CHAPTER 8

Computer Ethics

In November of 2007, the United Kingdom's tax agency reported a major security breach to the police. Tax information, including intimate personal knowledge and bank account numbers, for some 25 million British citizens—almost half the country's population—had been loaded onto two disks and sent by mail courier to an audit office. To the astonishment of all, the disks had gone missing. Worse, the information on them was unencrypted. The British populace was thrown into a state of financial terror. The competency of the five-month-old government of Prime Minister Gordon Brown was brought into question. The case illustrates the scale of concerns about privacy and security in the age of computers, and also the unpredictable interaction of sophisticated technological structures and human fallibility.

Computers have become the technological backbone of society. Their degree of complexity, range of applications, and sheer numbers continue to increase. Through telecommunication networks they span the globe. Yet electronic computers are still only a few decades old, and it is difficult to foresee all the moral issues that will eventually surround them. The present state of computers is sometimes compared to that of the automobile in the early part of this century. At that time the impact of cars on work and leisure patterns, pollution, energy consumption, and sexual mores was largely unimagined. If anything, it is more difficult to envisage the eventual impact of computers because they are not limited to any one primary area of use as is a car's function in transportation.

It is already clear, however, that computers raise a host of difficult moral issues, many of them connected with basic moral concerns such as free speech, privacy, respect for property, informed consent, and harm.[1] To evaluate and deal with these issues, a new area of applied ethics called computer ethics has sprung up. Computer ethics has special importance for the new groups of professionals emerging with computer technology, for example, designers of computers, programmers, systems analysts, and operators. To the extent that engineers design, manufacture, and apply computers, computer ethics is a branch of engineering ethics. But the many professionals who use and control computers share the responsibility for their applications.

Some of the issues in computer ethics concern shifts in power relationships resulting from the new capacities of computers. Other issues concern property, and still others are about invasions of privacy. All these issues may involve "computer abuse": unethical or illegal conduct in which computers play a central role (whether as instruments or objects).

The Internet and Free Speech

The Internet has magnified all issues in computer ethics. The most powerful communication technology ever developed, and a technology used daily by hundreds of millions of people, the Internet gained widespread use only during the 1990s. Its modest beginning, or forerunner, came from a simple idea of J. C. R. Licklider.[2]

Licklider was a psychologist who had wide interests in the newly emerging computer technology. In 1960 he conceived of a human-computer symbiosis in which the powers of humans and computers were mutually enhancing.[3] The breadth of his vision, together with his administrative skills, led to his appointment a few years later as the director of the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. He quickly saw that the variety of computer-involved military projects was becoming a Tower of Babel, and he wrote a revolutionary memo

[1] For an overview of issues affecting business, see Richard T. De George, "Ethical Issues in Information Technology," in *The Blackwell Guide to Business Ethics,* ed. Norman E. Bowie (Malden, MA: Blackwell, 2002), 267–88. There are now many useful anthologies on computer ethics, including Richard A. Spinello and Herman T. Tavani, eds., *Readings in CyberEthics*, 2nd ed. (Boston: Jones and Bartlett, 2004), and Terrell Ward Bynum and Simon Rogerson, eds., Computer Ethics and Professional Responsibility (Malden, MA: Blackwell Publishing, 2004).

[2] M. Mitchell Waldrop, *The Dream Machine: J. C. R. Licklider and the Revolution that Made Computing Personal* (New York: Penguin, 2001); and *John Naughton, A Brief History of the Future: The Origins of the Internet* (London: Weidenfeld, 1999).

[3] "Man-Computer Symbiosis," *IRE Transactions on Human Factors in Electronics,* vol. HFE-1 (March 1960): 4–11; reprinted in *In Memorium: J. C. R. Licklider, 1915–1990,* ed. Robert W. Taylor (Palo Alto, CA: Digital Systems Research Center Reports, 1990).

calling for a move toward a unified communication system. In 1969, ARPA funded projects in universities and corporations that created an ARPA network, or ARPANET. In the 1980s, some universities developed their own communications networks, and their eventual merging with ARPANET became the Internet, which is now a global network of networks, initially using the infrastructure of the telephone system and now carried by many telecommunication systems by wire, fiber, or wireless systems. The World Wide Web (Web), which is a service run on the Internet, emerged from the Hypertext Markup Language and transfer protocol developed at the European particle physics lab and is used in a multimedia format of text, pictures, sound, and video. During the early 1990s, the Web was opened to business, e-mail, and other uses that continue to expand.

