# SOCIAL AND ETHICAL ASPECTS OF INFORMATION TECHNOLOGY

Although many of us marvel at the conveniences information technology has provided, some social scientists and philosophers have raised concerns over the ways in which certain uses of that technology have impacted our social institutions and challenge our conventional moral notions. Social issues frequently associated with the use of information technology include, but are not limited to, the following concerns: employment and worklife, information privacy and databases, electronic surveillance and social control, computer crime and abuse, and equity of access. Before discussing individual social issues that arise from the use of information technology, it is appropriate to define what is meant by information technology and by social issues.

*Information technology* or IT has been defined differently by different authors and has, unfortunately, become a somewhat ambiguous expression. For our purposes, IT can be understood to mean those electronic technologies which are used in information processing (i.e., in the acquisition, storage, or transfer of information). Such information can be gained from three distinct sources: stand-alone (or nonnetworked) computer systems, electronic communication devices, and the convergence of computer and electronic communication technologies. An example of the first instance of IT is information acquired from computerized monitoring of employees in the workplace. An example of the second is information gained through the use of digital telephony, such as cellular telephones and caller-ID technology. And an example of the kind of information gained from the intersection of computer and electronic communications technologies is information acquired from computer networks, including the Internet.

*Social issues,* which arise because of phenomena that have an impact on either society as a whole or certain groups/social classes of individuals, can have implications that are moral as well as nonmoral. We can distinguish between those social issues that are essentially sociological or descriptive in nature and those that are also moral or ethical. To appreciate the distinction, consider the impact of information technology on the contemporary workplace. When tens of thousands of workers are displaced, or when the nature of work itself is transformed because of the introduction of a new technology, the societal impact can clearly be described and debated as a social issue. At the stage of analysis where attention is paid primarily to descriptive features such as the number and kinds of jobs affected, for example, the social issue could be viewed as essentially sociological. Does this particular social issue also have an ethical aspect? Not necessarily. However, if it is also shown that certain groups or individuals in that society's workforce (e.g., women, racial or ethnic minorities, or older workers) are unfairly or disproportionately affected

J. Webster (ed.), *Wiley Encyclopedia of Electrical and Electronics Engineering.* Copyright © 1999 John Wiley & Sons, Inc.

by that new technology—especially at the expense of other groups or individuals who stand to prosper because of it—then the issue has an ethical aspect as well. So, even though sociological and ethical aspects of a particular social issue can intersect, not every social issue will necessarily be ethical in nature or have ethical implications. Thus it is possible that an issue that is clearly a legitimate social issue will have no ethical implications whatsoever.

Many authors currently use the term *ethics* to refer to social issues that are sociological as well as moral. Forester and Morrison (1), for example, use the expression "computer ethics" to refer to a range of social issues related to information technology, many of which have nothing to do with ethics per se. In the present study, the expression "social issue" is used in a broad or generic sense to refer to issues in the use of IT that have either a sociological component, an ethical component, or both. Note, however, that no attempt is made to separate the ethical and sociological aspects of each social issue into separate categories of analysis. Instead, sociological and ethical components of individual social issues are discussed under categories such as work, privacy, surveillance, crime, equity of access, and so forth.

## EMPLOYMENT AND WORK

We begin with an examination of the impact of IT on employment and worklife, which Rosenberg (2, p. 317) claims to be the "most serious and complex problem associated with the impact of computers on society." Regardless of whether such a claim can be substantiated, IT has clearly had a profound impact on both the number of jobs and the kind of work performed in the contemporary workplace (i.e., in the transformation of work) as well as on the quality of worklife. Before examining issues affecting the quality of work, we briefly examine a cluster of issues related to the transformation of work, which include job displacement, de-skilling, automation, robotics, expert systems, remote work, and virtual organizations.

### Job Displacement, De-skilling, and Automation

A central question in the controversies underlying societal concerns related to work and IT is whether the latter creates or eliminates jobs. Arguments have been advanced to support both sides of this debate. Studies maintaining that IT use has reduced the total number of jobs often point to the number of factory and assembly jobs that have been automated. Opposing studies frequently cite the number of new jobs that have been created because of IT, maintaining that the net result has been favorable. Even though certain industries have eliminated human jobs through the use of IT in the workplace, other industries, such as computer-support companies, have created jobs for humans. Social theorists often refer to the overall effect of this shift in jobs as *job displacement.*

Whether one subscribes to the view that fewer jobs or that more jobs have resulted from the use of IT, hardly anyone would seriously challenge the claim that the kind of work performed has changed significantly as a result of IT. Optimists and pessimists offer different accounts on whether the transformation of work has on the whole been beneficial or nonbeneficial to employees. Perhaps a specific case will serve to illustrate key points. Wessells (3) describes an interesting case involving a small, family-owned publishing company that specialized in making marketing brochures for local businesses. Because of the need for a skilled typesetter, a paste-up artist, and an expensive array of machines, the cost to customers was over $20 per page. By investing $10,000 into a PC with desktop publishing software, the company could do all its publishing on the computer. Within six months the company had recovered its initial investment and was able to double its production without expanding its staff. The cost per page to customers was reduced from $20 to $5. Moreover, the workers enjoyed using the computer system because it eliminated much of the "drudge work," freeing them to concentrate on the more creative aspects of their jobs. Can we conclude that, overall, workers' skills have been enhanced or upgraded in the transformation process?

Unfortunately, the story of the small, family-owned publishing company is not representative of certain industries affected by computers and IT. Some jobs have been affected by a process called Computer Numerical Control (CNC), where computers are programmed to control machines such as lathes, mills, and drill presses. With CNC, computers, not the workers, guide the speed at which machines operate, the depth to which they cut, and so on; hence control over complex machines is transferred from skilled workers to computers. The transfer of skill has severely affected many highly skilled machinists who traditionally were responsible for the design, production, and use of machine tools. Because computers now perform several of those machine-related tasks, many workers are currently employed in jobs that require fewer and less-sophisticated skills—a phenomenon known as *de-skilling.* So while many workers have applauded the use of computers to assist them in their jobs—such as the use of computer-aided design (CAD) systems to enhance their work and (as in the preceding case of the desktop publishing company) to make certain job-related tasks more meaningful—others remain justifiably concerned over the de-skilling effects that have resulted from certain uses of IT in the workplace.

Issues related to de-skilling have become associated with, and sometimes linked to, those surrounding *automation.* Social scientists note that prior to the Industrial Revolution workers generally felt connected to their labor and often had a strong sense of pride and craftsmanship. This relationship between worker and work began to change, we are told, during the Industrial Revolution when many jobs were transformed into smaller, discrete tasks that could be automated by machines. It should be noted that heated social reaction to machine automation is by no means peculiar to recent developments in IT. We need only look to various accounts of the notorious Luddites, an eighteenth century group of disenchanted workers in England who smashed machines used to make textiles because the new automated technology had either replaced or threatened to replace many workers. In more recent years, we have seen attempts by what some label "Neo-Luddites" to stall developments in microprocessor-based technology, for fear that this technology would lead to further automation of jobs. Although the practice of automating jobs through the use of machines may have been introduced in the Industrial Revolution, IT has played a significant role in perpetuating the automation process and the controversies associated with it.

### Robotics and Expert Systems

Closely associated with social issues in industrial automation are concerns arising from recent developments in *robotics.* A robot, which can be described as the integration of computer and electromechanical parts, can be understood to mean a mobile robotic limb or arm as well as a full-fledged robotic system. Composed of sensory, tactile, and motor abilities that enable them to manipulate objects, robots can be programmed to perform a number of different tasks such as assembling parts, spray painting, and welding. Robots can also be programmed to perform tasks considered hazardous to many humans, such as removing nuclear waste and making repairs in outer space or under water. Until recently, many robots were fairly unsophisticated and had very limited sensory capacity. First-generation robots were often dedicated to performing specific tasks such as those on automobile assembly lines and factory floors. Many of the new generation robots, however, are now able to perform a broader range of tasks and are capable of recognizing a variety of objects by both sight and touch. Even though robots offer increased productivity and lower labor costs, they also raise several issues related to automation and job displacement.

