

Chapter 13: Educational Computing and Society

Chapter Thirteen
Computers, Education, and Society

It is useless to bemoan the departure of the good old days of children's modesty, reverence, and implicit obedience, if we expect merely by bemoaning and by exhortation to bring them back. It is radical conditions which have changed, and only an equally radical change in education suffices.

John Dewey (1859-1952)

Science cannot stop while ethics catches up.

Elvin Stackman

Some are born good, some make good, some are caught with the goods.

Thomas Jefferson (1743-1826)

For every man there exists a bait which he cannot resist swallowing.

Friedrich Wilhelm Nietzsche (1844-1900)

A teacher who can arouse a feeling for one single good action, ... accomplishes more than he who fills our memory with row on row of natural objects, classified with name and form.

Johann Wolfgang von Goethe (1749-1832)

LEARNING OUTCOMES

The children in our classrooms have been raised in a world where computers and computer-based technologies have changed the landscape of daily life. What does this technology-enabled reality mean for our students? What is their mindset? How does this affect their day-to-day lives? That is what this chapter is all about.

Our examination of the sociological impact of computers begins with a broad sweep across the canvas of our world. We will consider the computer as a tool that supports research, enables discovery, stimulates invention, fosters environmental and organizational control, and facilitates communication between individuals and groups, which in turn fosters understanding, cooperation, and accord. We will next concentrate on the increasingly central importance of education as the key to the survival of the individual in a modern, computer-controlled, information-based society when what you know is at least as important as what you can do.

Lest we have too rosy-eyed a view of the computer's impact on our world, we also will examine the dark side of the rapid proliferation of computer-based technologies. Privacy is threatened—some would say it is dead and gone. Inequities are becoming more, rather than less, pronounced. New kinds of crime have emerged, such as software piracy and illegal computer hacking.

Chapter 13: Educational Computing and Society

Teachers and students need to be aware of these negative aspects of computerization so that they will be less likely to become victims of the negative outcomes of a computerized society. The knowledge that comes with this awareness empowers the individual, and that is what learning is all about.

Here then are the topics that will be discussed in chapter 13.

- Computers are Transforming Our World
 - Extending the Capabilities of the Mind
 - Extending the Capabilities of the Body
- Education and the Information Society
 - Information Overload
 - Information and Wealth
- The Place of Computer-Based Learning in Schools
- Ethical and Legal Issues and Computers
 - Privacy invasion
 - Computing Inequities: Haves and Have-nots
- Software piracy
 - The scope of the piracy problem
 - Types of software piracy
 - Copyright law and What You Can Do
 - Other reasons to avoid piracy
- Free and not-free software—Software licensing
 - Public Domain and Software
 - Open Source Software
 - Freeware
 - Shareware
 - Licensed Commercial Software
 - Software protection
- Steps Schools Should Take to Discourage Software Piracy
- Security: Hacking and Cracking
 - Computer viruses and other malware
 - Malware: Worms and Trojan Horses
 - Spyware and Spam
 - Trespass of Computer Systems
 - Money theft (Embezzlement)
- Steps Schools Should Take to Secure Networks and Computers

Chapter 13: Educational Computing and Society

COMPUTERS ARE TRANSFORMING OUR WORLD

Not all computerization is for the better. Weizenbaum (1976) reminds us of the words of John Dewey, who wrote: "Every thinker puts some portion of an apparently stable world in peril and no one can predict what will emerge in its place." The invention of the computer has indeed changed the world. According to Weizenbaum, the very existence of the computer makes it possible to manage more data than ever before. This has resulted in our *collecting* more data than ever before.

While this is a boon to researchers, it also affects the way we solve problems. As Weizenbaum points out, "the computer did arrive 'just in time.' But in time for what? In time to save—and save very nearly intact, indeed to entrench and stabilize—social and political structures that otherwise might have been radically renovated or allowed to totter under the demands that were sure to be made on them." The computer has "buttressed" and "immunized" social and political structures "against enormous pressures for change." Weizenbaum goes on to question the use of the term *Computer Revolution*, arguing that computers have done more to *prevent* change than bring it about.

Beniger (1986), however, makes clear that increased levels of control promote progress in any field of endeavor. The computer, by giving us greater control over systems such as transportation, communications, banking, science, and industry, directly affects the rate of discovery, invention, and progress. Artists and artisans from all walks of life—including teaching—recognize the potential of the computer to extend human capabilities in the realms of creativity and problem-solving. The computer thus seems likely to have a beneficial impact on our world. Let us begin then by briefly examining some of these beneficial social impacts.

Extending the Capabilities of the Mind

Alan Turing, an English philosopher and mathematician, published a paper in 1937 which anticipated the invention of the modern electronic digital computing machine. Turing described a theoretical, logical machine (Turing, 1937), now known as the Turing machine, which would be capable of processing any *computable* function.

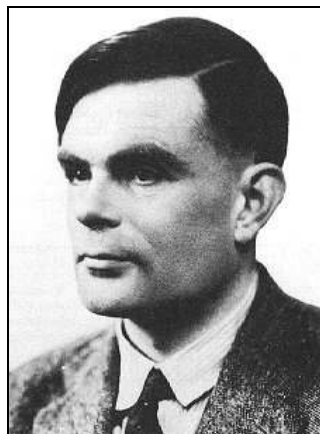


Fig. 13.1 Alan Turing, Mathematician and Cryptographer, 1912-1954

Chapter 13: Educational Computing and Society

Kurt Gödel (1931) had already shown that there was a class of problems in mathematics that were simply unprovable. But what Turing established for the record was that, given time, we could build a machine that could come up with the solution to any *computable* problem we set our minds to! So he called his theoretical machine "The Universal Machine."



Fig. 13.2 Kurt Gödel, Mathematician and Logician, 1906-1978

Turing might be called the Father of Artificial Intelligence (AI) because of his early recognition of the electronic computer's extraordinary potential as a 'thinking machine.' He liked to compare the computer to the human brain. As Hodges (1982) notes, Turing had always been interested in physiology. Certainly, he showed a thoroughly modern understanding of neurophysiology when, in 1930, he observed: "We have a will which is able to determine the actions of the atoms probably in a small portion of the brain... The rest of the body acts so as to amplify this."

The brain proposes, the body disposes. By analogy the computer, like the brain, can be programmed to control an endless series of machines and environments which would otherwise need the presence of a thinking human being. These would include social or community environments such as transportation, all areas of science (including health and welfare), communications (including entertainment), agriculture, accounting and other processes in business and industry, and so forth.

More and more tasks previously carried out by intelligent human beings are now being given over to suitably programmed computers. The computer is just a dumb machine which, once programmed, is able to work tirelessly, processing data of all kinds at high speed and at little cost. It is also much less error-prone than the human data processor. This is why folks such as Gottfried Wilhelm von Leibnitz and Charles Babbage racked their brains to devise automatic calculators: human computers just make too many mistakes!

Ironically, the electronic digital computer mindlessly performs operations that enhance our ability to think. Human thought is predicated on knowledge, which is the outcome of acquired and assimilated information, which itself is made possible by symbol systems (data expressed in the lexicon of a language). We think using the tools of the language(s) we have learned. Where computers today come in handy is by allowing us fast, easy access to the information that we need to think about things—anything!