CERN

It is now clear to all that the Internet provides a wellspring of new ways to be in contact with other people and with sources of information. It has also created greater convenience in ordering consumer items, paying bills, and trading stocks and bonds. Like other major “social experiments,” it also has raised a host of new issues. One set of issues centers on free speech, including control of obscene forms of pornography, hate speech, spam (unwanted commercial speech), and libel.

In a wide sense, pornography is sexually explicit material intended primarily for sexual purposes (as distinct, say, from medical education). *Obscene* pornography is pornography that is immoral or illegal in many countries, and is not protected in the United States by the First Amendment rights to free speech. U.S. laws define obscenity as sexually explicit materials that appeal to sexual interests, lack serious literary, artistic, scientific, or other value, and are offensive to reasonable persons as judged by a community’s standards. Needless to say, there is considerable disagreement about what this means, and the definition is relative to communities that might have differing standards. At the same time, there is wide agreement that child pornography and extremely violent and degrading portrayals of women are obscene, and most local communities have attempted to control them. The Internet has made such control extremely difficult, as images and texts can be transmitted easily from international sources to a child’s home computer. There are now hundreds of thousands of pornographic Web sites, with hundreds more created each day, many of which contain obscene material.

Hate speech, unlike obscenity, is not forbidden constitutionally. Not surprisingly, then, the Internet has become a powerful resource for racist and anti-Semitic groups to spread their messages. Those messages were heard, for example, by Eric Harris and Dylan Klebold, who massacred their fellow students at

Columbine High School in 1999. And there is no question that this most powerful medium makes it much easier for hate groups to organize and expand.

Two types of control of pornography and hate speech have been attempted: top-down control by governments, and bottom-up controls by individuals and groups in the marketplace.[4] Top-down controls have been attempted by both Democrats and Republicans. For example, Congress passed the Communications Decency Act, signed by President Clinton in 1996, which forbade transmitting indecent and patently offensive material to minors. A year later the Supreme Court declared the act unconstitutional. In contrast, a 2001 federal statute, the Children's Internet Protection Act, required libraries receiving federal funds to use filters to block pornographic material from library computers used by the public. In 2003 the statute was upheld as constitutional by the Supreme Court in *United States v. American Library Association*. Legislatures and courts continue to seek reasonable balance between protecting free speech and advancing other important values.

Parents who purchase blocking or filtering software exemplify bottom-up controls. If those controls are extended from homes to schools and other public settings, according to Richard Spinello, certain procedures should be followed.[5] The controls should be voluntary, in the sense that the relevant constituencies are allowed full participation in the process. Web sites that provide rating services for screening material should openly acknowledge the criteria they use. They should avoid hidden political agendas. (CyberSitter, for example, presented itself as blocking child pornography but then also blocked access to the National Organization for Women.) And the level of blocking should be low-level, rather than at unnecessarily blanket levels.

Some enthusiasts argue that controlling free speech on the Internet not only will prove unfeasible on any large scale, but also that such uncontrollability is good. The Internet could be the ultimate defender of principles of freedom, equality, and opportunity. It could gradually undermine the power of tyrants who have blocked democratic freedoms in their country, if unfettered communication channels can be maintained.

Power Relationships

Computers and the Internet dramatically increase the ability of centralized bureaucracies to manage enormous quantities of data,

[4] Richard Spinello, *Cyberethics: Morality and Law in Cyberspace* (Boston: Jones and Bartlett Publishers, 2000), 35–42.