Another IT-related technology that has begun to have an impact on certain kinds of jobs, which are mostly professional in nature, is *expert systems.* An expert system (ES) is a computer program or a computer system that is "expert" at performing one particular task. Because it can be simply a computer program, an ES need not, as in the case of a robot, be a physical or mechanical system. Growing out of research and development in Artificial Intelligence or AI, ESs are sometimes described as problem-solving systems that use an inference engine to capture the decision-making strategies of "experts," usually professionals. In effect, ES programs execute instructions that correspond to a set of rules an expert would use in performing a professional task. The rules are extracted from human experts in a given field through a series of questions asked by a knowledge engineer, who designs a program based on responses to those questions.

Initially expert systems were designed to do work in the professional fields of chemical engineering and geology, primarily because that work, which required the expertise of highly educated persons, was often considered too hazardous for humans. Shortly thereafter, nonhazardous professions such as medicine were affected by expert systems. An early expert system called MYCIN (The MYCIN Experiments of the Stanford Heuristic Programming Project, Stanford University), developed in the 1970s, assisted physicians in recommending appropriate antibiotics to treat bacterial infections. Recently, expert systems have been developed for use in professional fields such as law, education, and finance.

A number of social issues have arisen with the increased use of ES technology. Forester and Morrison (1) raise an interesting ethical question with respect to developing an "expert administrator." If we design such a system, should we program it to *lie* in certain cases? Is the practice of lying or at least being deceptive with respect to certain information a requirement that is essential for being an expert human administrator? Other controversies surrounding ES have to do with critical decisions, including life and death decisions. For example, should "expert doctors" be allowed to make decisions that could directly result in the death of, or serious damage to, a patient? If so, *who* is ultimately responsible for the ES's decision? Is the hospital who owns the particular ES responsible? Should the knowledge engineer who designed the ES be held responsible? Or is the ES itself responsible? If the answer to this last question is yes, what implications would this have for our conventional notions of moral responsibility?

### Remote Work and Virtual Organizations

Recent communications technologies associated with modems, e-mail, facsimile (FAX) machines, and so forth, have had a significant impact on work performed in offices. In addition to automating office work, IT has also made it possible for many employees to work out of their homes (i.e., in *virtual organizations* such as a "virtual office," a "virtual team," or a "virtual corporation"). Mowshowitz (4, p. 30) defines a virtual corporation as a "virtually organized company dynamically . . . linked to a variety of seemingly disparate phenomena, including . . . virtual teams and virtual offices." Whereas virtual teams allow managers to "assemble groups of employees to meet transient, unanticipated needs," virtual offices allow employees to "operate in dynamically changing work environments." Virtual teams, offices, and corporations raise a number of social concerns. One area of concern has to do with the kind of commitment employees will be able to expect from their employers. For example, Spinello (5) points out that virtual organizations may feel less obligated to provide employees benefits or other workplace amenities. Another area of concern has to do with certain social relationships in the workplace. When work is performed in an office or at a physical site, workers are required to interact with each other and with managers. As a result of interactions between employees and between employers and employees, certain dynamics and interpersonal relationships emerge. Virtual organizations now pose a threat to many of the dynamics and relationships that have defined the traditional workplace.

Closely related to issues surrounding virtual organizations are concerns associated with *remote work.* While once considered a perk for a few fortunate workers who happened to be employed in certain industries (often in high-tech companies), remote work is now done by millions of employees. It is worth noting that some social theorists, when discussing remote work, further distinguish between "telework" and "telecommuting." Rosenberg (2, pp. 342–343), for example, defines *telework* as "organizational work performed outside the organizational confines," and *telecommuting* as the "use of computer and communications technologies to transport work to the worker as a substitute for physical transportation of the worker to the workplace." Many authors, however, use the two terms interchangeably. We will discuss social issues surrounding both telecommuting and telework under the general heading "remote work."

Although a relatively recent phenomenon, the practice of remote work has already raised a number of social and ethical questions. For example, do all workers benefit equally from remote work? Are well-educated, white-collar employees affected in the same way as those less-educated and less-skilled employees who also perform remote work? It is one thing to be a white-collar professional with an option to work at home at one's discretion and convenience. It is something altogether different, however, to be a clerical or "pink collar" worker to be required to work remotely out of one's home. Even though some professional men and women may prefer to work at home, possibly because of child-care considerations or because they wish to avoid a long and tedious daily commute, certain employees—especially those in lower-skilled and clerical jobs—are required by their employers to work at home. Such workers are potentially deprived of career advancement and promotions, at least in part because their interpersonal skills as well as certain aspects of their job performance cannot be observed and measured as directly as those who carry out their job-related tasks in the traditional office or physical workplace setting.

In addition to questions of equity and access to job advancement for those workers in lower-skilled and lower-paying jobs, remote work has also recently begun to pose a threat to certain professional classes of workers. Some corporations and business in developed countries have elected to farm out professional work requiring programming skills to employees in third-world countries who are willing to do the work for a much lower wage? In recent years, for example, some American-based companies have exported computer programming jobs to Asian countries, where skilled programmers are willing to work for a fraction of the wages received by American programmers. Without IT, of course, such a practice would not be possible.

### The Quality of Worklife

Thus far we have focused on the transformation of work in the information age and on the quantity of jobs that are alleged to have resulted from the use of IT. Even though there is general agreement that IT has contributed both to productivity in the workplace and profitability for businesses, many social theorists have raised concerns with respect to the impact of IT on the *quality* of worklife. Some quality issues have to do with health and safety concerns, whereas others are related to employee stress such as that brought about by computerized monitoring. We begin with a brief discussion of certain health and safety issues.

Some *health and safety issues* attributed to IT use in the workplace stem from effects of computer screens [i.e., screens on computer monitors or Video Display Terminals (VDTs)]. Reported health problems associated with computer screens include eye strain, fatigue, blurring, and double vision. These and similar problems frequently associated with prolonged use of a computer screen have been referred to as Video Operator's Distress Syndrome (VODS). Other health-related problems associated with the use of electronic keyboards and hand-held pointing/tracking devices include arm, hand, and finger trauma. Several cases of carpal tunnel syndrome and tendonitis as well as other musculo-skeletal conditions, now commonly referred to Repetitive Strain Injury (RSI), have been reported in recent years. Fearful of litigation, many computer manufacturers as well as businesses that require extensive computer use by their employees have paid serious attention to ergonomic considerations. Companies such as L. L. Bean, for example, have installed ergonomically adjustable workstations to accommodate individual employee needs. For example, each worker's ergonomic measurements (i.e., appropriate height-level for keyboards and desktop work surfaces, proper eye-to-monitor distance, and appropriate measurements related to an employee's neck, back, and feet requirements) are recorded. When an employee begins work on his or her shift, the workstation is automatically adjusted according to that individual's prerecorded ergonomic measurements. Other companies, both within and outside the computer industry, have adopted ergonomic practices and policies similar to those used at the L. L. Bean company.

Another quality-of-work issue associated with IT is employee stress. Because of IT, worker stress has been exacerbated by practices such as *computerized monitoring* of employees. Many workers' activities are now monitored closely by an "invisible supervisor" (viz., the computer). For example, information about employees with respect to the number of keystrokes entered per minute, the number of minutes spent on a telephone call completing a transaction (such as selling a product or booking a reservation), the number and length of breaks taken, etc., is frequently recorded on computers. As a result, many employees have complained that the practice of monitoring their activities has resulted in increased workplace stress. Perhaps somewhat ironically, it is the "information workers" (i.e., those whose work is concerned solely with the use of IT to process information) who are the most vulnerable to computerized monitoring by their employers.