Chapter 13: Educational Computing and Society

Teachers thus have a golden opportunity today to improve the educational experience for their students by creating an environment in which children can take advantage of computer-based technology to extend their ability to think and learn.

Research has shown that writing is a pre-eminent learning tool. The very act of writing—of organizing thoughts into a coherent form—is an important step towards understanding, which is itself as fundamental building block of learning.

Research also has shown that children's writing skills are considerably enhanced when they use the computer as a writing tool. This is partly because they are liberated from the constraint of having to form letters by hand, but it is also because they are able to capture their thoughts and, above all, revise their thoughts much more easily using a word processor than with pen and paper.

Thus the computer promotes learning by promoting writing. It also promotes learning by taking much of the drudgery out of processing data.

Put the computer in the hands of trained (educated) individuals and those individuals can “think” with their fingertips, processing and analyzing huge databases of information on the way to drawing conclusions about our world—in science, technology, business, government, philosophy, the arts—which advance our understanding and increase our ability to control our environment.

As we shall see later in this chapter, this increasing level of control is not necessarily a good thing. The computer helps us think; unfortunately, it can't help us act morally or ethically. That is something we still have to do on our own.

Extending the Capabilities of the Body

Even animals use tools to help them accomplish physical tasks. Computers are no different from other tools in this respect, except that they have a lot more flexibility and versatility as Universal Machines.

Robotics Scientists routinely are able to pick up and examine rocks on the surface of distant planets. Back on earth they slip their hands into “gloves” that are connected by radio signals to the “hands” or, more accurately, claws of robots that have been sent to those planets to do the scientists’ exploring for them. The robots have cameras fore and aft to transmit pictures of the objects they sample, and the scientists manipulate them remotely as if they were there on the planet inside the shell of the robot. The robot responds precisely and delicately, controlled from hundreds of thousands, maybe even millions, of miles away.

The picking and placing of rocks is analog; the data processing, including the control of the robot and the imaging, is entirely digital—just as Alan Turing in 1937 figured it could be done.

Other remotely operated vehicles (ROVs) are used to study the ocean depths, or to investigate unexploded bombs, or to check out areas that may have been contaminated as a result of toxic emissions. In general, ROVs allow us to go where it would be either very difficult or very dangerous for us to go in person.

Robots rule.

Chapter 13: Educational Computing and Society

Robots, in the form of robotized cameras, rule the roads in the United Kingdom. If you go there for a visit, watch your back because they will probably be watching you. This is very convenient for the government since the cameras control computers that automatically mail offending drivers and thus generate a great deal of revenue from tickets for speeding fines. The cameras also keep an eye on things in the neighborhood without the police officers hardly needing to lift a finger!

Help for the disabled In the United States there are over 50 million people with some kind of physical disability—that's almost 1 in 5 of the population. Today we can say that if a person can control the movement of any part of his or her body—the raising of an eyebrow, the blink of an eye, the flick of a finger, the twitch of a toe—a computerized device can be designed to use that movement to allow a disabled person to function independently in the mainstream of society.

The growing industry for computerized devices to assist this segment of the population has already produced inventions that give one reason to hope that the term *handicapped* will eventually all but disappear from our vocabulary. Consider what has already been achieved.

Consider the quadriplegic, paralyzed from the neck down, who has a voice-controlled robot programmed to be his companion, preparing his meals, feeding him, fetching and carrying for him, and so forth (NOVA, 1985). Consider the paraplegic, paralyzed from the waist down, and now able to walk because of mind-directed, computer-controlled functional electrical stimulation of the leg muscles (NOVA, 1985). This is old news.

Consider the blind person able to see faint images for the first time in his life because of a computer-based system that literally plugs into his visual cortex at the back of his brain and transmits to the visual cortex pictures captured by a video camera, bypassing the eyes altogether.

Computers also produce some surprising and moving "high tech, high touch" outcomes. Dr. Rena Upitis at the Hennigan school in Boston, Massachusetts relates the story of "one little girl—classified as non-verbal because she had never spoken in school—[who] spoke for the first time at the computer, asking her teacher to come and see her work" (Spence, 1987). In another example, an autistic child was able to be mainstreamed because of the computer's capability as a voice synthesizer. "In time," the child said with the computer's help, "I will utter the truth of my plight. I will remember the people who helped me. I cannot do this without help."¹ Without the computer the child would probably have been trapped forever inside his disability.

"The blind see and the lame walk..." The more aware we become of the many extraordinary computer-based applications that are being designed by inventors and researchers all over the world, the more we can appreciate the relevance of the term *computer revolution* as an apt description of the transformation that is taking place in every corner of our world.

In schools, computers are making possible the elusive dream of individualized education even as they facilitate collaborative learning and inter-cultural communication. As Melmed (1988)

¹ From a TV documentary on autism.

Chapter 13: Educational Computing and Society

observed: "The application of science and technology, which has had such a powerful effect in other social and economic sectors, can be the basis of a new instructional model with much improved learner productivity."

EDUCATION AND THE INFORMATION SOCIETY

Information Overload

Revolutions create chaos as readily as they bring about change. A significant accompaniment of the computer revolution has been an information explosion that threatens to overwhelm the decision maker at every turn. While too little data, like too little knowledge, is a dangerous thing, so too is too MUCH data, otherwise known as information overload.

This problem is not new. Francis Bacon (1561-1626), the English essayist, philosopher and statesman, was perhaps one of the last people to have had the temerity to say: "I have taken all knowledge to be my province." A century later, Voltaire (1694-1778), the French writer and philosopher, was forced to admit that "the multitude of books is making us ignorant."

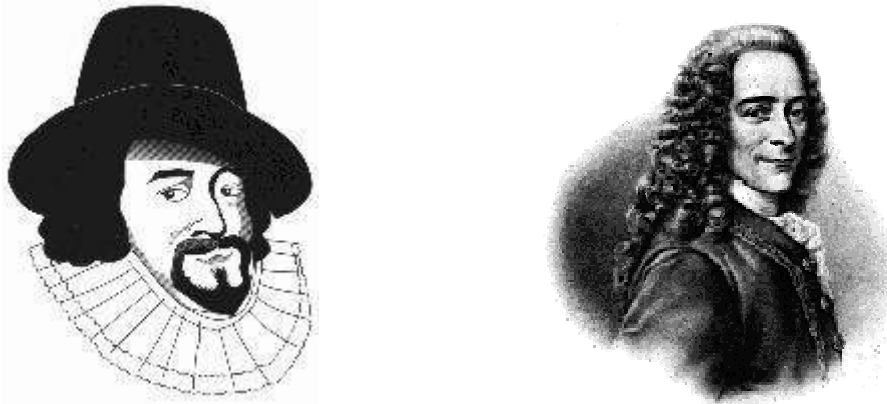


Fig. 13.3 Francis Bacon, 1561-1626 and François Marie Arouet (penname Voltaire) 1694-1778
Information overload was definitely a problem in the 17th and 18th centuries, and it is getting worse rather than better, even *with* the data-processing capabilities of the computer.

