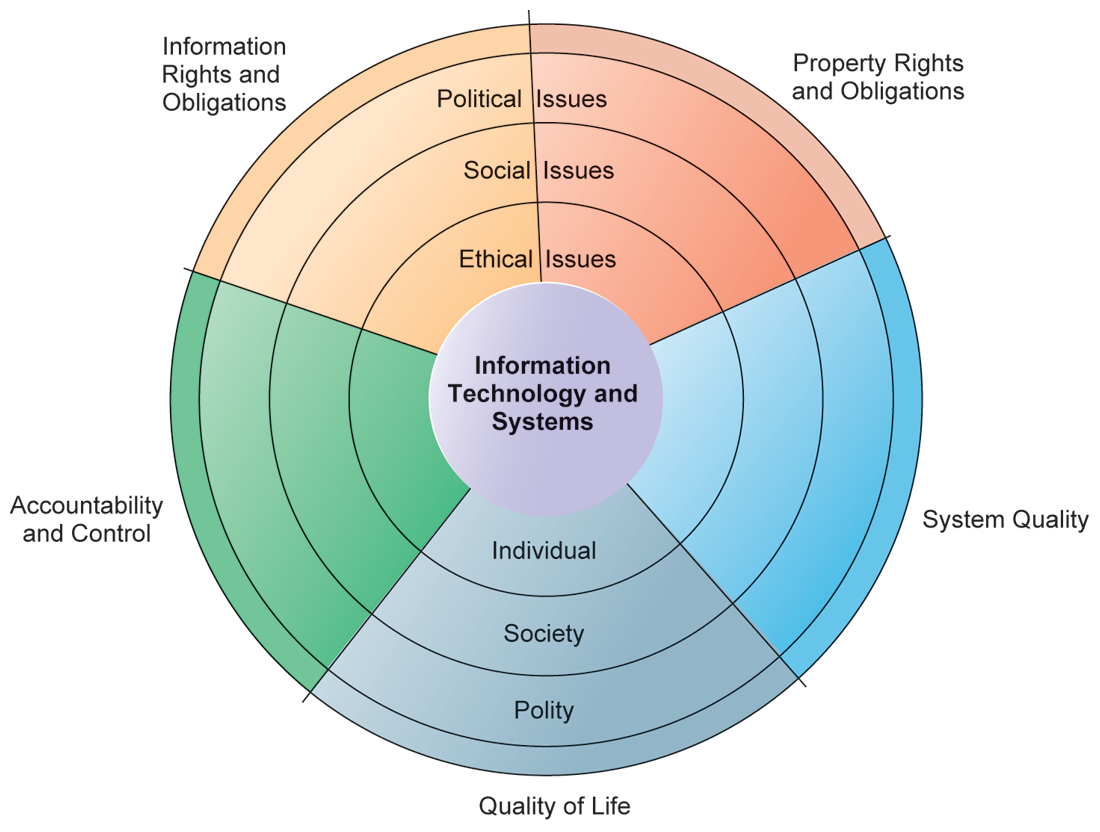
**Ethical and Social Issues in Information Systems**

**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, the telephone, and the 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**.

**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 shown in Figure 4.1. 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 supported 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. What happens? **Ripples, of course**. Imagine instead that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. 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.



**FIVE MORAL DIMENSIONS OF THE INFORMATION AGE**

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

1. **Information rights and obligations.** What information rights do individuals and organizations possess with respect to themselves? What can they protect?
2. **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?
3. **Accountability and control.** Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?
4. **System quality.** What standards of data and system quality should we demand to protect individual rights and the safety of society?
5. **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?

**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 five key technological trends responsible for these ethical stresses.

* Doubling of computer power

• More organizations depend on computer systems for critical operations.

* Rapidly declining data storage costs

• Organizations can easily maintain detailed databases on individuals.

* Networking advances and the Internet

• Copying data from one location to another and accessing personal data from remote locations are much easier.