Some employers have defended the practice of computer monitoring on the grounds that it is an essential tool for improving efficiency and worker productivity. Many of these employers also claim that monitoring aids managers in motivating employees as well as in helping businesses to reduce industrial espionage and employee theft. Opponents of monitoring, however, see the matter quite differently. Many employees and employee unions see computer monitoring as a "Big-Brother" tactic or as an "electronic whip" used unfairly by management, which often results in an "electronic sweatshop." Some opponents cite an attitude of distrust on the part of managers as a key motive behind decisions to use monitoring. Many also claim that because monitoring invades individual privacy, it disregards human rights. Some critics also charge that monitoring, which may accurately measure the quantity of work produced, fails to measure the overall quality of the work completed. Others argue that computer monitoring is ultimately counterproductive because employee morale generally declines, and with it so does overall workplace productivity.

Although not endorsing the practice of computer monitoring, Marx and Sherizen (6) have proposed a "code of ethics" that they believe would help to place some measure of control on employee monitoring. Under this code, employees would be required to receive advanced notice that their work will be monitored by a computer. Employees also would be given an opportunity to see the records of their monitored activities and would be able to verify the accuracy of those records before such information could be used to evaluate them. This code would also require that a statute of limitations be established for how long information on an employee that was gathered from computer monitoring could be used and kept on record in an employee's file.

Computer monitoring of employees clearly raises a number of issues related to privacy, especially workplace privacy. Other employee privacy issues include the use of e-mail in the workplace. For example, do employees have a right to private e-mail communications on an employer's computer system? Even though some companies, such as Merill Lynch, have explicit policies regarding the use of e-mail and other computer-system resources, many do not. As a result, it is not always clear what kinds of personal privacy protections employees can expect in the workplace. Many concerns associated with IT and personal privacy are examined in the two sections that follow.

## INFORMATION PRIVACY AND DATABASES

Of all the social issues associated with IT, perhaps none has caused as much public concern as the threat or perceived threat of privacy loss. In a Harris Poll conducted in 1994, 84% of Americans surveyed claimed to be either "very concerned" or "somewhat concerned" about threats to their personal privacy. In a similar poll taken in 1970, only 34% had expressed the same concerns (2, p. 274). Most Americans believe they have a legal right to privacy. Some assume that such a right is guaranteed by either the Constitution or the Bill of Rights. Many are often astonished to find that there is no explicit mention of a right to privacy in either document. Some legal scholars have argued that such a right is implied in the First and Fourth Amendments. In recent years, the Congress has passed a number of privacy-related statutes, including the Privacy Act of 1974. This Act established a Privacy Protection Commission, which issued a report in 1977 that included several recommendations for developing "fair information practices." To date, very few of the recommendations included in the Commission's Report have been enacted into law.

### How Does Information Technology Threaten Privacy?

IT has facilitated the collection of information about individuals in ways that would not have been possible before the advent of the computer. Consider, for example, the *amount* of personal information that can now be gathered and stored in computer databases. Also consider the *speed* at which such information can be exchanged and transferred between databases. Furthermore, consider the *duration* of the information (i.e., the length of time in which the stored information can be kept). Contrast these factors with record-keeping practices employed before the computer era, where information had to be manually recorded and stored in folders, which in turn had to be stored in (physical) file cabinets. There were practical limits as to how much data could be collected and as to how long it could be stored. Eventually, older information needed to be eliminated to make room for newer information. Because information is now stored electronically, it requires very little physical space. For example, information that might previously have required a physical warehouse for storage can now reside on several hundred CDs that fit on a few shelves. And because information can now be stored indefinitely, an electronic record of an individual's elementary school grades or teenage traffic violations can follow that individual for life.

In addition to concerns about the amount of information that can be collected, the speed at which it can be transferred, and the indefinite period for which it can be retained, IT also raises questions related to the *kind* of information collected. For example, every time we engage in an electronic transaction, such as making a purchase with a credit card or withdrawing money from an ATM (Automatic Teller Machine), *transactional information* about us is collected and stored in several computer databases. Such information can be used to construct an "electronic dossier" on each of us—one that contains detailed personal information about our transactions, including a history of our purchases, travels, habits, preferences, and so forth.

### What Is Personal Privacy?

An appropriate starting point in examining issues concerning individual privacy is to ask the question "What exactly is *personal privacy?*" Even though many definitions and theories of personal privacy have been put forth, three have received serious attention in recent years. One popular theory, originating with Warren and Brandeis (7), suggests that privacy consists in "being free from unwarranted intrusion" or "being let alone." We can call this view the "nonintrusion theory" of privacy. Another theory, which can be found in the works of Gavison (8) and Moor (9), views privacy as the "limitation of access to information about oneself." Let us call this account of personal privacy the "limitation theory." A third and very popular conception of privacy, advanced by Freid (10) and Rachels (11), is one that defines privacy as "control over personal information." On this view, one enjoys privacy to the extent that one has control over information about oneself. We can call this view the "control theory" of privacy.

Against nonintrusion theorists, proponents of the control theory argue that privacy consists not simply in being let alone or in being free from intrusion—both of which are essentially aspects of liberty rather than privacy—but in being able to have some say or control over information about us. And against the limitation theorists, control theorists maintain that privacy is not simply the limitation or absence of information about us—a view that confuses privacy with secrecy—it is having *control* over who has access to that information. Essentially, privacy consists in having control over whether we will withhold or divulge certain information about ourselves. Having control over information about ourselves means having the ability to authorize as well as to refuse someone access to that information. To understand the importance of being able to have control over the amount and kind of information about ourselves we are willing to grant or deny to others is, according to control theorists, to understand the value of personal privacy.

Johnson (12) argues that privacy is highly valued because it is essential for autonomy. To be autonomous, one must have some degree of choice over the relationships one has with others. Because information mediates relationships, to take away a person's ability to control information about oneself is to take away a considerable degree of that individual's autonomy. So when individuals cannot control who has what information about them, they lose considerable autonomy with respect to control over their relationships. Along similar lines, Rachels (11) argues that privacy is important because it makes possible a diversity of relationships. In having control over information about ourselves, we can decide how much or how little of that information to reveal to someone. Thus we can determine how close or how distant our relationship with that person will be. Consider how much information about ourselves we share with our spouses or with close friends versus the amount of information we share with casual acquaintances. Because it would now seem that most of us have lost considerable control over information about ourselves, and thus have lost a great deal of individual privacy, we can ask to what extent certain uses of IT have contributed to the erosion of personal privacy.

It can be argued that certain organizations have a legitimate need for information about individuals to make intelligent decisions concerning those individuals. And it can also be argued that individuals should have a right to keep some personal information private. Perhaps then the crux of the privacy-and-computers question is, as Johnson (12) suggests, finding an "appropriate balance" between an organization's need for personal information to make intelligent business decisions and an individual's right to keep certain information private. A crucial question here is what kind of control over personal information an individual can expect after that individual has given the information to an organization. Can, for example, an individual expect that personal information provided to an organization for legitimate use in a certain context will remain within that organization? We begin with a look at how some professional information-gathering organizations—such as Equifax, Trans Union, and TRW (credit reporting bureaus) as well as the MIB (Medical Information Bureau)—threaten personal privacy because of the practices used in exchanging and merging information about individuals.

### Merging Computerized Records

*Computer merging,* the merging of computerized records, happens whenever two or more disparate pieces of information contained in separate databases are merged. Consider a case in which you voluntarily give information about yourself to three different organizations. You give information about your income and credit history to a lending institution in order to secure a loan. You next give information about your age and medical history to an insurance company to purchase life insurance. You then give information about your position on certain social issues to a political organization you wish to join. Each of these organizations can be said to have a legitimate need for information to make certain decisions about you. For example, insurance companies have a legitimate need to know about your age and medical history before agreeing to sell you life insurance. Lending institutions have a legitimate need to know information about your income and credit history before agreeing to lend you money to purchase a house or a car. And insofar as you voluntarily give these organizations the information requested, no breach of your privacy has occurred. However, if information about you contained in an insurance company's database is exchanged and merged with information about you in a lending institution's database or a political organization's database, without your knowledge and consent, then you have lost control over certain information about yourself.