This is because the computer can only process data—the raw material of information; you need the human brain to process information. Figure 13.4 illustrates the Knowledge Spectrum (Debons, 1988), which we discussed in some detail in Chapter 8. Notice the two segments of the spectrum—the Data Driven and the Cognitive Driven segments. The computer helps us more efficiently handle data processing in the Data Driven segment. Beyond that, it's up to us to use our mind to make sense of what the computer presents to us. Only then does it have the potential to become information.

Chapter 13: Educational Computing and Society

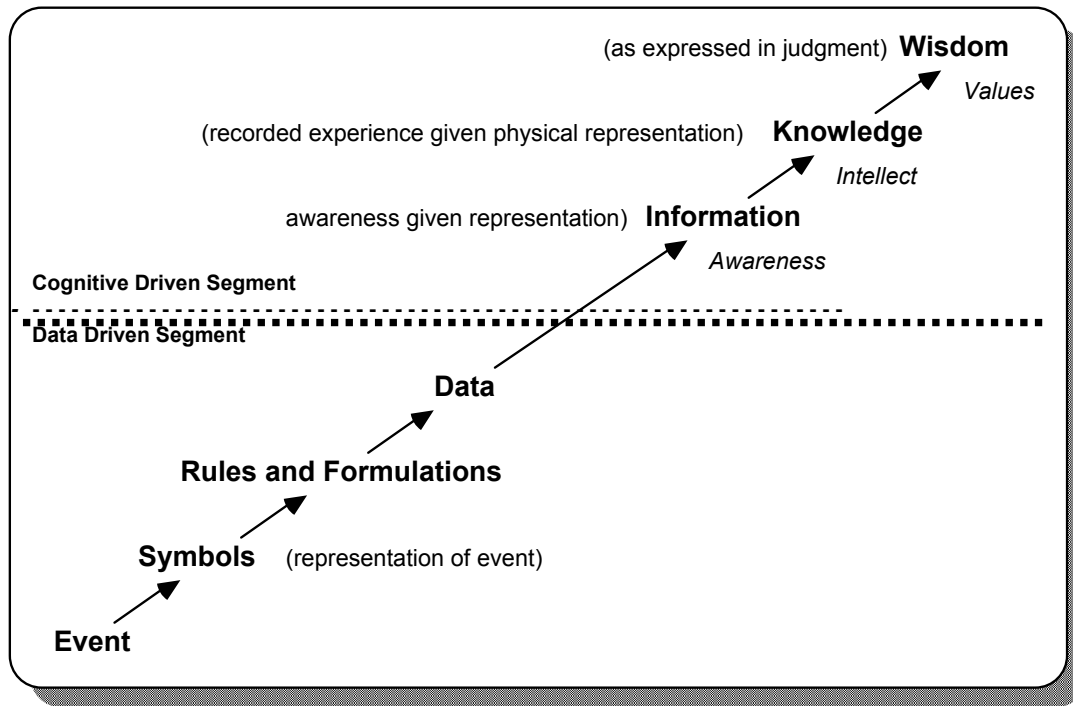


Fig. 8.1 The Knowledge Spectrum (Debons, 1988)

Information overload is brought about by advances in technology. In this sense, technology is driven by its own success, like a dog chasing its own tail. Computer hardware and software engineers are increasingly challenged to develop and refine the highly complex systems of control that will allow us to maintain political, economic, and social equilibrium in these technologically turbulent times.

Information and Wealth

In a pre-industrial society, the source of wealth was land. Then, in the 18th century the Industrial Revolution caused a shift to capital as a primary source of wealth. Today, information is a major source of wealth. Data is the raw material of information, and processing it effectively is what makes one company more competitive than another.

An increasingly large percentage of the workforce in an increasingly large percentage of companies earns a living from transmitting, receiving, and processing information. Since 1890, the numbers of those employed in agriculture in the United States has fallen from 95% of the population to no more than 1% today. Since 1950, the number of those employed in blue collar labor (construction, production, transportation, and so forth) has fallen from 62% to what is projected to be less than 23% by 2012. By 2012, it also is projected that close to 80% of the workforce will be processing data in information-intensive or service-oriented jobs (US Bureau of Labor Statistics, 2004).

This has significant implications for education. As Ogilvy (1993) observes, "What the farm was to the agricultural era, and the factory to the industrial era, educational institutions will be to the information era."

Chapter 13: Educational Computing and Society

The Place of Computer-Based Learning in Schools

In light of this new reality, education is essential for *all* citizens so that they can contribute effectively and benefit from the wealth that the society produces. Two questions arise:

- To what extent can computers be used to improve the process whereby an individual acquires an education?
- What role will teachers play in "schools" where much of the learning is computer-based?

The myriad computer-based learning applications developed for K-12 education can help you as a teacher by releasing you from the primary burden of responsibility for knowledge transfer. Learning, after all, is ultimately the responsibility of the individual student. You, the teacher, through the thoughtful integration of student-centered methodologies and computer-based technology, can become the facilitator of knowledge acquisition—a knowledge broker, if you will. Your role is to create and sustain an environment in which children can seek, find, and assimilate data, thus becoming informed through the acquisition of knowledge.

The teachers of the future will need intellectual skills of a different kind from teachers of the past. Teachers will still need to know math, history, geography, chemistry, and so forth, but this kind of knowledge will be less important than knowing:

- how to manage a learning environment;
- how to select and set up appropriate individualized learning experiences for children based on their age, propensities, capabilities, and interests;
- how to motivate children;
- how to recognize and work with the subtlest of learning disabilities;
- how to create positive and productive interaction between the child, the school, and the home.

Researchers (Van Dam, 1991), monitoring a classroom where computer-based technology was integrated intensively into the curriculum, noticed that the teacher seemed to have very little to do. The children were working alone or in groups; some with and some without computers. There was a quiet hum of activity; everyone was involved in the learning process. The teacher was attentive to everything that was going on, moving easily from one group to another, sometimes in response to a verbal or non-verbal call for help, other times to more precisely feel the pulse of the learning process as it occurred.

One of the researchers asked one of the 9 year olds: "What does the teacher do?"

"He's very important...", one of the youngsters replied.

The researcher was not satisfied with the response. What did the youngster mean? So the question was put again. "Yes, but what does the teacher *do*?"

"Well, he's there in case we need him," said the boy, after a moment's pause.

"He's very important... He's there in case we need him..." What a beautiful description of the role of the teacher in the student-centered, student-directed learning environment. The teacher does

Chapter 13: Educational Computing and Society

not direct the entire learning experience. Rather, the teacher sets up and maintains an environment that fosters learning for the student participants. The teacher does not pass on all the knowledge. Rather, the teacher ensures optimal conditions for knowledge acquisition. The teacher is not an officer in a regimented educational system. Rather, the teacher is a "knowledge broker," acting as an intermediary between students and the data that they seek to fulfill their *individual* information needs.

Children need teachers more than ever in a world where information overload creates confusion in immature minds. But they need teachers less and less as imparters of knowledge, and more and more as imparters of wisdom.

"He's very important... He's there in case we need him..." There is an increasing number of classrooms worldwide where this concept of the teacher as facilitator of learning is a reality, and in many of those classrooms the computer is becoming an invaluable, if not essential, learning tool.