* Advances in data analysis techniques

• Profiling –Combining data from multiple sources to create dossiers of detailed information on individuals

• Nonobvious relationship awareness (NORA) –Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists

* Mobile device growth

• Tracking of individual cell phones

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 8) 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. Very large data storage systems capable of working with terabytes of data are inexpensive enough for large firms to use in identifying customers.

Advances in data analysis techniques for large pools of data are another technological trend that heightens ethical concerns because companies and government agencies are able to find out highly detailed personal information about individuals. With contemporary data management tools, 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, local, state, and federal government records (including court and police records), and visits to Web sites. Put together and mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, what you read and watch, and your political interests. Companies with products to sell purchase relevant information from these sources to help them more finely target their marketing campaigns.

The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called profiling. For example, several thousand of the most popular Web sites allow DoubleClick (owned by Google), 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 is sold to companies to help them target their Web ads more precisely. ChoicePoint gathers data from police, criminal, and motor vehicle records, credit and employment histories, current and previous addresses, professional licenses, and insurance claims to assemble and maintain electronic dossiers on almost every adult in the United States. The company sells this personal information to businesses and government agencies. Demand for personal data is so enormous that data broker businesses such as ChoicePoint are flourishing. In 2011, the two largest credit card networks, Visa Inc. and MasterCard Inc., were planning to link credit card purchase information with consumer social network and other information to create customer profiles that could be sold to advertising firms. In 2012, Visa will process more than 45 billion transactions a year and MasterCard will process more than 23 billion transactions. Currently, this transactional information is not linked with consumer Internet activities.

A new data analysis technology called nonobvious relationship awareness (NORA) has given both the 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. 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.

Finally, advances in networking, including the Internet, promise to greatly reduce 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.

**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 4.1. 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.

1. **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. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

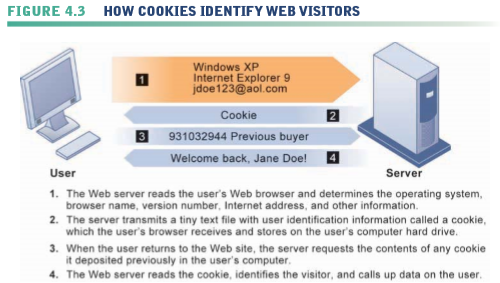
**Internet Challenges to Privacy**

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.

Web sites track searches that have been conducted, the Web sites and Web pages visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. This monitoring and tracking of Web site visitors occurs in the background without the visitor’s knowledge. It is conducted not just by individual Web sites but by advertising networks such as Microsoft Advertising, Yahoo, and DoubleClick that are capable of tracking personal browsing behavior across thousands of Web sites. Both Web site publishers and the advertising industry defend tracking of individuals across the Web because doing so allows more relevant ads to be targeted to users, and it pays for the cost of publishing Web sites. In this sense, it’s like broadcast television: advertiser-supported content that is free to the user. The commercial demand for this personal information is virtually insatiable.

**Cookies** are small text files deposited on a computer hard drive when a user visits 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 content for each visitor’s interests. For example, if you purchase a book on Amazon.com 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, described 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 4.3 illustrates how cookies work.

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. So-called “super cookies” or Flash cookies cannot be easily deleted and can be installed whenever a person clicks on a Flash video. These so-called “Local Shared Object” files are used by Flash to play videos and are put on the user’s computer without their consent.



Marketers use **Web beacons** as another tool to monitor online behavior. Web beacons, also called Web bugs (or simply “tracking files”), are tiny software programs that keep a record of users’ online clickstream and report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail. Web beacons are placed on popular Web sites by third-party firms who pay the Web sites a fee for access to their audience. So how common is Web tracking?

Some popular sites such as Dictionary. com, MSN, and Comcast, installed more than 100 tracking files! Two-thirds of the tracking files came from 131 companies whose primary business is identifying and tracking Internet users to create consumer profiles that can be sold to advertising firms looking for specific types of customers. The biggest trackers were Google, Microsoft, and Quantcast, all of whom are in the business of selling ads to advertising firms and marketers.