Even though you voluntarily gave certain information about yourself to three different organizations, and even though you authorized each organization to have the specific information you voluntary granted, it does not follow that you thereby authorized any one organization to have some combination of that information. That is, granting information $X$ to one organization, information $Y$ to a second organization, and information $Z$ to a third organization does not entail that you authorized any one of those organizations to have information $X + Y + Z$. Mason (13) has described such a technique of information exchange as the "threat of exposure by minute description." When organizations merge information about you in a way that you did not specifically authorize, you lose control over the way in which certain information about you is exchanged. Yet, this is precisely what happens to personal information gathered in the private sector. So the use of computer databases by private corporations to merge computerized records containing information about individuals raises serious concerns for personal privacy.

### Matching Computerized Records

A variation of merging computerized records is used in a technique that has come to be referred to as *computer matching.* Dunlop and Kling (14) describe computer matching as the use of databases, whose purposes are typically unrelated, to cross-check information in order to identify potential law violators. Matching is frequently used by law enforcement agencies to identify and track down certain individuals. Consider a case in which you complete a series of forms for various federal and state government agencies. In filling out a form for a particular agency, such as the Internal Revenue Service (IRS), your state government's motor vehicle registration department, or your local government's property tax assessment department, you supply the specific information requested. In addition, you are also asked to include general information on each form, such as your social security number and driver's license number, which can be used as "identifiers" in matching records about you that reside in multiple databases. The information is then electronically stored in the respective databases used by the various government agencies and routine checks (matches) can be made against information (records) about you contained in those databases. For example, your property tax records can be matched against your federal tax records to see whether you own an expensive house, but declared only a small income. Records in an IRS database of divorced or single fathers can be matched against a database containing records of mothers receiving welfare payments to generate a list of potential "deadbeat dads."

In filling out the various governmental forms, you voluntarily gave some information to each government agency. It is by no means clear, however, that you authorized information given to any one agency to be exchanged in the way it has with other agencies. In the process of having information about you in one database matched against information about you residing in other databases, you effectively lost control of how certain information about you has been exchanged. So it would seem that the computerized matching of information, which you had not specifically authorized for use by certain government agencies, raises serious threats for personal privacy.

While Kusserow (15) has argued that computer matching is needed to "root out government waste and fraud," Shattuck (16) claims that computer matching violates "individual freedoms," including one's right to privacy. At first it might seem that a practice such as matching computer records is socially desirable because it would enable us to track down "deadbeat parents," welfare cheats, and the like. Although few would object to the ends that could be achieved, we must also consider the means used. Tavani (17) has argued that computer matching, which like computer merging deprives individuals of control over personal information, is incompatible with individual privacy.

It is worth noting that computer matches are often conducted even when there is no suspicion of an individual or group of individuals violating some law. For example, computer records of entire categories of individuals, such as government employees, have been matched against databases containing records of welfare recipients, on the chance that a "hit" will identify one or more "welfare cheats." The practice of computer matching has also raised questions related to governmental attempts at social control, which are examined in the following section.

## ELECTRONIC COMMUNICATIONS, SURVEILLANCE, AND SOCIAL CONTROL

Thus far we have examined privacy concerns related to computerized records stored in and exchanged between databases. Johnson and Nissenbaum (18) suggest that privacy issues related to IT can be divided into two categories: "information privacy" and "communications privacy." Whereas the former focuses on issues related to information residing in computer databases, such as those considered in the previous section, the latter centers on more recent privacy concerns related to communications technologies such as the Internet, digital telephony, and data encryption. We begin with an examination of some privacy concerns arising from certain uses of two Internet-related technologies: search engines and bulletin board systems.

### Internet Search Engines and Bulletin Board Systems

Electronic *bulletin board systems* (BBS) allow Internet users to carry on discussions, upload and download files, and make announcements without having to be connected to the service at the same time. Users "post" information on an electronic BBS for other users of that service to access. For the most part, BBSs have been considered quite useful and relatively uncontroversial. However, personal information about individuals—which in some cases has been defamatory and, in other cases, false or inaccurate—can also be posted to these systems. Furthermore, some Internet providers have allowed "anonymous postings" in which the name (or real name) of the individual posting the controversial message is not available to the users of that BBS. An important point to consider is that individuals who have information about them posted to BBSs do not typically have control over the way personal information about them is being disseminated. Controversies resulting in claims on the part of certain individuals that their privacy (as well as their civil liberties) had been violated have caused some Internet providers either to shut down their BBSs altogether or to censor them. Currently, there is no uniform policy among Internet providers with respect to privacy and BBSs. It is also worth noting that some privacy issues associated with BBSs also border on issues related to free speech and censorship in cyberspace.

Another set of privacy issues has recently emerged from certain uses of Internet *search engines,* which are computer programs that assist Internet users in locating and retrieving information on a range of topics. Users request information by entering one or more keywords in a search engine's "entry box." If there is a match between the keyword(s) entered and information in one or more files in the search engine's database, a "hit" will result, informing the user of the identities of the file(s) on the requested topic. Included in the list of potential topics on which search-engine users can inquire is information about individual persons. By entering the name of an individual in the program's entry box, search-engine users can potentially retrieve information about that individual. However, because an individual may be unaware that his or her name is among those included in a search-engine database, or may perhaps be altogether unfamiliar with search-engine programs and their ability to retrieve information about persons, questions concerning the implications of search engines for personal privacy have been raised.

It could be argued that information currently available on the Internet, including information about individual persons, is, by virtue of its residing on the Internet, public information. We can, of course, question whether all such information available on the Internet *should* be viewed as public information. One response might be that if information is already publicly available in one medium (e.g., in hardcopy format) then converting that information to an electronic format and including it on the Internet would not seem unreasonable or inappropriate.

The following case may cause us to reconsider whether certain information about individual persons, which is currently included on the Internet, and which is accessible to all Internet users, should be viewed as public information. Consider a case in which an individual contributes to a cause sponsored by a homosexual organization. That individual's contribution is later acknowledged in the organization's newsletter (a hardcopy publication that has a limited distribution). The organization's publications, including its newsletter, are then converted to electronic format and included on the organization's Internet Web site. The Web site is "discovered" by a search-engine program and an entry about that site's URL (Universal Resource Locator) is recorded in the search engine's database. Suppose that you enter this individual's name in the entry box of a search-engine program and a "hit" results, identifying that person (and suggesting that person's association with the homosexual organization). You then learn that this person contributed to a certain homosexual organization. Has that individual's privacy been invaded? It would seem that one can reasonably ask such a question. Because individuals may not always have knowledge of or control over whether personal information about them included in databases accessible to search-engine programs, Tavani (19) has suggested that questions regarding the implications of search-engine technology for personal privacy can be raised.

Another privacy concern related to search engines is one that involves Internet "cookies," which enable Internet search-engine facilities to store and retrieve information about users. Essentially, certain information submitted by the user to a search-engine facility can be stored on the user's machine and then resubmitted to that search engine the next time the user accesses it. This "cookie" information is used by the search-engine facility to customize or personalize the order of "hits" that will be visible to the user on his or her next visit to the search-engine facility. That is, the order and rank in which the "hits" appear to the user are predetermined according to a search engine's estimate of that user's preferences. Defenders of "cookies" maintain they are doing repeat users of a search-engine service a favor by customizing their preferences. Privacy advocates, on the other hand, maintain that search-engine facilities cross the privacy line by downloading information on to a user's PC (without informing the user) and then using that information in predetermining the sequential order "hits" a user will see. As in the case of electronic BBSs, there are currently no universal privacy policies for using Internet search engines.