ETHICAL AND LEGAL ISSUES AND COMPUTERS

Many societies today are faced with serious problems regarding the upbringing of their children. This is especially true in the so called developed world where half of all marriages fail and where, even when the marriages last, both parents feel constrained to work to make enough money to have a decent standard of living¹. With the best will in the world, parents in such families have difficulty giving their children the care they have every right to expect from the dependable and attentive presence of a nurturing adult. Many children are "latch key kids," coming home to an empty house and left to fend for themselves for several hours until a parent comes home. Other children come home to a house where the parents have little energy left to respond to their need for attention.

Too often, the children *are* finding at home all the wrong kinds of role models pacifying them hour after hour over largely unsupervised, dubiously educational, TV channels and, much more dangerous, largely unsupervised internet access. As Postman (1986) observed, "We are now a culture whose information, ideas, and epistemology are given form by television, not by the printed word." Shanker (1992) further reminds us that "Studies and statistics—and our own observations—tell us that American families are increasingly fragile and unstable, and we fear that, as a result, many children are being seriously damaged." In a culture where the immediate family appears to have less and less control over a child's upbringing, children need all the help they can get.

In some countries, such as in the kibbutzim (collective farms) in Israel, children are put in the almost total care of specially appointed nurses and educators from a very early age. Today, however, this responsibility is more important than ever. Societies such as those described above are relying more and more on professionally-managed institutions such as schools to act *in loco parentis*. Acting *in loco parentis*—*in the place of parents*—is nothing new for teachers because

¹ The percentage of households where both spouses work full time is increasing year by year to where it is now nearly triple what it was in 1969 (Source: Bureau of Labor Statistics, *Currently Population Survey*, 1999).

Chapter 13: Educational Computing and Society

children have always spent a large proportion of their waking day in school. What, then, are some of the contemporary legal and ethics issues that teachers should discuss with students?

Privacy Invasion

"Privacy," observes Rothfeder (1992), "is an issue charged with emotion. Nothing makes Americans angrier than the suspicion that somebody is looking over their shoulders or peering into their private affairs. And people often describe privacy deprivation with the same words used by rape victims: We say we feel violated, vulnerable and ineffectual." However, Johnson (1985, 1) reminds us that "much to the surprise of many Americans there is no explicit constitutional guarantee to privacy."

But it is a right; we do have a right to privacy. As Philip Zimmerman, the author of PGP (Pretty Good Privacy) points out: "Privacy is a right like any other. You have to exercise it or risk losing it." PGP is software designed to help protect your privacy. It is used to encrypt and decrypt digital documents such as email or other files stored on your computer. The authors of this book have made available a tutorial to teach you how to download a free copy of the software from the web and how to use it. The tutorial can be found at <http://www.pitt.edu/~poole/PGPintro.htm>.

All over the world, the institutions established by government for the maintenance of law and order, along with most major and many minor corporations and private investigative agencies, use technology to an ever-increasing extent to spy on people. Surprisingly enough, most of the spying is legal, either sanctioned by law or at least not proscribed by it—which does not necessarily make it right. On the other hand, some of the spying is illegal, but because we do not know it is going on we do not become concerned.

Is ignorance bliss, in this case? Do our students need to be sensitized to the reality of privacy invasion? Is there any harm in it anyway, especially if one is behaving oneself? And in any case, is there anything we can do about it?

When it comes down to it, as Rothfeder (1992) points out, "It's an information free-for-all, and even people with little computer expertise can get [most any data they want]." The problem is that in many instances we are content to have our privacy invaded. Hospitals need to keep a record of our medical history so they can more efficiently take care of us when we need treatment. Banks need to keep a record of our accounts so they can help us manage our hard-earned money.

Ultimately you can best control invasion of your privacy by being sensitive to the fact that it does go on more than you think. That awareness alone will give you a healthy skepticism whenever you are in the situation where you are asked to divulge personal data. As teachers we should also help our students to become sensitive to this negative side to the otherwise predominantly positive social change brought on by computer technology.

The United States Government as long ago as 1966 passed the *Freedom of Information Act* which, in tandem with the 1974 *Privacy Act*, ensured controlled public access to any database maintained by the federal government. To be more specific, the *Freedom of Information Act* opened up governmental databases to public scrutiny while the *Privacy Act* limited access by

Chapter 13: Educational Computing and Society

making it dependent on the permission of the individual whose records were to be made available.

Meanwhile the *Fair Credit Reporting Act* was passed in 1971 to protect people's rights of access to data gathered by the financial credit reporting industry. The *Family Educational Right and Privacy Act* of 1974 guaranteed public access to student reports in the files of federally-funded educational institutions. The *Right To Financial Privacy Act* of 1978 prohibited federal government access to banking records without either the permission of individuals who are the subject of the search or a search warrant. Other similar legislation has been passed, and there will be more to follow as situations arise in which individual freedoms are violated in more and more creative, and no doubt computerized, ways. Ethics continues to plod along in pursuit of science.

Computing Inequities: Haves and Have Nots

Rich versus Poor "For computer-based knowledge to become an extension of a human mind, that mind must at least have access to the technology. The poor will not immediately have such access, placing them at a ... disadvantage" (Madron, 1985). Pillar (1992) describes "the creation of the technological underclass in America's public schools." "In 1984," he notes, "white children used computers in elementary and secondary schools at about twice the rate of African Americans and Hispanics. By 1989," Pillar writes, "according to the U.S. Bureau of Census, nearly the same percentages of those three groups [White, African American, and Hispanic] used computers in high schools. Elementary schools also made dramatic progress. And disparities between rich and poor and between public and private schools seemed to narrow just as sharply."

But Pillar was skeptical of the relevance of the United States Bureau of Census statistics and decided to see for himself what was going on in the schools. His findings were somewhat discouraging. "I visited inner-city, rural, and suburban schools in various parts of the country," he wrote, "and after discussions with scores of teachers, students, and school administrators, an inescapable conclusion emerged: Computer-based education in poor schools is in deep trouble. Not only did these schools lack the funds and skills to finance the maintenance of their computer hardware. They also lacked the training to make the best use of the machines. "In most cases," Pillar concluded, "computers simply perpetuate a two-tier system of education for rich and poor."

Right now there are pockets of privilege, so to speak, among the poorer school districts where forward-looking parents, administrators, and teachers, sometimes sponsored by local business and/or by one or other of the major personal computer manufacturers, have taken on the challenge of providing the best possible educational opportunity for the children. The key ingredient of success has usually been the driving force of significant individuals who have galvanized the community and done what is necessary, through grants and donations, to make computer-integrated teaching a reality in their schools.

Unfortunately, however, there are still many school districts, even in the United States, where a half-hearted acceptance of the value of suitably integrated educational technology, tempered to some extent by economic realities, have resulted in children being denied the opportunity to share in the benefits enjoyed by the privileged few. There is hardly a school in America today

Chapter 13: Educational Computing and Society

that does not have computers for student use; every year the ratio of students to computers improves in the students' favor. Yet, as Pillar (1992) observed, many of the machines in the poorer schools are used "so rigidly and ineptly as to repel students."

Girls versus Boys Women continue to suffer from stereotyping which casts them in the mold of the technologically inept. The problem pervades our social institutions, starting with the home and continuing in school. Sanders (1987) observed that "girls and boys use the computer equally when they are *required* to in class, but as soon as they're allowed a choice—such as after school or in elective computer courses—girls see that boys take advantage of the opportunity far more often than girls do. This reinforces the notion that computers are a male thing."