[5] Ibid., 54.

involving multiple variables, and at astonishing speed. During the 1960s and 1970s social critics became alarmed at the prospect that computers would concentrate power in a few centralized bureaucracies of big government and big business, thereby eroding democratic systems by moving toward totalitarianism.

These fears were not unwarranted, but they have lessened because of recent developments in computer technology. In the early stages of computer development there were two good reasons for believing that computers would inevitably tend to centralize power.[6] Early large computers were many times cheaper to use when dealing with large tasks than were the many smaller computers it would have taken to perform similar tasks. Thus it seemed that economics would favor a few large and centrally located computers, suggesting a concentration of power in a few hands. Moreover, the large early computer systems could only be used by people geographically close to them, again implying that relatively few people would have access to them.

The development and proliferation of microcomputers changed all this. Small computers became increasingly powerful and economically competitive with larger models. Furthermore, remote access and time-sharing allowed computer users in distant locations to share the resources of large computer systems. These changes opened new possibilities for decentralized computer power. More recently, the purpose of linking computers has not been so much for the purpose of reaching machines with greater number-crunching capabilities as for the opportunities to exchange information. The physical links that make this possible, and the data processing technology that is associated therewith, make up the Internet.

Once, it was feared that computers would give the federal government far greater power to control nationally funded systems, such as the welfare and medical systems, lessening control by local and state governments. But in fact, data systems have turned out to be two-way, allowing both small governments and individuals to have much greater access to information resources amassed at the federal level.

Computers are powerful tools that do not by themselves generate power shifts. They contribute to greater centralization or decentralization insofar as human decision makers direct them. This is not to say that computers are entirely value-neutral. It is to say that moral issues about power relationships tend to be nuanced and contextual. A few examples follow.

[6] Herbert A. Simon, "The Consequences of Computers for Centralization and Decentralization," in *The Computer Age: A Twenty-Year View,* ed. Michael L. Dertouzos and Joel Moses (Cambridge, MA: MIT Press, 1979), 212–28.

Job Elimination. Computers have led and will continue to lead to the elimination of some jobs. What employer attitudes are desirable in confronting this situation? No employer, of course, can afford to pay people for doing no work. Yet especially within large corporations, it is often possible to readjust work assignments and workloads, to wait for people to retire, to change jobs voluntarily, to retrain employees for jobs within or outside the company, or even to introduce a 32-hour work week for all before laying off employees. Such benign employment practices have often been embraced from prudential motives to prevent a public and employee backlash against the introduction of computer technologies that eliminate jobs,[7] but moral considerations of human costs should be weighed even more heavily.

Customer Relations. There are questions about the public accountability of businesses using computer-based services. It can be either very difficult or relatively simple for a consumer to notice and correct computer errors or computer printed errors. For example, a grocery-store receipt can itemize items either by obscure symbols or by simple words understandable to a customer. The prices on cash register receipts have been shown to sometimes vary from those posted on the shelves. Here again moral reasons reinforce long-term good business sense in favoring policies that are beneficial to consumer needs and interests, making consumers feel less vulnerable.

Biased Software. In addition to computer hardware there is software, and programs can quite easily be biased, as can any form of communication or way of doing things. For example, a computerized study of the feasibility of constructing a nuclear power plant can easily become biased in one direction or another if the computer program is developed by a group entirely for or against nuclear energy.[8]

Stock Trading. Programmed trading is the automatic, hands-off, computer trading of stocks, futures, and options on the stock market. Did this practice contribute to the "meltdown on Black Monday" (October 19, 1987), when the U.S. stock market took a precipitous plunge, and should it be controlled? What assurances are there that NASDAQ, an electronic trading system linking

[7] Rob Kling, *Social Issues and Impacts of Computing* (Irvine, CA: University of California Press, 1979), 10.

[8] Deborah G. Johnson, *Computer Ethics,* 3rd ed. (Upper Saddle River, NJ: Prentice Hall, 2001).

510 stock traders, can prevent its members from exercising their power to manipulate the market when, as alleged, some have postponed requested purchases until after they have bought some shares of the same stock on their own, thereby raising the value of their newly acquired shares as well as increasing their commissions on the subsequent purchase of the shares requested by the customer? Controls have since been put into effect, but critics argue that more needs to be done.