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 report the user’s movements on the Internet to other computers.

About 75 percent of global Internet users use Google Search and other Google services, making Google the world’s largest collector of online user data. Whatever Google does with its data has an enormous impact on online privacy. Most experts believe that Google possesses the largest collection of personal information in the world—more data on more people than any government agency. The nearest competitor is Facebook.

After Google acquired the advertising network DoubleClick in 2007, Google has been using behavioral targeting to help it display more relevant ads based on users’ search activities and to target individuals as they move from one site to another in order to show them display or banner ads. Google allows tracking software on its search pages, and using DoubleClick, it is able to track users across the Internet. One of its programs enables advertisers to target ads based on the search histories of Google users, along with any other information the user submits to Google such as age, demographics, region, and other Web activities (such as blogging). Google’s AdSense program enables Google to help advertisers select keywords and design ads for various market segments based on search histories, such as helping a clothing Web site create and test ads targeted at teenage females. A recent study found that 88 percent of 400,000 Web sites had at least one Google tracking bug.

Google has also been scanning 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. Profiles are developed on individual users based on the content in their e-mail. Google now displays targeted ads on YouTube and on Google mobile applications, and its DoubleClick ad network serves up targeted banner ads. 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. 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. Here, the default option is no collection of user information. The online industry has preferred self-regulation to privacy legislation for protecting consumers. The online advertising 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 Google’s DoubleClick, 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. Individual firms like Microsoft, Mozilla Foundation, Yahoo, and Google have recently adopted policies on their own in an effort to address public concern about tracking people online. Microsoft has promised to ship its new Internet Explorer 10 Web browser with the opt-out option as the default in 2012. AOL established an opt-out policy that allows users of its site to not be tracked. Yahoo follows NAI guidelines and also allows opt-out for tracking and Web beacons (Web bugs).

In general, 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. For commercial Web sites that depend on advertising to support themselves, most revenue derives from selling customer information. Of the companies that do post privacy policies 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.

**Technical Solutions**

In addition to legislation, there are a few technologies that can 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. For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another.

Because of growing public criticism of behavioral tracking and targeting of ads, and the failure of industry to self-regulate, attention has shifted to browsers. Many browsers have Do Not Track options. For users who have selected the Do Not Track browser option, their browser will send a request to Web sites requesting the user’s behavior not be tracked. Both Internet Explorer 9 and Mozilla’s Firefox browsers implement this opt-out option. However, these browsers are shipped with tracking turned on as the default. And most consumers never visit the Options Privacy tab in their browser. The online advertising industry has bitterly opposed Microsoft’s plans and warns that Web sites are not obligated to follow users’ requests to Do Not Track. There is no online advertising industry agreement on how to respond to Do Not Track requests, and currently no legislation requiring Web sites to stop tracking.

1. **PROPERTY RIGHTS: INTELLECTUAL PROPERTY**

Contemporary information systems have severely challenged existing laws 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 secrets, 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.

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.

* **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 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 United States Patent and Trademark 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. In what some call the patent trial of the century, in 2011, Apple sued Samsung for violating its patents for iPhones, iPads, and iPods. On August 24, 2012, a California jury in federal district court delivered a decisive victory to Apple and a stunning defeat to Samsung. The jury awarded Apple $1 billion in damages. The decision established criteria for determining just how close a competitor can come to an industry-leading and standard-setting product like Apple’s iPhone before it violates the design and utility patents of the leading firm. The same court ruled that Samsung could not sell its new tablet computer (Galaxy 10.1) in the United States. This was not just a loss for Samsung but a warning shot across the bow for Google, which developed the Android operating system, and all other makers of Android phones, including Google’s newly purchased Motorola Mobile Devices, makers of Motorola Mobility phones.

**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 in 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.

The Internet was designed to transmit information freely around the world, including copyrighted information. With the World Wide Web in particular, you can easily copy and distribute virtually anything to thousands and even millions of people around the world, even if they are using different types of computer systems. Information can be illicitly copied from one place and distributed through other systems and networks even though these parties do not willingly participate in the infringement.