This belies the evidence from extensive research which strongly suggests that girls are at least equal to boys in tasks that involve communication skills and skills related to math and problem-solving. The problem is one of opportunity.

Dorothy Ellen Wilcox (1996), in her Masters Thesis at the University of Alaska titled "Computers and the Internet: Listening to Girls' Voices," presented her findings that girls do need help in overcoming the cultural stereotype that causes them to be less inclined towards technology-based careers than boys. The full report may be found at <http://www.northstar.k12.ak.us/home/dwilcox/thesis/contents.html#contents>. In her conclusion, Ms Cox had this to say:

"Instead of socializing girls toward passivity and docility, non-hierarchical technology like e-mail and the Internet has the capability to assist communication and provoke development of the ability to critique the status quo among adolescents. Education is not apolitical; the curriculum masks prevailing politics and power as natural and results in their maintenance. Freer access to materials that reveal the inequities of power relationships and allow adolescents to unmask and unpack gender and racial issues will encourage debate and nourish the formulation of students' critical cognitive skills. I see educational technology as a vehicle that can initiate and nurture such dialogue, and in doing so, set the stage for inevitable change. In the faceless culture of computer-mediated communication, skilled young people will be able to pass as adults and elucidate their own concerns. Girls who are educated to an activist stance will feel comfortable participating in the networked communications web. After that, they will not need adults to interpret their words; electronic mail and the internet will become the means they can use to speak for themselves."

Cynthia Lanus, Executive Director of the Center for Excellence and Equity in Education at Rice University, quotes a report of the National Science Foundation which found that "Degrees awarded in computer science decreased among both men and women from 1985 to 1995, and **women** went from earning **36%** of those degrees in 1985 to only **28%** in 1995." "The problem's repercussions are staggering," she goes on to report. "The [Bureau of Labor Statistics](#) lists computer scientists, computer engineers, and systems analysts as the top three occupations with the fastest employment growth, 1996-2006. Teachers working with high-school students using technology observe that, in general, girls don't seem to be as intrigued by computers as

Chapter 13: Educational Computing and Society

boys are.” The full GirlTECH report: “*Getting Girls Interested in Computers*” can be read online at <http://math.rice.edu/~lanius/club/girls.html>.

The following are examples of the kinds of strategies that can help to overcome the stereotypes that perpetuate the computer gender gap (Table 13.1). Appendix E includes a full discussion of Jo Sanders’ Principles of Computer Equity.

PRINCIPLES OF COMPUTER EQUITY

Focus specifically on girls.
Target girls in groups.
Design activities around girls' existing interests.
Stress the usefulness of computers.
Eliminate biased computer practices.
Pay attention to your software.
Let others know.
Do it again next year.

Table 13.1 The Principles of Computer Equity
Courtesy Jo Sanders

Whites versus Minorities It seems absurd to have to point out that the color of one's skin makes no difference whatsoever with regard to one's level of intelligence. This author's experience teaching in schools K-12 in Europe, Africa, the Middle East, and North America has taught him that the range of intelligence among these diverse cultural and ethnic groups is the same. Those who believe otherwise should be helped to recognize one simple fact: that they are guilty of inexcusable prejudice born of unfortunate cultural bias.

Such bias continues to plague our social structures in general, and our educational institutions in particular. African Americans and Hispanics are not expected, and often do not expect themselves, to achieve success in technology fields such as those associated with computers. Much of the problem is that children in these ethnic groups are more likely to come from families living below the poverty line, which translates into a lower likelihood that these children will either attend schools in the wealthier, more technology-rich districts, attend school on a regular basis, or graduate from high school.

The Lack of Equal Access to Information Since knowledge is power, and since not all children have equal access to information because of disparities in the funding and management of different school systems, then it stands to reason that many children are at a serious disadvantage. They are on the wrong side of the Digital Divide.

Chapter 13: Educational Computing and Society

Some students are fortunate to attend schools where they have access to libraries of electronic data in the form of interactive text and video¹, with quality educational software to complement other forms of instruction, and with open lines of communication between themselves and students in other schools at home and abroad. These fortunate students are also more likely to have their own computer at home, with on-line, multimedia encyclopedias and access to the world wide web. Such privileged students will be more likely to receive a more rounded and comprehensive educational experience than students attending less technologically-endowed schools.

SOFTWARE PIRACY—THEFT OF PROGRAMS

Everyone is directly or indirectly vulnerable to becoming a victim of computer crime. Many of us will also be tempted at one time or another to perpetrate the crime of stealing software. A very small minority of our students, especially those that are more technically-oriented, may well find themselves involved in activities associated with hacking or, still worse, "cracking"--a once popular name for criminal hacking. The likelihood of our students being involved in unauthorized infiltration of computer systems or in electronic theft of money² is remote. Nonetheless, it will be useful to know what is involved in each of these types of computer crime. It is also important that our students discuss these issues, so that on the one hand they can be helped to make good ethical judgments about what is right and wrong in these matters, and, on the other hand, to help them avoid becoming victims of computer crime.

Needless to say, you, the teacher, will need to decide what would be an appropriate time to bring up these issues with students. A useful brainstorming session (see the Do Something About It section at the end of the chapter) would be to join with a group of colleagues or classmates to come up with ideas as to just when and how such a discussion might take place with students.

The remainder of this section will look briefly at two types of computer crime--software piracy and violation of intellectual rights--which are most likely to involve us as teachers in schools where policies are not well laid down and applied. Then in the following section we will deal with the unethical activities that come under the umbrella of hacking.

The Scope of the Piracy Problem

You may not be aware of it, but it is quite possible that you are running pirated software³ on the computers you use at school or at home. Your students may well be doing the same. On the other hand, you may be very well aware of the existence of pirated software and know that it is strictly speaking stolen property. Yet your sense of guilt is not strong enough to cause you to erase the unauthorized version from the computer system(s) you and your students use. Do not feel bad.

¹ In chapter 8 we discussed online data base retrieval services such as DIALOG Information Services' CLASSMATE™ instruction program.

² The current rage of "identity theft" is a form of computer theft.

³ In previous sections, the piracy of copyrighted media, especially music and video recordings, has been discussed. This is perhaps an even more pervasive problem. The solutions and dangers discussed in this chapter apply equally to illegally downloaded or shared .mp3 and video files.

Chapter 13: Educational Computing and Society

Suits have been won against more than one large school district and many large businesses involving the theft of copyrighted software.

The Business Software Alliance has reported that in 2001 alone the software industry in the United States lost \$5.6 billion and in excess of 110,800 jobs to piracy (BSA 2002). The good news is that the losses for 2001 represented a decrease of 10% from what they were in 2000, thanks in no small measure to the efforts of watchdog groups such as the BSA and the SAI (Software and Information Industry Association, SPA Anti-Piracy Division). North American had, in fact, the lowest rate of software piracy, the highest being in Eastern Europe. Globally, almost \$11 billion dollars was lost due to piracy (BSA 2001).