Military Weapons. Military officials have often supported autonomous weapons that can be aimed and fired by onboard computers that make all necessary decisions, including enemy identification. The “launch-on-warning” policy for strategic missiles advanced by the U.S. military during the late 1980s could be considered an autonomous weapon. There is a dangerous instability in such automated defense systems, even if they are working perfectly. Even if all the nuclear warning software works without error, and the hardware is fail-safe, the combination of two such correctly functioning but opposing systems is unstable. This is because secrecy prevents either system from knowing exactly what the other is doing, which means that any input that could be interpreted as a danger signal must be responded to by an increase in readiness on the receiving side. That readiness, in turn, is monitored by the opposing side, which then steps up its readiness, and so on. This feedback loop triggers an escalating spiral. Does the possibility of an entirely unprovoked attack triggered by the interaction of two perfectly operating computer-based systems enhance security?[9]

Property

The most troublesome issues about property and computers fall under two general headings. The first is the use of computers in embezzlement and other forms of stealing money or financial assets. It is the most widely publicized form of computer crime and also the most morally clear-cut. The second set of issues concerns the theft of software and information. Here the issues are more complex.

Embezzlement. Computers are only incidentally involved when extortion is attempted through a phone that is part of a computerized telephone system.[10] By contrast, computers are

[9] Boris V. Rauschenbakh, “Computer War,” in *Breakthrough: Emerging New Thinking,* ed. Anatoly Gromyko and Martin Hellman (New York: Walker, 1988).

[10] Rob Kling, “Computer Abuse and Computer Crime as Organizational Activities,” *Computer/Law Journal* 2 (Spring 1980): 408.

centrally involved when an extortionist disguises his voice by means of a computer as he talks into a phone. And computers are even more centrally involved when an unauthorized person uses a telephone computer system to obtain private phone numbers, or when someone maliciously alters or scrambles the programming of a telephone computer.

Two factors make computers especially troublesome: (1) their speed and geographic coverage, which allows large numbers of people to be victimized, and (2) the difficulty of tracing the underlying transactions to apprehend the thieves. This problem is compounded when the communication lines linking the computers involved cross national boundaries.

Some of the most commonly discussed cases of computer abuse are instances of outright theft and fraud, of which there are many forms: (1) stealing or cheating by employees at work; (2) stealing by nonemployees or former employees; (3) stealing from or cheating clients and consumers; (4) violating contracts for computer sales or service; (5) conspiring to use computer networks to engage in widespread fraud. Especially alarming, the Internet has led to an explosion of identity theft, in which personal information is obtained and used to forge documents and commit fraud.

Public interest has often been drawn to the glamorous capers of computer criminals.[11] Enormous sums of money have been involved. The amount for an average computer-related embezzlement is 20 times the amount stolen in conventional embezzlement; many millions are often involved. Yet the giant thefts uncovered are believed to be only a small fraction of computer theft.

Crime by computer has proved to be unusually inviting. Computer crooks tend to be intelligent and to view their exploits as intellectual challenges. In addition, the computer terminal is both physically and psychologically far removed from face-to-face contact with the victims of the crimes perpetrated. Unlike violent criminals, computer criminals find it easy to deceive themselves into thinking they are not really hurting anyone, especially if they see their actions as nothing more than pranks. In addition, there are often inadequate safeguards against computer crime. The technology for preventing crime and catching criminals has

[11] Thomas Whiteside, *Computer Capers* (New York: Crowell, 1978); Tom Logsdon, *Computers and Social Controversy* (Potomac, MD: Computer Science Press, 1980), 163–64.

lagged behind the implementation of new computer applications. Computers reduce paperwork, but this has the drawback of removing the normal trail of written evidence involved in conventional white-collar crime (forgeries, receipts, etc.). Finally, the penalties for computer crime, as for white-collar crime in general, are mild compared with those for more conventional crimes.