Individuals have been illegally copying and distributing digitized MP3 music files on the Internet for a number of years. File-sharing services such as Napster, and later Grokster, Kazaa, and Morpheus, sprung up to help users locate and swap digital music files, including those protected by copyright. Illegal file sharing became so widespread that it threatened the viability of the music recording industry and, at one point, consumed 20 percent of Internet bandwidth. The recording industry won the legal battles for shutting these services down, but it has not been able to halt illegal file sharing entirely.

While illegal file sharing still goes on, it has actually declined since the opening of the iTunes Store in 2001. As legitimate online music stores expanded, and more recently as Internet radio services like Pandora expanded, illegal file sharing has declined. Technology has radically altered the prospects for intellectual property protection from theft, at least for music, videos, and television shows (less so for software). The Apple iTunes Store legitimated paying for music and entertainment, and created a closed environment where music and videos could not be easily copied and widely distributed unless played on Apple devices. Amazon’s Kindle also protects the rights of publishers and writers because its books cannot be copied to the Internet and distributed. Streaming of Internet radio, on services such as Pandora and Spotify, and Hollywood movies (at sites such as Hulu and Netflix) also inhibits piracy because the streams cannot be easily recorded on separate devices. Moreover, the large Web distributors like Apple, Google, and Amazon do not want to encourage piracy in music or videos simply because they need these properties to earn revenue.

1. **ACCOUNTABILITY, LIABILITY, AND CONTROL**

Along with privacy and property laws, new information technologies are challenging existing liability laws and social practices for holding individuals and institutions accountable. If a person is injured by a machine controlled, in part, by software, who should be held accountable and, therefore, held liable? Should a public bulletin board or an electronic service, such as America Online, permit the transmission of pornographic or offensive material (as broadcasters), or should they be held harmless against any liability for what users transmit (as is true of common carriers, such as the telephone system)? What about the Internet? If you outsource your information processing, can you hold the external vendor liable for injuries done to your customers? Some real-world examples may shed light on these questions.

1. **SYSTEM QUALITY: DATA QUALITY AND SYSTEM ERRORS**

The debate over liability and accountability for unintentional consequences of system use raises a related but independent moral dimension: What is an acceptable, technologically feasible level of system quality? At what point should system managers say, “Stop testing, we’ve done all we can to perfect this software. Ship it!” Individuals and organizations may be held responsible for avoidable and foreseeable consequences, which they have a duty to perceive and correct. And the gray area is that some system errors are foreseeable and correctable only at very great expense, an expense so great that pursuing this level of perfection is not feasible economically—no one could afford the product. For example, although software companies try to debug their products before releasing them to the marketplace, they knowingly ship buggy products because the time and cost of fixing all minor errors would prevent these products from ever being released. What if the product was not offered on the marketplace, would social welfare as a whole not advance and perhaps even decline? Carrying this further, just what is the responsibility of a producer of computer services—should it withdraw the product that can never be perfect, warn the user, or forget about the risk (let the buyer beware)? Three principal sources of poor system performance are

(1) Software bugs and errors,

(2) Hardware or facility failures caused by natural or other causes, and

(3) Poor input data quality.

1. **QUALITY OF LIFE: EQUITY, ACCESS, AND BOUNDARIES**

The negative social costs of introducing information technologies and systems are beginning to mount along with the power of the technology. Many of these negative social consequences are not violations of individual rights or property crimes. Nevertheless, these negative consequences can be extremely harmful to individuals, societies, and political institutions. Computers and information technologies potentially can destroy valuable elements of our culture and society even while they bring us benefits. If there is a balance of good and bad consequences of using information systems, who do we hold responsible for the bad consequences? Next, we briefly examine some of the negative social consequences of systems, considering individual, social, and political responses.

* **Maintaining Boundaries: Family, Work, and Leisure**

Parts of this book were produced on trains and planes, as well as on vacations and during what otherwise might have been “family” time. The danger to ubiquitous computing, telecommuting, nomad computing, mobile computing, and the “do anything anywhere” computing environment is that it is actually coming true. The traditional boundaries that separate work from family and just plain leisure have been weakened.