Why is there so much blatant copying of software? Is it because computer software is intangible and therefore not *real*? Is it because it is so easy to get away with, and so we do not worry about getting caught? Is it because it is so easy to copy software that it just does not seem wrong to do so? Is it because we think of software like a book which we borrow from a library--intellectual property of which we feel we have unlimited use? Is it because we know that there is a lot of software that is free and so we question why we should have to pay for any of it? Or is it because we are not fully aware of the law? As Ken Wasch, past executive director of the SPA observed: "It's ironic that people who would never think about stealing a candy bar from a drugstore seem to have no qualms about copying a \$500 software package" (Lewis, 1992).

Let us take a look at the specifics of software piracy, copyright, and licensing, so that you can better understand the law.

Types of Software Piracy

The Business Software Alliance (BSA 2000-2004) identifies five distinct categories of software piracy. They can be applied to schools in this way:

- End-user piracy—This happens when one employee or the school
 - makes multiple copies without authorization or legally obtained license,
 - installs the software on more computers than the license allows,
 - duplicates OEM (Original Equipment Manufacturer) software that came with computers for installation on other machines or uses master system disks for this purpose,
 - takes advantage of an upgrade offer without having purchased equivalent licensing for the previous version,
 - installs an application licensed for educational use on a computer not used for education (e.g. a friend's computer, a tutor's computer),
 - shares or swaps software with other teachers, other schools or other individuals,
- Client-server piracy—This happens when the school installs an application on a network software server and allows it to be used by more simultaneous users than the license allows.

Chapter 13: Educational Computing and Society

- Internet piracy—This is downloading counterfeit or illegally copied software from the Internet to bypass the legal purchase process¹. This includes peer-to-peer software sharing, which large and inexpensive hard drives and high speed networks have made feasible.
- Hard disk loading—Resellers and other computer distributors can install, or "bundle," unlicensed software on computers sold to schools to make the purchase more attractive. Similarly, laptops and desktops can be recycled by schools without removing the software and transferring the license. This is illegal if the same software is then reloaded on the replacement machines.
- Software counterfeiting—Illegal copying and selling of software in imitation of the genuine product is one of the most wide-spread forms of piracy, especially with regard to large commercial applications such as the Microsoft *Office* suite.

It is easy to see how software piracy can be unintentional. However, ignorance of the piracy is no legal excuse—schools and teachers that break the law by doing any of the above acts can be, and are, prosecuted by the software industry and software producers.

It is also easy to see how software piracy can be appealing. Many applications, such as specialized paint and design software, cost a great deal and are used minimally by their purchasers. Other software, such as games, have a limited "life" in terms of the interest of their purchasers. Why not recycle them?

The answer is: because of licensing and copyright law. When you purchase a piece of software, you do NOT purchase the copyright to the software; you do not OWN it. What you purchase is a *license* to use the software in a legally specified way. This license is a document, either on paper or in a digital file (you should print it), that spells out the rights you have in terms of legal use of the software.

Violation of this license constitutes piracy. Moreover, your software is protected by U.S. Copyright Law (assuming it was produced by a U.S. company)². It is the owner of the copyright who "makes the rules" that are set forward in the license.

Copyright Law and What You Can Do

Software is copyrighted the minute it is published. This copyright is generally held by the producer of the software if it is *proprietary*³, and by the author or commercial venture responsible for the development if it is not proprietary. The extent to which the producer or creator of the software wants copyright law to NOT apply, if at all, is spelled out in the license. Unless

¹ Much software is now sold and distributed legitimately by way of Internet download. Legal sales, however, include electronic, PO, or snail mail payment before registration can be completed and licensing transferred.

² Canada and other nations have their own copyright laws and policies. According to the WIPO (World Intellectual Property Organization), software copyright is viewed and legally protected differently in various countries. Global copyright of digital material, including computer programs and software, is thus somewhat cloudy. (WIPO)

³ The Free Software Foundation defines *proprietary* as software published with full copyright protection applicable (not "free for all uses" or "semi-free for all uses"). This applies to almost all commercially available software. (FSA). Note that some software that is free (no-cost) is restricted under licensing and some software that has been commercially produced is distributed under an open ("free") license. It can be very complicated!

Chapter 13: Educational Computing and Society

specified, the buyer is allowed to use the software on one computer—period (school titles often extend this to one free copy for archiving).

We have discussed copyright and Fair Use in previous chapters as it applies to images, media elements and text that teachers and students might want to use in instructional materials. What exactly does U.S. copyright law say about software?

Federal Copyright Law explains it thus: "It is illegal to make a copy of a piece of software for any reason other than as a back-up without the permission of the copyright holder." Copyright law has the same overall objective as patent law: "to promote the progress of science and useful arts." Why, after all, should software developers waste time and money inventing products of benefit to society if someone else can, with impunity, steal their ideas and get all the profit from them? As summarized by Biegel (1998 and 2001), the "No Electronic Theft" act of 1997 and the Digital Millennium Copyright Act of 1998 make all of the above acts of software piracy illegal. There is no such thing as Fair Use with regard to software applications.

The SPA (now part of the SIIA, Software and Information Industry Association) has been the principal trade group of the PC software industry since 1984. One of its roles has been that of watch-dog for the industry, maintaining an anti-piracy hotline (1-800-388-7478) which accepts calls reporting software violations and an online report form (<http://www.siiia.net/piracy/report/default.asp>). SPA is currently offering cash rewards for corporate piracy that is verified by their Anti-Piracy team. According to their literature, the SPA investigates these reports and, if there is solid evidence that an institution (including schools) has illegally duplicated large numbers of software programs, they take one of three actions: "a cease and desist letter is sent, an audit is conducted or a lawsuit is filed." (SPA). Funding to support any ensuing litigation is provided by SIIA member companies.

BSA is a global organization dedicated to promoting "a safe and legal digital world." Like SPA, it is a watch-dog group, taking it upon itself to police software use, providing online piracy report forms (<http://www.bsa.org/usa/report/Reporting-Form.cfm>) and both U.S. (1-888-NOPIRACY) and International telephone numbers. BSA investigates software piracy that takes place outside the United States as well as inside, especially in countries where software is copied wholesale by bootleg operations and marketed at a fraction of the normal cost. An archive of press releases documenting their successful "sweeps," as well as their research into the economic affects of software piracy, can be found on the BSA website (<http://www.bsa.org/usa/press/Education-and-Enforcement-Releases.cfm>).

In addition to their watch-dog actions, both SPA and BSA¹ provide information, education, and global action to support the battle against software piracy. For teachers, parents and students, both organizations provide quality online resources for learning about all aspects of cybercrime².

¹ The US is not the only country with such organizations. Canada, for example, has CAAST (The Canadian Alliance Against Software Theft): <http://www.caast.org>.

² Play It Cybersafe from BSA (<http://www.playitcybersafe.com/>) and CyberSmart! from SPA (<http://www.siiia.net/divisions/edpiracy/piracy.asp>).

Chapter 13: Educational Computing and Society

Both groups have been proactive in their efforts to prevent software piracy. In addition to the educational materials, they provide materials and resources to help you detect pirated software, especially that which is counterfeit and that made available on a network server. BSA, for example, makes two network license tracking/auditing tools available to schools and businesses free of charge (<http://www.bsa.org/usa/antipiracy/Free-Software-Audit-Tools.cfm>).