Computer crime raises obvious moral concerns of honesty, integrity, and trust. It also forces a rethinking of public attitudes about crime and its punishment. Is it fair that the penalty for breaking into a gas station and stealing $100 should be the same as for embezzling $100,000 from a bank account? How should society weigh crimes of minor violence against nonviolent crimes involving huge sums of money?

The potential for computer crime should enter significantly into the thinking of engineers who design computers. In fact, protection against criminal abuse has become a major constraint for the effective and successful design of many computer systems and programs. Engineers must envisage not only the intended context in which the computer will be used, but both likely and possible abuses.

For some time, secret computer passwords have been used as a security feature. More recently introduced, and still of limited effectiveness, is data encryption. This technique is widely employed to prevent theft from funds transfer systems. In data encryption, messages are scrambled before transmission over communication lines and unscrambled after reception according to secret codes. Such devices, of course, require special precautions in maintaining confidentiality and security, and engineers have a major role to play in making recommendations in these areas. Of particular concern is the insistence by investigative agencies of the government that they be given access to decryption keys and that only prescribed codes be used. All of this tends to reduce the privacy of every user of the transmission system.

Data and Software. *Data,* in this context, refers to information stored in a computer, whether the information expresses facts or falsehoods. *Software* refers to programs that direct an electronic machine (hardware) to perform certain tasks, typically tasks involving problem solving. Programs have several aspects: (1) an algorithm, which explicitly states the steps in solving a problem; (2) a source code, which expresses the algorithm in a general computer language (such as Pascal, C, or FORTRAN); and (3) an object code, which translates a source code into the specific machine language of ones and zeros. Which of these aspects of computers are property, which can be privately owned, and which can be protected?

The question turns out to be surprisingly complex, and it forces us to clarify what property and property rights are (as we noted in Chapter 3). According to one primitive idea, persons' property is anything they create through their labor. John Locke, in the seventeenth century, developed this idea. According to Locke, we own our body and anything we "mix" with our body through labor. Locke had in mind a "state of nature" in which a person came to own a tree by either growing it or cutting it down, assuming no one else had previously done so. But once within a "state of society," property cannot be defined entirely by this simple idea. Property becomes primarily what laws define as the permissible use of things.

Laws define what can be owned, how exchanges of ownership may occur, and especially what ownership means in terms of the use of things of a given type. A car owner cannot drive on public roads until he or she satisfies laws about vehicle registration, insurance, and driver's licenses.[12] Again, a purchased book is the owner's, but that does not mean he or she can copy the entire book and sell it. What about ideas that a person or company develops for creating computers? Who owns them?

In the United States, computer hardware is protected by patent laws. Software can be protected by trade secret laws or by copyrights. Trade secret laws permit employers to require their employees not to divulge proprietary information. Obviously, trade secrets are useless once software is made publicly available as a marketed product. Here copyright laws offer the best protection.

Because of the newness of software, traditional laws are being extended to software gradually, often on a case-by-case basis. Generally, algorithms cannot be copyrighted. They are regarded as mathematical formulas that can be discovered but not owned. Laws stipulate that copyrighted material must be "intelligible," and the courts have tended to rule that object codes (written in machine language of ones and zeros) are not intelligible to humans and hence cannot be copyrighted. Source codes, however, are regarded as intelligible and can be copyrighted.

Patents on software are restricted to detailed coding sequences and other processes rather than final products. Not only are software patents difficult to obtain, they also create international disagreements because of differences in patent laws.

What does this mean? Does a company steal the property of a software producer if it buys one copy and then reproduces dozens of copies for its other employees? Yes, unless a special agreement has

[12] Deborah G. Johnson, *Computer Ethics.*

been reached with the software producer. Is making a dozen copies of a program borrowed from a friend for resale stealing? Yes.

Of course, one can always argue that particular laws are unjust, or, alternatively, that there are other overriding moral reasons that justify breaking a particular law. Nevertheless, the widespread practice of copying clearly denies the creators and producers of the programs the money to which they are entitled, and as such it is a form of theft. Forming user groups where self-generated programs are freely exchanged is another matter and a practice that should be encouraged.