### Electronic Surveillance and Social Control

Not only do computer networks pose a threat to personal privacy because of the way information about us is communicated in public forums such as those on the Internet, they also make it possible for governments to keep track of the activities of private citizens. To illustrate this point, we can consider the island nation of Singapore, which has made a commitment to become a full-fledged information society by the end of the 1990s. To this end, the government of Singapore has engaged in a comprehensive program of converting all the nation's physical records—public and private—to electronic format. More significantly, it has created a centralized computer network, called "The People Data Hub," which links all the nation's databases, including those containing personal information about each citizen. For example, government officials know the precise time a citizen purchases a ticket for use on Singapore's transportation system. They also know what time an individual boards and leaves a commuter transportation station. In fact, the government of Singapore has, as Palfreman and Swade (20) note, considerable personal knowledge about each of its citizens—knowledge that many in the West would find inappropriate information for governments to have about individual citizens.

Even though individual privacy may be highly valued in many Western industrialized societies, it would seem that privacy is not universally valued. Singapore's political leaders recognize that many of their practices would raise serious privacy concerns in the West, but they argue that its citizens accept being governed in a certain way because it is the only way they will be able to move directly to an information society, with its many benefits including the ability to compete successfully in a global market. In some ways, Singapore can be seen as a test case for what it will be like for citizens to live in a full-fledged, government-controlled, information society. Perhaps Singapore's citizens will decide that government control is an acceptable price to pay for security, low crime, and clean transportation systems. Regardless of the outcome, Singapore's commitment to IT and the implications of that commitment for social control of its citizens will be an interesting experiment to watch. In the United States, recent concerns over what some fear as the federal government's attempt at social control through electronic surveillance are at the heart of the debate over encryption-related technology issues surrounding the Clipper Chip.

### Cryptography, Data Encryption, and the Clipper Chip

Some Americans fear that practices such as those used by the government of Singapore to monitor its citizens' activities will eventually spread to the United States, resulting in a governmental system of social control similar to the one portrayed in George Orwell's classic novel *1984.* Some see recent proposals by the US government involving *data encryption* as a first step in that direction. Data encryption or *cryptography,* the art of encrypting and decrypting messages, is hardly new. The practice is commonly believed to date back to the Roman era, where Julius Caesar encrypted messages sent to his generals. Essentially, cryptography involves taking ordinary communication (or "plain text") and encrypting that information into "ciphertext." The party receiving that communication then uses a "key" to decrypt the ciphertext back into plain text.

Using IT, encryption can be implemented in either the software or the hardware. So long as both parties have the appropriate "key," they can decode a message back into its original form or plain text. One challenge with respect to ensuring the integrity of encrypted communications has been to make sure that the key, which must remain private, can be successfully communicated. Thus, an encrypted communication will be only as secure and private as its key.

The cryptographic technique described thus far is referred to as private-key encryption or "weak encryption," where both parties use the same encryption algorithm and the same private key. A recent technology, called public cryptography or "strong encryption," uses two keys: one public and the other private. If $A$ wishes to communicate with $B$, $A$ uses $B$'s public key to encode the message. That message can then only be decoded with $B$'s private key (which is secret). Similarly when $B$ responds to $A$, $B$ uses $A$'s public key to encrypt the message. The message can only be decrypted using $A$'s private key. Here the strength is not so much in the encryption algorithm as it is in the system of keys used. Although information about an individual's public key is accessible to others, that individual's ability to communicate encrypted information is not compromised.

Strong encryption has raised concerns for certain US government agencies, especially those concerned with law enforcement. Such agencies want to be assured they can continue to perform legal wiretap operations on electronic communications devices that employ strong encryption. Citing issues such as terrorism, national security, and organized crime, the Clinton Administration in February 1994 proposed that a certain device, which has come to be known as the *Clipper Chip,* be installed in all electronic communications devices. The proposal also called for the keys to this encryption system to be held in escrow by the federal government. So when a government agency needed to wiretap a phone, it would first get the necessary court order and then request the keys from the agency in which they were being held in escrow.

Critics of Clipper, which include groups and individuals as diverse as the ACLU and Rush Limbaugh, have raised several concerns. For example, some have questioned how secure the chip really is. Because no one outside of the government has access to Clipper, independent tests regarding the security and reliability of this technology—a computer chip whose encryption algorithm, known as "Skipjack," is embedded in the hardware—cannot be independently confirmed. Also, some have questioned whether we can/should actually trust the federal government. Levy (21) has noted that with Clipper (or with any government-controlled encryption system like it), we could be sure that our communications will be completely private—except, of course, from the government itself! Some critics have wondered whether appeals to national security could become a convenient excuse for particular government administrations to engage in questionable political practices. Other critics have raised questions about the commercial implications of the Clipper Chip. For example, certain nations that trade with the United States have made it clear that they would not purchase electronic communications devices from the United States, if such devices contained the Clipper Chip. Because of the sustained efforts on the part of the anti-Clipper coalitions, the Clinton administration withdrew its support for Clipper. Although the controversy around Clipper itself has subsided, many fear that the government will in the future try to impose some kind of encryption standard similar to the Clipper Chip.

Just as some have argued that computer matching is necessary to track down criminals and undesirables, proponents of Clipper argue that the use of such technology for wiretapping operations is essential for keeping tabs on organized crime members, international drug dealers, terrorists, and so on. Defenders of Clipper also argue that individuals' civil rights will be no more threatened or compromised than before because government agencies are currently permitted to eavesdrop on citizens or organizations only if they have a legal warrant to do so. Controversies related to Clipper, especially with respect to the ease at which some electronic communications can be compromised, have also surfaced in the privacy debate surrounding digital telephony.

### Digital Telephony

One recent set of communications-privacy concerns related to *digital telephony* has emerged from a technology sometimes referred to as Caller Number Identification, but more commonly known as *caller-ID.* Some find this technology appealing because the party on the receiving end of the communication sees a display of the phone number from which the incoming call is made. That information can then be used in determining whether or not to answer a particular phone call. A criticism frequently leveled against this technology is that information about a caller's phone number, which may be an unlisted number, becomes publicly available to anyone who has caller-ID technology. Certain businesses and organizations favor this technology because it gives telephone-related information about consumers that can be used for prospective future transactions. Many privacy advocates, however, have opposed caller-ID technology on grounds such that certain individuals who might otherwise be disposed to call an anonymous "hotline" number if their anonymity could be ensured, would not do so because of caller-ID technology.

Other privacy concerns related to digital telephony have arisen because of an electronic communications device known as the *cellular phone.* Cases have been reported in which telephone conversations carried out on cellular phones have been intercepted by private citizens as well as by corporate and industrial spies who are eager to find out information about their competitors. Concerns related to privacy and telephony have caused considerable debate and have resulted in recent legislation. Because cellular phones transmit their serial number and billing information at the beginning of each call, such information is vulnerable to interception. Baase (22) points out that a popular criminal technique for avoiding charges is "cloning" (i.e., reprogramming one's cellular phone to transmit another customer's name). Certain cases involving the use of electronic communications devices for fraud and abuse are discussed in greater detail in the following section on computer crime.

## COMPUTER CRIME AND ABUSE

Another IT-related social issue that has received considerable public attention is *computer crime.* We often hear and read about stories involving disgruntled employees who alter files in computer databases or who sabotage computer systems in the act of seeking revenge against employers. Other highly publicized news stories describe computer hackers penetrating computer systems—thought to be highly secure—either as a prank or as a malicious attempt to subvert data or disrupt its flow. Many analysts believe that the number of reported computer crimes to be merely a fraction of those actually committed. Not all crimes are reported, it is alleged, because the revelation of such crimes on the part of those businesses impacted would amount to a tacit admission that their security was inadequate. Such an admission could, it is further argued, have negative repercussions. If, for example, a customer discovers that the bank where he or she deposits and saves money was broken into by hackers from outside the institution or had electronic funds altered by employees on the inside, he or she may wish to transfer funds to a more secure institution.