Other Reasons to Avoid Piracy

In addition to legal risks and the ethical dimension, there are important reasons for schools to avoid pirated software. Any one of the following cautions should make schools and teachers think twice before knowingly installing or using such software:

- First, like all digital data transmitted over a network or on portable media, copied or counterfeited software has a high risk of exposure to computer viruses. Not only can these viruses corrupt the local computer, they can spread throughout the school, the district, and all other networks to which a single user connects.
- Second, copied and counterfeited software comes with no warranties. These documents, in addition to the purchase record, make it possible for the user to replace or return the software in case of damage or flaw. It is not unusual, for example, for a CD to be misboxed, scratched, water damaged or even broken. In each of these cases, a legitimately purchased software title will be swiftly replaced. In the case of pirated titles, users are stuck with "bad goods," no matter how much they paid for them
- Third, users of pirated software are not eligible for software upgrades, made available by producers when titles are improved or updated and sometimes when compatible products are made available. Such upgrades are always less expensive than "full versions" and are sometimes free. Although it may be possible for users to purchase or download upgrades, installation or activation generally requires either the "digital signature" that is stored on the computer upon official registration or a registration key.
- Fourth, pirated software generally lacks documentation. In addition to the license and warranty, this may mean a manual! Education software often comes with extensive support for implementation in the classroom, at times including a loose-leaf notebook of lesson plans and worksheets.
- Last, proper licensing of software generally makes it possible for the user, especially the user of large or sophisticated applications, to receive technical support. Users of pirated applications will have to go it alone.

For many reasons, then, caution should be the rule, even when a well-meaning colleague, student or parent presents you with the offer of a software title "just for a little while."

But what about software that is available on the Internet from reputable download sources such as Tucows (<http://www.tucows.com>) and Version Tracker (<http://www.versiontracker.com>)? Isn't it "free"? How can you tell?

Chapter 13: Educational Computing and Society

FREE AND NOT-FREE SOFTWARE—SOFTWARE LICENSING

Public domain and software

In the US, public domain for software is the same as public domain for other copyrighted creations. In real terms, considering the probable useable life of the software in terms of operating systems and hardware, this means that no copyrighted software application is or will ever be in the public domain¹. In terms of copyright questions, this also means that applications that were useful and popular 10-15 years ago, and which may still be viable on some school computers, are still under copyright law—although they can not longer be purchased, and they are no longer supported in any way (in fact, the producer may no longer exist), they are still protected by copyright, and thus by the original license agreement. Therefore, there is no such thing, in practical terms, as public domain software. How then, can software be "free"?

As one might expect in a democracy, there is an association called the Free Software Foundation which argues that it is wrong to make people pay for software. The Foundation believes that, like other intellectual property such as library books, software and its underlying program code should be available free of charge. There are several ways in which this vision has become reality.

Open Source Software

GNU (GNU's not Unix Project) offers a GNU GPL (GNU General Public License) for software developers that is as close to "free" as software comes today. The GPL is a "free published software license," giving the user freedom to copy, study and improve upon the code, and redistribute (even for a price) and adapt the software (FSA 2001). This license applies to most of the software developed by the Free Software Foundation and to software programs whose author's commit to using the GPL. Because there is no requirement in the U.S. to register a copyright, program and software authors wishing to grant a GNU GPL need only to include the freely distributed license agreement with the software (<http://www.opensource.org/licenses/gpl-license.php>). The Open Source project is global and well indexed. In fact, open source versions of major software applications, including Microsoft *Office* (called *OpenOffice*) are freely available as of the writing of this text. SourceForge (<http://sourceforge.net/>) is a repository and portal for finding open source software.

There are many other versions of the Open Source license. One found in the academic world of the U.S. is the Creative Commons License (<http://creativecommons.org/>), which grants access with some limitations to non-profit and academic institutions.

Schools seeking safe and legal open source software should look for, verify and comply with such license statements. Because it is generally developed by a team of programmers, not just by an individual, open source software is reliable. Additionally, it is generally well-supported with tutorials, FAQ, user manuals and user forums.

¹ *public domain*, in the US, means that the product is, by surpassing legally set limits, no longer subject to copyright law. For software published after 1978, this means "life plus 70 years."

Chapter 13: Educational Computing and Society

Freeware

Freeware is copyrighted software available on the Internet for download with no charge. The copyright is owned by the developer, who may be an individual or a group. Freeware generally does contain a restricting license. This license generally states that individuals who download the software agree not to alter the program itself, the source code, or to distribute a copied or adapted version for any reason. Freeware software applications can often be installed on multiple computers and even distributed, as is, for to others as long as there is no change to copyrighted content and no change in the "freeware" license. Unlike Open Source applications, then, freeware is NOT "free."

But let the user beware! Freeware is often neither supported nor warranted by the author, and it can be not as well developed and tested as software that you pay for. In other words, you may regret using it for anything other than trivial applications. Indeed, even for trivial applications such as games you may regret using it if it interferes with the operating system or with the data you have stored elsewhere on your disks. Also, you should be warned that freeware can be a vehicle for the infiltration of computer viruses onto computer systems.

On the other hand, many reliable commercial software publishers, such as Apple, Adobe and Qualcomm, make some utility applications available as freeware. These include QuickTime Player, Acrobat Reader, and the Eudora Light e-mail client. These applications are fully functional but lack many of the "extras" that are available with purchase of the "pro" version.

Shareware

Shareware is software that has been developed for sale and made available in full version, generally on the Internet, via the "shareware marketing method." This is a "try before you buy" marketing strategy. The author has the copyright for the software and always includes a license statement. Generally, when the program is run, an introductory screen describes the conditions under which the software may be used. Typically, if you like the software and intend to continue using it, you are asked to make a payment to the author of either a specified dollar amount or any sum of your choosing (presumably reflecting what you think the program is worth). Today many shareware applications will "time out" after a specified trial period; further use will require purchase and a registration key. Some shareware is made available with limited features that are "unlocked" upon registration.

Shareware is often more fully supported than freeware. Once you have made your contribution, the software is supported by the author or producer. Registered users are often entitled to free upgrades when there are new versions of the software.

It is wise to download freeware and shareware from reliable portal sites, such as Version Tracker and Tucows, that send you to the producer's site for download rather than to a server of questionable legality. In addition to helping you to locate titles, they both have a "rating system" and include user reviews (if any).

Chapter 13: Educational Computing and Society

Licensed Commercial Software

Licensed software is software which is registered for your use and which entitles you to full support from the company that sold you the product. As you have just read, freeware and shareware is often licensed and open source software comes with a license of a sort (an "open" license). Commercial, proprietary applications have the most restrictive licensing, and, because they are the corporations that tend to supply schools with major courseware and productivity tools, their rights must be understood and respected.

The license agreement defines and controls the use of the software and specifies exactly how many copies may be made. If the license is for a single user, then you are entitled to make one backup copy unless otherwise specified in the agreement. If the license is a "site license," the exact nature of the site license will have been negotiated between you and the company.¹ If the license is for a "lab-pack" you will purchase a set number of installations but only one copy (usually) of the installation disk. A "network license" will allow you to install a network version of the software on one network server; it may or may not restrict you in terms of the number of users who can use the application simultaneously.

For example, if you purchase a site license for your middle school, the contract may specify that the software may be loaded only onto computers in the building that houses the middle school. So you would not be able to use it on the high school computers next door--unless you want to receive a call from the SPA! Nor would you be able to make copies of the software for use on your computer at home.