Although authors have traditionally worked just about anywhere (typewriters have been portable for nearly a century), the advent of information systems, coupled with the growth of knowledge-work occupations, means that more and more people are working when traditionally they would have been playing or communicating with family and friends. The work umbrella now extends far beyond the eight-hour day into commuting time, vacation time, and leisure time.

Even leisure time spent on the computer threatens these close social relationships. Extensive Internet use, even for entertainment or recreational purposes, takes people away from their family and friends. Among middle school and teenage children, it can lead to harmful anti-social behavior, such as the recent upsurge in cyberbullying.

Weakening these institutions poses clear-cut risks. Family and friends historically have provided powerful support mechanisms for individuals, and they act as balance points in a society by preserving private life, providing a place for people to collect their thoughts, allowing people to think in ways contrary to their employer, and dream.

* **Computer crime**

Computer crime is the commission of illegal acts through the use of a computer or against a computer system. Computers or computer systems can be the object of the crime ( destroying a company’s computer center or a company’s computer files), as well as the instrument of a crime (stealing computer lists by illegally gaining access to a computer system using a home computer). Simply accessing a computer system without authorization or with intent to do harm, even by accident, is now a federal crime.

* **Health Risks: RSI, CVS, and Technostress**

The most common occupational disease today is **repetitive stress injury (RSI)**. RSI occurs when muscle groups are forced through repetitive actions often with high-impact loads (such as tennis) or tens of thousands of repetitions under lowimpact loads (such as working at a computer keyboard).

The single largest source of RSI is computer keyboards. The most common kind of computer-related RSI is carpal tunnel syndrome (CTS), in which pressure on the median nerve through the wrist’s bony structure, called a carpal tunnel, produces pain. The pressure is caused by constant repetition of keystrokes: in a single shift, a word processor may perform 23,000 keystrokes. Symptoms of carpal tunnel syndrome include numbness, shooting pain, inability to grasp objects, and tingling. Millions of workers have been diagnosed with carpal tunnel syndrome.

RSI is avoidable. Designing workstations for a neutral wrist position (using a wrist rest to support the wrist), proper monitor stands, and footrests all contribute to proper posture and reduced RSI. Ergonomically correct keyboards are also an option. These measures should be supported by frequent rest breaks and rotation of employees to different jobs.

RSI is not the only occupational illness computers cause. Back and neck pain, leg stress, and foot pain also result from poor ergonomic designs of workstations. Computer vision syndrome (CVS) refers to any eyestrain condition related to display screen use in desktop computers, laptops, e-readers, smartphones, and handheld video games. CVS affects about 90 percent of people who spend three hours or more per day at a computer (Beck, 2010). Its symptoms, which are usually temporary, include headaches, blurred vision, and dry and irritated eyes.

The newest computer-related malady is **technostress**, which is stress induced by computer use. Its symptoms include aggravation, hostility toward humans, impatience, and fatigue. According to experts, humans working continuously with computers come to expect other humans and human institutions to behave like computers, providing instant responses, attentiveness, and an absence of emotion. Technostress is thought to be related to high levels of job turnover in the computer industry, high levels of early retirement from

computer-intense occupations, and elevated levels of drug and alcohol abuse. The incidence of technostress is not known but is thought to be in the millions and growing in the United States. Computer-related jobs now top the list of stressful occupations based on health statistics in several industrialized countries.

In addition to these maladies, computer technology may be harming our cognitive functions or at least changing how we think and solve problems. Although the Internet has made it much easier for people to access, create, and use information, some experts believe that it is also preventing people from focusing and thinking clearly.

**Conclusion**

The computer has become a part of our lives—personally as well as socially, culturally, and politically. It is unlikely that the issues and our choices will become easier as information technology continues to transform our world. The growth of the Internet and the information economy suggests that all the ethical and social issues we have described will be heightened further as we move into the first digital century