Stories of computer fraud and abuse have often made the headlines of major newspapers and have sometimes been the focus of special reports on television programs. Yet, the criteria for what constitutes a computer crime has not always been clear; perhaps, then, such a concept would benefit from further elucidation. We can begin by asking whether all crimes involving computers are qualitatively different from those kinds of crimes in which no computer is present. We must also consider whether the use of a separate category of computer crime can be defended against those who argue that there is nothing special about crimes that involve a computer? In considering these questions, we will need to examine concepts such as hacking, cracking, computer viruses, computer sabotage, software piracy, and intellectual property. We begin with a general inquiry into a definition of computer crime.

### What Is Computer Crime?

We can first ask whether every crime involving a computer is, by definition, a *computer crime.* People steal computers, and they also steal automobiles and televisions (both of which, by the way, may also happen to contain computer components). Yet, even though there are significant numbers of automobile thefts and television thefts, we don't have categories of "automobile crime" and "television crime." Thefts of items such as these are generally considered ordinary instances of crime. Can we infer, then, that there is no need for a separate or unique label such as computer crime? It should be noted that certain crimes can be committed only through the use of a computer! Perhaps a computer crime should, as Forester and Morrison (1, p. 29) suggest, be defined as a "criminal act that has been committed using a computer as the principal tool." On that definition, the theft of an automobile or a television—regardless of whether either item also happens to contain a computer part (e.g., a microprocessor)—would not count as an instance of computer crime.

But what about the theft of personal computers or of computer peripherals from a computer lab? Would such thefts be considered instances of computer crime? Because in these cases a computer is not the "principal tool" for carrying out the criminal acts, the crimes would not seem to count as computer crimes. So while breaking into a computer lab and stealing computers and computer accessories is a crime that coincidentally involves computers, it would not, at least on the preceding definition, meet the criteria of a computer crime. What then would constitute a typical case of computer crime? Perhaps a paradigm case, which also illustrates the central point in the preceding definition of a computer crime, is a "computer break-in" [i.e., the use of an IT device (such as a personal computer) to penetrate a computer system]. Here a computing device *is* the principal tool used in carrying out the criminal activity.

In recent years, discussions about computer crimes have frequently focused on issues related to electronic "break-ins" and system security. Even though some computer break-ins have allegedly been performed for "fun," others have been conducted for gain or profit. Some break-ins have seemed relatively benign or innocuous; others, unfortunately, have been quite mischievous to the point of being potentially disastrous for society as a whole. To understand some of the reasons given for, as well some of the arguments advanced in defense of, breaking into computer systems, it is worth looking briefly at what might be described as the hacker culture.

### Hacking and Cracking

Often, computer criminals are referred to as *hackers.* Consequently the term *hacker* has taken on a pejorative connotation. In its neutral sense, hacking can be understood as a form of tinkering. Originally, computer hackers were viewed as computer enthusiasts who were often fascinated with computers and IT—some hackers were known for spending considerable time experimenting with computers, whereas others were viewed as programmers whose (programming) code would be described as less than elegant. To preserve the original sense of computer hacker, some now distinguish between hackers and *crackers.* The latter term is used to describe a type of online behavior that is illegal and improper, whereas the former refers to what some view as a form of "innocent experimentation." The art of hacking has become a favorite past time of certain individuals who are challenged by the possibility of gaining access to computer systems. For hackers, the challenge often ends at the point of being able to gain access. Crackers, on the hand, go one step farther. After they penetrate an unauthorized system, they engage in activities that are more overtly illegal.

Several ethical questions related to hacking have emerged. For example, is computer hacking inherently unethical? Should every case of hacking be treated as criminal? Can some forms of hacking be defended? Certain First-Amendment-rights advocates see hacking as an expression of individual freedoms. Some advocates for "hacker's rights" argue that hackers are actually doing businesses and the government a favor by exposing vulnerable and insecure systems. (Perhaps somewhat ironically, many ex-hackers, including convicted computer criminals, have been hired by companies because their expertise is useful to those companies wishing to build secure computer systems.) Other advocates, such as Kapor (23), point out that hacking, in its nonmalicious sense, played an important role in computer developments and breakthroughs. They note that many of today's "computer heroes" and successful entrepreneurs could easily be accused of having been hackers in the past. To support younger hackers and to provide them with legal assistance, advocates have set up the Electronic Frontier Foundation (EFF).

Even though hackers may enjoy some support for their activities from civil liberties organizations as well as from certain computer professional organizations, business leaders and government officials see hacking quite differently. Trespassing in cyberspace is itself, they argue, a criminal offense, regardless of whether these hackers are engaging merely in fun or pranks or whether they also go on to steal, abuse, or disrupt. Current legislation clearly takes the side of business, government, and law enforcement agencies with respect to hacking. Many on both sides of the debate, however, support legislation that would distinguish between the degree of punishment handed to "friendly" vs. "malicious" hackers. Many believe that current legislation, such as the Computer Fraud and Abuse Act of 1986, does not allow sufficiently for such distinctions.

### Computer Viruses and Computer Sabotage

Other "criminal" and abusive activities currently associated with computer use include *viruses, worms,* and related forms of computer sabotage. Rosenberg (2, p. 230) defines a computer virus as a "program that can insert executable copies of itself into programs," and a worm as a program or program segment that "searches computer systems for idle resources and then disables them by erasing various locations in memory." Some authors further distinguish categories such as *Bacterium, Trojan Horse, Time Bomb,* and *Logic Bomb.* Certain notorious worms and viruses have been referred to with names such as the *Michelangelo Virus,* the *Burleson Revenge,* and the *Pakistani Brain.* Not everyone, however, cares about such distinctions and subtleties. Branscomb (24) suggests that all flavors of worms and viruses can be referred to simply as rogue computer programs and that those who program them can be referred to as computer rogues.

A number of celebrated cases have brought attention to the vulnerability of computer networks, including the Internet, as well as to viruses, worms, and other rogue programs. One such case has come to be known as the Internet Worm or the Cornell Virus. Robert T. Morris, a graduate student at Cornell in 1988, released a worm that virtually brought activity on the Internet to a halt. To complicate matters, Morris was the son of one of the government's leading experts on computer security and a scientist at NSA (the National Security Agency). Morris later maintained that he did not intend to cause any damage, arguing that his program (virus) was just an experiment. Nonetheless, the incident raised questions of national security, vulnerability, and culpability that have since sparked considerable debate. Morris was eventually prosecuted and received a sentence that consisted of probation and community service.

A popular conception of the classic computer criminal is that of a very bright, technically sophisticated, young white male—as portrayed in the film *War Games.* Forester and Morrison (1, p. 41), however, describe the typical computer criminal as a "loyal, trusted employee, not necessarily possessing great computer expertise, who has been tempted by flaws in a computer system or loopholes in the controls monitoring his or her activity." They go on to note that *opportunity* more than anything else seems to be the root cause of such individuals engaging in criminal activities. It is also worth noting that the majority of computer crimes are carried out by employees of a corporation or internal members of an organization (such as a college student who alters academic transcripts) rather than by outsiders or those external to an organization. An interesting point also worth noting is that it would very likely not even occur to many of these individuals to steal physical property or currency from another person or from an organization. Perhaps then a closer look at the concept of intellectual property would be useful at this point.

### Software Piracy and Intellectual Property

At least one type of computer crime is made possible by the very nature or kind of property resulting from the code used to program computers (viz., *intellectual property*), which, unlike our conventional notion of (physical) property, is not tangible. As such, intellectual property is a concept that helps us better understand how at least some computer crimes, especially those involving *software piracy,* might be genuinely distinguished from noncomputer crimes. Instances of computer crimes related to software piracy can be viewed at two levels: one involving stand-alone computers and the other involving computer networks, including the Internet.