Privacy

Storage, retrieval, and transmission of information using computers as data processors has revolutionized communication. Yet this very benefit poses moral threats to the right to privacy.[13] By making more data available to more people with more ease, computers make privacy more difficult to protect. Here we will discuss privacy and confidentiality for individuals, but the issues are similar for corporations.

Inappropriate Access. Imagine that you are arrested for a serious crime you did not commit—for example, murder or grand theft. Records of the arrest, any subsequent criminal charges, and information about you gathered for the trial proceedings might be placed on computer tapes easily accessible to any law enforcement officer in the country. Prospective employers doing security checks could gain access to the information. The record clearly indicates that you were found innocent legally. Nevertheless, that computerized record could constitute a standing bias against you for the rest of your life, at least in the eyes of many people with access to it.

The same bias could exist if you had actually committed some much less serious crime, say a misdemeanor. If you were arrested when you were 15 years old for drinking alcohol or swearing at an officer, for example, the record could stay with you. Or imagine that medical data about your visits to a psychiatrist during a period of depression could be accessed through a data bank. Or that erroneous data about a loan default were placed in a national credit data bank to which you had limited access. Or merely suppose that your tastes in magazine subscriptions were known easily to any employer or ad agency in the country and in the world.

[13] M. David Ermann, Mary B. Williams, and Michele S. Shauf, *Computers, Ethics, and Society,* 2nd ed. (New York: Oxford University Press, 1997).

Hackers. Finally there are "hackers," by which we mean that minority of computer enthusiasts sometimes called "crackers," who compulsively challenge any computer security system.[14] Some carry their art to the point of implanting "time bombs" or "Trojan horses" (unwanted codes that copy themselves into larger programs) that will "choke networks with dead-end tasks, spew out false information, erase files, and even destroy equipment."[15] This form of vandalism can be extremely harmful and is a straightforward violation of property rights, if only by reducing productivity by shutting down computer systems.

But suppose that the hacker's activities are limited to breaking into systems for shock value and a display of cunning. Is that so bad? After all, isn't it the responsibility of people to take appropriate steps to maintain their privacy, and isn't the hacker actually providing a stimulus for organizations to be more careful in protecting sensitive information? That is like arguing that it is all right to videotape the private activities of a neighbor who accidentally or carelessly leaves a window open. It is like arguing that if I do not invest in maximum security for my car that I authorize others to enter it.

Hackers sometimes employ a more extreme rationale in defending their activities. They contend that all information ought to be freely available, that no one should be allowed to own information, especially in a democratic society that respects individual rights to pursue knowledge. Essentially, this argument makes freedom of information paramount. Yet, there are at least three other important values that place legitimate limits on access to information: individual privacy, national security, and freedom within a capitalist economy to protect proprietary information essential in pursuing corporate goals.

Legal Responses. The potential abuses of information about us are unlimited and become more likely with the proliferation of access to that information. For this reason, a series of laws has been enacted.[16] For example, the 1970 Fair Credit Reporting Act restricted access to credit files. Information can be obtained only by consumer consent or a court order, or for a limited

[14] For a wider and positive meaning of "hacker," see Steven Levy, *Hackers* (New York: Penguin, 2001); and Pekka Himanen, *The Hacker Ethic* (New York: Random House, 2001).

[15] Eliot Marshall, "The Scourge of Computer Viruses," *Science* 240 (April 8, 1988): 133–34.

[16] James Rule, Douglas McAdam, Linda Stearns, and David Uglow, *The Politics of Privacy* (New York: New American Library, 1980).

range of valid credit checks needed in business, employment, and insurance transactions or investigations. The act also gave consumers the right to examine and challenge information about themselves contained in computerized files.

The Privacy Act of 1974 extended this right of inspection and error correction to federal government files. It also prohibited the information contained in government files from being used for purposes beyond those for which it was originally gathered unless such use was explicitly agreed to by the person whose file it is. Unfortunately, there is a loophole in the act that allows sharing of information among government agencies. Accordingly, there are now more than 100 separate computer matching programs to routinely pass data between agencies, greatly compromising personal privacy. However, many other laws have been passed and are being considered to extend the protection of individual privacy within private business and industry.

