus), and colors are not protectable by copyright law (*Brown Bag v. Symantec Corp., 1992*).

PATENTS

A patent grants the owner an exclusive monopoly on the ideas behind an invention for 20 years. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or methods receive the full financial and other rewards of their labor and yet still make widespread use of the invention possible by

providing detailed diagrams for those wishing to use the idea under license from the patent's owner. The granting of a patent is determined by the Patent Office and relies on court rulings.

The key concepts in patent law are originality, novelty, and invention. The Patent Office did not accept applications for software patents routinely until a 1981 Supreme Court decision that held that computer programs could be a part of a patentable process. Since that time, hundreds of patents have been granted and thousands await consideration.

The strength of patent protection is that it grants a monopoly on the underlying concepts and ideas of software. The difficulty is passing stringent criteria of nonobviousness (e.g., the work must reflect some special understanding and contribution), originality, and novelty, as well as years of waiting to receive protection.

CHALLENGES TO INTELLECTUAL PROPERTY RIGHTS

Contemporary information technologies, especially software, pose severe challenges to existing intellectual property regimes and, therefore, create significant ethical, social, and political issues. Digital media differ from books, periodicals, and other media in terms of ease of replication; ease of transmission; ease of alteration; difficulty classifying a software work as a program, book, or even music; compactness—making theft easy; and difficulties in establishing uniqueness.

The proliferation of electronic networks, including the Internet, has made it even more difficult to protect intellectual property. Before widespread use of networks, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed. A study conducted by the International Data Corporation for the Business Software Alliance found more than onethird of the software worldwide was counterfeit or pirated and the Business Software Alliance reported $29 billion in yearly losses from software piracy (Geitner 2004; Lohr, 2004).

The proliferation of electronic networks, including the Internet, has made it even more difficult to protect intellectual property. Before widespread use of networks, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed. A study conducted by the International Data Corporation for the Business Software Alliance found more than onethird of the software worldwide was counterfeit or pirated and the Business Software Alliance reported $29 billion in yearly losses from software piracy (Geitner 2004; Lohr, 2004).

Individuals have been illegally copying and distributing digitized MP3 music files on the Internet. Napster provided software and services that enabled users to locate and share digital music files, including those protected by copyright. In February 2001, a U.S. federal district court ruled that Napster had to stop listing all copyrighted files without permission on its central index and the company was

forced to declare bankruptcy. (It eventually became a Web site selling only legal music downloads.)

Major entertainment industry groups subsequently filed suit to block illegal file sharing on other Web sites, such as Madster, Grokster, Kazaa, and Morpheus. However, these sites, as well as software and services for file trading over the Web, such as Gnutella, cannot be so easily regulated, so copyrighted music continues to be traded for free. Illegal file sharing is so widespread that it is threatening the viability of the music recording industry. (More detail on this topic can be found in the case study concluding Chapter 4.) As more and more homes adopt high-speed Internet access, illegal file sharing of videos will pose similar threats to the motion picture industry.

The manner in which information is obtained and presented on the Web further challenges intellectual property protections. Web pages can be constructed from bits of text, graphics, sound, or video that may come from many different sources. Each item may belong to a different entity, creating complicated issues of ownership and compensation (see Figure 5-5). Web sites use a capability called framing to let one site construct an on-screen border around content obtained by linking to another Web site. The first site's border and logo stay on-screen, making the content of the new Web site appear to be offered by the previous Web site.