Consider a case in which an individual takes a diskette containing a computer manufacturer's word processing program, which was legitimately purchased by a friend, and makes a copy of that program for use on his or her personal computer. Unlike the preceding examples of theft involving automobiles or televisions, and unlike the case involving the theft of computers and computer accessories from a lab, in this instance no physical property has changed hands. The individual's friend still retains his or her original diskette with the word processing program. The difference, of course, is that the individual in question now also has a copy of the software contained on the original disk. In this case of "stolen" property, the original owner has neither lost possession of, nor has been deprived of, the original property. Of course, a case can be made that the company or organization who manufactured the software has been deprived of something (viz., a certain profit it would have received if the software had been purchased legally).

The preceding example illustrates a form of computer crime—an act of software piracy—carried out on a stand-alone computer system. Now consider an actual case that occurred on the Internet. In the Spring of 1994, an MIT student named David LaMacchia operated an electronic bulletin board system that posted the availability and address of copyrighted software applications on an anonymous Internet server in Finland. Users of the bulletin board were invited to download (make copies of) those applications, which they could then use on their own computers or possibly distribute to others. It should be noted that LaMacchia himself did not make copies of the software nor did he receive any payment for his services. Nonetheless he was arrested by federal agents and eventually prosecuted. It was unclear, however, what charges could be brought against LaMacchia because there was no legal precedent. For example, it was not clear that he could be prosecuted through the Computer Abuse and Fraud Act of 1986, because there was no clear intention to defraud or abuse. Eventually, authorities appealed to a federal wire-fraud statute to bring charges against the MIT student. Fortunately for LaMacchia, and unfortunately for many interested computer corporations who saw this particular case as a precedent for future cases, charges against LaMacchia had to be dropped. Consequently, the LaMacchia incident would seem to illustrate yet another case in which the legal system has failed to keep pace with IT.

So computers and computer networks, each in their own ways, make possible new kinds of criminal activities. First, the advent of stand-alone computers made possible a new kind of theft—one that did not require that stolen property necessarily be viewed as physical or tangible property. Nor did it require that the property be removed from its original place of residency or that the original owner of the property be deprived of its future possession. Using a personal computer, for example, one could simply duplicate or make several copies of a software program. Such a possibility, and eventual practice, required legislators to draft new kinds of crime, patent, and copyright legislation. It also forced judicial bodies to review certain legal precedents related to patents and copyright protections. Now issues involving "criminal" activity on computer networks, especially on the Internet, force legislators once again to reconsider certain laws.

## ACCESS AND EQUITY ISSUES

In the previous section we examined issues related to unauthorized access to computers and computer networks. Another side of the access issue is whether everyone should have at least some minimal means of Internet access. Many organizations, including those responsible for designing and implementing the National Information Infrastructure (NII), are currently wrestling with this question (viz., whether all citizens should have *universal access* to the Internet).

When IT was relatively new, there was much concern that this technology would be centralized and that centralization of IT would inevitably lead to the federal government having increased power and control. Also of concern was the question whether centralized computing on the part of government would favor those already in power and further serve to perpetuate inequities for those underprivileged and underrepresented groups. Other concerns focused on whether this phenomenon would ultimately lead to two classes of citizens: computer literate and noncomputer literate, or computer "haves" and "have-nots?" Although many concerns related to "information poor" and "information rich" still exist, those related to the fear of a strong centralized national computer network controlled by the federal government have, for the most part, subsided. In fact, many now fear that because cyberspace is so decentralized it is currently in a state of anarchy or chaos. Ironically, some now believe that cyberspace would benefit from greater government regulation and intervention, especially with respect to assisting certain disadvantaged groups.

Unlike earlier stand-alone computers, which were often viewed as "toys" for either the technically sophisticated or certain well-to-do Americans, networked computers—especially those connected to the Internet—have taken on a significance in our daily lives that few would have predicted in the early days of IT. Consequently, some now argue that everyone should have access to the Internet. However, it is not yet clear *who* should be responsible for ensuring that everyone has such access. In other words, should it be the role of government, or should the market itself be the driving force? A related question that also needs to be answered has to do with what form this access should take. For example, should there be a policy that merely guarantees access to anyone who wants it, or should such policy go one step farther and guarantee *universal service* to those unable to afford the basic costs currently required?

An analogy with telephone service may offer some insight on this issue. The Communications Act of 1934 guaranteed Americans universal service to telephones. Under that act, telephone companies were required to provide telephone service to poor people at low rates. Because having a telephone was considered an *essential* service for one's well being, rates were subsidized so that poorer citizens could enjoy this service. Many now believe that the Internet is (or will shortly become) an essential service for one's well being, from which they conclude that a policy similar to the Communications Act of 1934 should be established for the Internet? Chapman and Rotenberg (25), representing CPSR (Computer Professionals for Social Responsibility), argue that not only must everyone have universal access to the NII but that pricing should be structured so that service is affordable to everyone. When asked whether universal access should include hardware in addition to a mere point of Internet connection, Chapman and Rotenberg would respond by asking what good having a phone line would be if a person could not afford to purchase a telephone. They also believe that providing full service, and not mere access, is the morally responsible thing to do and that everyone will benefit from such a service.

Some critics of universal service point out that issues related to Internet access for the poor are complex and cannot be solved by simply applying a "techno-fix" to a problem that is political or social at its base. They point out that simply giving technology to people (e.g., donating computers to poor children in inner-city schools) does not address deeper issues such as those related to convincing parents and children of the importance Internet technology. Other critics are opposed to the use of tax subsidies to achieve universal service on the grounds that such a policy would be unfair to taxpayers with moderate incomes. Some critics of universal service also point out that because nearly everyone who wants to own a television or an automobile can find a way to purchase such items, the issue of Internet access for poorer citizens is at bottom really an issue of personal priorities and values.

Baase (22) notes that both critics and proponents of universal service seem to agree that there ought to be at least some level of universal *access* to the Internet for everyone who desires it. Recently, computer companies such as Oracle Corporation have developed a low-end, network access computer that will sell for under $300. This "stripped down" version of a personal computer includes a Web browser, modem, and other hardware and software features required for accessing the Internet. Whether this technology will satisfy the concerns for those advocating universal service, however, is not yet clear.

With the discussion of universal access, we conclude our analysis of social issues in the use of information technology. Unfortunately, there are many concerns that, because of space limitations, could not be more fully considered under separate headings or as separate major categories. Most of these concerns have, however, at least been identified and briefly described in appropriate sections of this study. For example, important contemporary issues such as censorship and free speech on the Internet were briefly identified in the sections entitled "Internet Search Engines and Bulletin Board Systems" and "Software Piracy and Intellectual Property." Also considered in those two sections were relatively recent concerns related to anonymity and identity on the Internet. Some important political concerns related to IT were examined in the sections entitled "Cryptography, Data Encryption, and the Clipper Chip" and "Electronic Surveillance and Social Control." Issues sometimes considered under the heading of "human obsolescence" were briefly examined in the section entitled "Job Displacement, Deskilling, and Automation." Social issues related to research and development in artificial intelligence (AI) were briefly considered in the section entitled "Robotics and Expert Systems." Some relatively recent concerns associated with "virtuality" were briefly considered in the section entitled "Remote Work and Virtual Organizations." Also examined in that section were issues related to equity and access, both of which were reconsidered in the final section of this study. The final section also includes a discussion of issues frequently associated with the impact of information technology on education and gender. Even though not every social issue related to IT could be discussed in this article, and even though most issues that were examined could not be considered in the detail warranted by their complexity, an attempt has been made to familiarize readers with a range of topics—some perhaps more traditional and others slightly more contemporary—that have come to define the field of information technology and society.