Such laws are expensive to implement, sometimes costing tens and hundreds of millions of dollars to enforce. They also lessen economic efficiency. In special circumstances they can have harmful effects on the public. There is little question, for example, that it would save lives if medical researchers had much freer access to confidential medical records. And it would be much more convenient to have one centralized National Data Center. This idea was proposed in the mid-1960s and is still alive in the minds of many. But privacy within a computerized world can apparently be protected only by making it inconvenient and expensive for others to gather information about us in data banks.

Additional Issues

Many of the issues in engineering ethics arise within the context of computer work. New variations or new difficulties may be involved, often owing to the high degree of job complexity and required technical proficiency introduced by computers. We provide some representative examples in the paragraphs that follow.

Computer Failures. Failures can occur because of errors in hardware or software. Hardware errors do not occur often, and when they do they usually do so quite obviously. An exception was Intel's highly touted Pentium chip, introduced in 1993. It produced very slight and rare errors in floating-point arithmetic. Perhaps more serious was the loss of confidence Intel suffered by not revealing the error before it was detected by a user.

Software errors are a different matter. They can be very serious indeed, as exemplified by the collapse of the computer-designed "space-frame" roof for the Hartford Civic Center in

1978, the deaths of several patients who received uncontrolled amounts of radiation in a radiation therapy machine between June 1985 and January 1987, and a major disruption of AT&T's computer-controlled long distance telephone system in 1990.

Errors can occur because of faulty logic in the design formulation, or they can be introduced in coding the machine instructions. Trial runs are absolutely essential to check out new programs, but if seasoned designers have already been replaced by canned programs and inexperienced engineers, the chance of noticing errors is slim. Perhaps this challenge to responsible management can be best met by engaging consultants to oversee the programming effort and to check the results of trial runs when the company does not have such in-house talent.

Computer Implementation. It should not be necessary to say so, but a changeover to a new computer system should never be attempted without having the old system still operational. Computer vendors who are too sure of their machines to recommend some redundancy during a changeover display enough hubris for it to qualify as one of the seven deadly sins. What can happen? Take the case of a bakery that had to file for bankruptcy after 75 successful years in the business. Part of the blame goes to slow summer sales, but there were extraordinary losses during the switch to a new computer system.

Health Conditions. Engineers who supervise computer personnel or design computer terminals should check that ergonomic considerations are in effect to reduce back problems, provide wrist support, offer good keyboard layouts to prevent carpal tunnel syndrome, and offer good lighting and flicker control.

Discussion Questions

1. Consider an engineer who develops a program used as a tool in developing other programs assigned to her. Subsequently she changes jobs and takes the only copy of the first program with her for use on her new job. Suppose first that the program was developed on company time under the first employer's explicit directives. Taking it to a new job without the original employer's consent would be a violation of that employer's right to the product (and possibly a breach of confidentiality). As a variant situation, however, suppose the program was not written under direct assignment from the first employer, but was undertaken by the engineer at her own discretion to help her on her regular work assignments. Suppose also that to a large extent the program was developed on her own time on weekends, although she

did use the employer's facilities and computer services. Did the employer own or partially own the program? Was she required to obtain the employer's permission before using it on the new job?[17]

2. Dependence on computers has intensified the division of labor within engineering. For example, civil engineers designing a flood control system have to rely on information and programs obtained from systems analysts and implemented by computer programmers.