## BIBLIOGRAPHY

1. T. Forester and P. Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing,* 2nd ed., Cambridge, MA: MIT Press, 1994.
2. R. S. Rosenberg, *The Social Impact of Computers,* 2nd ed., San Diego: Academic Press, 1997.
3. M. G. Wessells, *Computer, Self, and Society,* Englewood Cliffs, NJ: Prentice-Hall, 1990.
4. A. Mowshowitz, Virtual organization, *Commun. ACM,* **40** (9): 30–37, 1997.
5. R. A. Spinello, *Case Studies in Information and Computer Ethics,* Upper Saddle River, NJ: Prentice-Hall, 1997.
6. G. Marx and S. Sherizen, Monitoring on the job: How to protect privacy as well as property, *Technol. Rev.,* 63–72, November/December 1986. Reprinted in T. Forester (ed.), *Computers in the Human Context: Information Technology, Productivity, and People,* Cambridge, MA: MIT Press, 1989, pp. 397–406.
7. S. Warren and L. Brandeis, The right to privacy, *Harvard Law Rev.,* **4** (5): 193–220, 1890.
8. R. Gavison, Privacy and the limits of the law, *Yale Law J.,* **89**: 421–471, 1980.
9. J. H. Moor, The ethics of privacy protection, *Library Trends,* **39** (1 & 2): 69–82, 1990.
10. C. Freid, Privacy (a moral analysis). In F. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology,* Cambridge, MA: Cambridge University Press, 1984, pp. 203–222.
11. J. Rachels, Why privacy is important, *Philosophy and Public Affairs,* **4** (4): 323–333, 1975.
12. D. G. Johnson, *Computer Ethics,* 2nd ed., Englewood Cliffs, NJ: Prentice-Hall, 1994.
13. R. O. Mason, Four ethical issues of the information age, *MIS Quart.,* **10** (1), 1986.
14. C. Dunlop and R. Kling, (eds.) *Computerization and Controversy: Value Conflicts and Social Choices,* San Diego: Academic Press, 1991.
15. R. Kusserow, The government needs computer matching to root out waste and fraud, *Commun. ACM,* **27** (6): 446–452, 1984.
16. J. Shattuck, Computer matching is a serious threat to individual rights, *Commun. ACM,* **27** (6): 538–541, 1984.

17. H. T. Tavani, Computer matching and personal privacy: Can they be compatible? In *Proc. Symp. Comput. Quality Life (CQL '96),* pp. 197–201, New York: ACM Press, 1996.

18. D. G. Johnson and H. Nissenbaum (eds.), *Computing, Ethics & Social Values,* Englewood Cliffs, NJ: Prentice-Hall, 1995.

19. H. T. Tavani, Internet search engines and personal privacy. In *Proc. Conf. Comput. Ethics: Philosophical Enquiry (CEPE '97),* pp. 169–177, Rotterdam: The Netherlands: Erasmus University Press, 1997.

20. J. Palfreman and D. Swade, *The Dream Machine: Exploring the Computer Age,* London: BBC Books, 1991.

21. S. Levy, The battle of the clipper chip, *The New York Times Magazine,* June 12, 1994. Reprinted in D. Johnson and H. Nissenbaum (eds.), *Computers, Ethics & Social Responsibility,* Upper Saddle River, NJ: Prentice-Hall, 1995, pp. 651–664.

22. S. Baase, *A Gift of Fire: Social, Legal, and Ethical Issues in Computing,* Upper Saddle River, NJ: Prentice-Hall, 1997.

23. M. Kapor, Civil liberties in cyberspace, *Sci. Amer.,* September 1991. Reprinted in D. Johnson and H. Nissenbaum (eds.), *Computers, Ethics & Social Responsibility,* Upper Saddle River, NJ: Prentice-Hall, 1995, pp. 645–650.

24. A. W. Branscomb, Rogue computer programs and computer rogues: Tailoring the punishment to fit the crime, *Rutgers Comput. Technol. Law J.,* **16**: 1–61, 1990.

25. G. Chapman and M. Rotenberg, The national information infrastructure: a public interest opportunity, *CPSR Newsletter,* **11** (2): 1–23, 1993.

### *Reading List*

C. Beardon and D. Whitehouse (eds.), *Computers and Society.* Norwood, NJ: Ablex Publishers, 1994.

T. W. Bynum, *Information Ethics: An Introduction,* Cambridge, MA: Blackwell Publishers, 1998.

S. L. Edgar, *Morality and Machines: Perspectives on Computer Ethics,* Sudbury, MA: Jones and Bartlett Publishers, 1997.

R. G. Epstein, *The Case of the Killer Robot: Cases About Professional, Ethical, and Societal Dimensions of Computing,* New York: Wiley, 1997.

M. D. Ermann, M. B. Williams, and M. S. Shauf (eds.), *Computers, Ethics, and Society,* 2nd ed., New York: Oxford University Press, 1997.

D. G. Garson, *Computer Technology and Social Issues,* Harrisburg, PA: Idea Group Publishing, 1995.

C. Huff and T. Finholt (eds.), *Social Issues in Computing: Putting Computing in Its Place,* New York: McGraw-Hill, 1994.

T. Jewett and R. Kling, *Teaching Social Issues of Computing: Challenges, Ideas, and Resources,* San Diego: Academic Press, 1996.

E. A. Kallman and J. P. Grillo, *Ethical Decision Making and Information Technology: An Introduction with Cases,* 2nd ed., New York: McGraw-Hill, 1996.

R. Kling (ed.), *Computerization and Controversy: Value Conflicts and Social Choices,* 2nd ed., San Diego: Academic Press, 1996.

C. Mitcham, *Thinking Through Technology: The Path Between Engineering and Philosophy,* Chicago: University of Chicago Press, 1994.

N. Negroponte, *Being Digital,* New York: Knopf, 1995.

E. Oz, *Ethics for the Information Age,* Burr Ridge, IL: William C. Brown Communications, 1994.

H. Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier,* New York: HarperPerennial, 1994.

S. Rogerson and T. W. Bynum (eds.), *Information Ethics: A Reader,* Cambridge, MA: Blackwell Publishers, 1998.

K. Schellenberg (ed.), *Computers in Society,* 6th ed., Guilford, CT: Dushkin Publishing Group, 1996.

R. E. Sclove, *Democracy and Technology,* New York: The Guilford Press, 1995.

R. A. Spinello, *Ethical Aspects of Information Technology,* Upper Saddle River, NJ: Prentice-Hall, 1995.

D. Tapscott, *Digital Economy: Promise and Peril in the Age of Networked Intelligence,* New York: McGraw-Hill, 1996.

H. T. Tavani (ed.), *Computing, Ethics, and Social Responsibility: A Bibliography,* Palo Alto, CA: Computer Professionals for Social Responsibility (CPSR) Press, 1996. (Identifies more than 2100 sources on IT, ethics, and society and is also available online at: http://www.siu.edu/departments/coba/mgmt/iswnet/isethics/biblio.)

A. H. Teich (ed.), *Technology and the Future,* 7th ed., New York: St. Martin's Press, 1997.

S. Turkle, *Life on the Screen: Identity in the Age of the Internet,* New York: Simon and Schuster, 1995.

S. H. Unger, *Controlling Technology: Ethics and the Responsible Engineer,* 2nd ed., New York: Holt, Rinehart, and Winston, 1994.

J. Weckert and D. Adeney, *Computer and Information Ethics,* Westport, CT: Greenwood Press, 1997.

P. A. Winters (ed.), *Computers and Society,* San Diego: Greenhaven Press, 1997.

HERMAN T. TAVANI
Rivier College

## SOCIAL AND ETHICAL ISSUES IN COMPUTING.

See SOCIAL AND ETHICAL ASPECTS OF INFORMATION TECHNOLOGY.