   Suppose the systems analysts refuse to assume any moral or legal responsibility for the safety of the people affected by the flood control plans, arguing that they are merely providing tools whose use is entirely up to the engineers. Should the civil engineers be held accountable for any harm caused by poor computer programs? Presumably their accountability does extend to errors resulting from their own inadequate specifications that they supply to the computer experts. Yet should not the engineers also be expected to contract with computer specialists who agree to be partially accountable for the end-use effects of their programs?[18]

3. An engineer working as a computer programmer played a minor role in developing a computer system for a state department of health. The system stored medical information on individuals identified by name. Through no fault of the engineer, few controls had been placed on the system to limit easy access to it by unauthorized people. Upon learning of this, the engineer first informed his supervisor and then higher management, all of whom refused to do anything about the situation because of the anticipated expense required to correct it. In violation of the rules for using the system, the programmer very easily obtained a copy of his own medical records. He then sent them to a state legislator as evidence for his claims that the right of citizens to confidentiality regarding such information was threatened by the system. Was his behavior improper? Was his subsequent firing justified?[19]

4. A project leader working for a large retail business was assigned the task of developing a customer billing and credit system. The budget assigned for the project appeared at first to be adequate. Yet by the time the system was half completed it was clear the funds were not nearly enough. The project leader asked for more money, but the request was denied. He fully informed manage-

[17] Donn B. Parker, *Ethical Conflicts in Computer Science and Technology* (Arlington, Virginia: AFIPS Press, 1979), 72–74. Case studies adapted in the text with permission of author and publisher.

[18] Ibid., 34–38.

[19] Ibid., 90–93.

ment of the serious problems that were likely to occur if he had to stay within the original budget. He would be forced to omit several important program functions for convenience and safety: for example, efficient detection and correction mechanisms for errors, automatic handling and reporting of special customer exceptions, and audit controls. Management insisted that these functions could be added after the more minimal system was produced and installed in stores. Working under direct orders, the project leader completed the minimal system, only to find his worst fears realized after it was installed. Numerous customers were given incorrect billings or ones they could not understand. It was easy for retail salespersons to take advantage of the system to steal from the company, and several did so. Within a year the company's profits and business were beginning to drop. This led to middle-level management changes, and the project leader found himself blamed for designing an inadequate system.

Did the project leader have an obligation either to clients or to the company to act differently than he did? Did he have a moral right to take further steps in support of his original request or later to protect himself from managerial sanctions?[20]

5. A team of engineers and biomedical computer scientists develop a system for identifying people from a distance of up to 200 meters. A short tube attached to a sophisticated receiver and computer, and aimed at a person's head, reads the individual's unique pattern of brain waves when standard words are spoken. The team patents the invention and forms a company to manufacture and sell it. The device is an immediate success within the banking industry. It is used to secretly verify the identification of customers at tellers' windows. The scientists and engineers, however, disavow any responsibility for such uses of the device without customer notification or consent. They contend that the companies that buy the product are responsible for its use. They also refuse to be involved in notifying public representatives about the product's availability and the way it is being used.

Does employing the device without customer awareness violate the right to privacy or to informed consent? Do the engineers and scientists perhaps have a moral obligation to market the product with suggested guidelines for its ethical use? Should they be involved in public discussions about permissible ways of using it?[21] (Retina scan identification systems using laser beams are already in use. An example would be to determine if a person using a particular computer is authorized to use it.)

[20] Ibid., 109–11.

[21] Ibid., 126–28.

6. The following warning to parents whose children use home computers was carried by the Associated Press: "In recent years more sexually oriented materials have been showing up for home computers—some on floppy disks with X-rated artwork and games, and other accessed by phone lines from electronic bulletin boards . . . with names like Cucumber, . . . Orgy, Nude pics, Porno, Xpics, and Slave."[22]

Discuss the ethical issues raised by pornography in this new medium, as well as the issues raised by racist, sexist, and libelous (false and defamatory) statements. How can access be denied to children? Should there be controls for adults? Already there are thousands of bulletin boards, largely because it is so easy and inexpensive to create them. Should bulletin board operators be held liable for failing to filter illegal forms of verbal assaults, even if that forces them to buy liability insurance and thereby raise the costs of creating bulletin boards?

7. Write a short research paper exploring the threats to privacy posed by data banks. In your essay, comment on some specific advantages and disadvantages of having one centralized national data bank that pools all available government information on citizens.

[22] Associated Press, *Los Angeles Times,* December 25, 1987, part 1, 47.