Some companies, FileMaker and Apple for example, have started negotiating liberal site licenses which, apart from allowing purchasers to use the software solely at the site, also allow teachers and teachers' assistants to install the program on one home computer.

Licenses come in many forms. Originally mailed with the software application in "hard copy," they are now often included in digital form as a file on the application's CD. Some companies, such as Adobe and Microsoft, have moved to online licensing for organizations—your license agreement includes access to a secure password-protected website where your purchase and registration keys are stored digitally.

Lastly, it is important to note the "extent" of the license. Although by and large the license lasts for the life of the application, there is a trend now days to make licenses available for "a number of years." It is possible, for example, for a school to purchase an application and not be able to use it legally for a third year without considerable expense—because the purchase came with a 2-year license!

A software license is an agreement between you and the company supplying the software. You can often negotiate the terms of the license agreement. But once the negotiations are over you are legally bound to its conditions. It is possible to transfer a license, a practice that should be followed if computers are recycled, or accepted as gifts, with operating systems and software included.

¹ Some site licenses consider a building to be a site; others extend to a district or all buildings on the school grounds.

Chapter 13: Educational Computing and Society

Software Protection

Most of the money in the computer industry is made by the manufacturers of hardware. However, the software sells the hardware since the machinery is useless without the programs that control its operations. As pointed out earlier, the software industry loses a far larger proportion of its revenues through unauthorized copying than does the hardware industry simply because it is a lot easier to copy software than hardware. There are two ways in which the creators of software can protect their product against theft: external protection in the form of legal prescription and built-in protection using hardware and/or software safeguards.

The three kinds of legal protection are provided by Patent law, Copyright law, and Trade Secret law. Of the three, only Copyright law and Trade Secret law offer any measure of practical protection (Gemignani, 1980). It is beyond the scope of this book to go into the detail as to why Patent law is an impracticable solution to the problem of software piracy, but in general you can not patent a computer program, any more than you can patent a novel. Trade Secret law allows a company to require employees and others with whom the "secret" (such as a database program developed in-house) has been shared to sign a legally binding contract that includes a non-disclosure clause. This is a routine practice when hiring new employees or sharing technology between companies. Of course, proving in court that the secret was really a secret and applied to something not already known is a stumbling block which more often than not reduces the weight of Trade Secret law to little more than an honor system. Even Copyright law fails to adequately protect software developers, notwithstanding the successful efforts of the SPA and BSA described above.

It has always been possible to protect software against unauthorized copying. Various methods have, and still are, being used. The simplest is to build instructions into the program which will override any command from the operating system to complete a copy of files or disks pertaining to the program. One problem with this is that it is difficult to add such a "lock" to an application distributed on CD. Another problem with this that it is not difficult to create a program which gets around the copy protection of an application installed on a hard drive. Often such programs are created by so-called "hackers" and are available free of charge. More about hackers later.

Another method of software protection involves setting a "time bomb" in the software which will go off after a certain period of time (days or weeks) if the user has not paid for an unauthorized copy. If the time bomb is triggered, the software may be programmed to erase itself, along with any files that have been created using the software; more often, it simply ceases to launch.

Yet another method of protection used by computer manufacturers is to embed a registration in the system files of a networked computer when the application is installed. Any attempt to use this same registration number on another installation on the network will result in an error message. This does not, obviously, prevent installation on a home or off-network computer.

A method encouraged by BSA is called "product activation." Simply put, it makes access to online secured registration information part of the installation procedure. Users who have not registered the application will not be able to complete the installation procedure.

Counterfeiting creates its own problems for software producers. Microsoft and other companies are using creative solutions to "flag" counterfeit CD-ROMs before they are purchased. For

Chapter 13: Educational Computing and Society

example, a hologram ("Genuine") may be pressed into legitimate software CDs. Many producers have developed content on their web sites to educate purchasers to look for full, well-written documentation and license statements in the packaging or bundled with a new computer.

Overall, software companies give a high profile to the pursuit and punishment of software copyright infringement through the efforts of associations such as the SPA and the Business Software Alliance.

They also rely on people's sense of ethical responsibility. Software copyright infringement is theft; it is against the law. We, as teachers, should unfailingly set an example to our students and we should take time out with them to help them become sensitized to the ethical and legal implications of what they are doing when they copy software. Remember: our job as teachers is to guide children in their quest for the knowledge that will empower them to become responsible members of their local, national, and global communities.

STEPS SCHOOLS SHOULD TAKE TO DISCOURAGE SOFTWARE PIRACY

The SPA has an anti-piracy education division on its website. Here you can find, and download, the FAQ Fact Sheet for Schools (<http://www.siiia.net/sharedcontent/piracy/policy/okschools.pdf>). Further, they recommend that organizations such as schools initiate the following Nine Steps to Getting and Staying Legal (SPA):

- **"Appoint a software manager"** responsible for keeping records of purchases and software use. Give the appointment a high profile in the school district so as to send a message that software theft is taken seriously. The software manager might ask for help from faculty representatives at each school in the district. The committee thus constituted would not only actively discourage piracy, but it might also act as a clearinghouse for the district in the purchase of software and the negotiation of sensible site licensing with a view to obviating piracy.
- **"Create and implement a software policy and code of ethics!"** The software management committee would be responsible for giving this code a high profile too.
- **"Establish software policies and procedures."** These would include such topics as who can install software, what limitations and responsibilities are part of installation, downloading demo and free software, software gifts, software on student laptops, software removal and license transfer. Policies and procedures should be included in an AUP (Acceptable Use Policy) signed by students, faculty and staff.²
- **"Conduct internal controls analysis"** yearly to test yourself for compliance. This might include a faculty self-check or quiz session, updating of all auditing software and firewall definitions, and adding new members to the management committee.

¹ Sample Codes of Ethics can be found at: <http://www.caast.org/resources/guide/default.asp?load=ethics> ,
<http://www.gc.maricopa.edu/ppcweb/Software/SoftwareCodeofEthics.htm> and
http://its.ndsu.nodak.edu/software_licensing/NDSU-open/code_of_ethics_form.html .

² Sample AUP's can be found at: <http://www.aupaction.com/aupsonweb.html>.

Chapter 13: Educational Computing and Society

- **"Conduct periodic software audits."** As already mentioned, the BSA makes network auditing software available free of charge. It is also possible to remotely or locally print a listing of all software on a hard drive. The list can then be compared against purchasing and installation records. This would be a simple process if a software manager has been appointed and keeps track of software purchase and use.
- **"Establish and maintain a software log of licenses and registration materials."** This would be an important part of the job of the software manager. It can easily be done digitally by creating a database that includes purchase, registration and specific installation information.
- **"Teach software compliance."** Not only students, but also faculty, administration and staff should regularly be reminded of their responsibilities vis a vis the law and the school's policies and procedures.
- **"Enjoy the benefits of software license compliance."** These would include home computer installations where allowed, technical support and inexpensive software upgrades.
- **"Thank employees and students for participating."** Positive reinforcement is a powerful educational tool! A thank you has the added effect of serving as a reminder to all to remain diligent. Good ethics, after all, can be catching.

Schools and districts which apply recommendations such as these not only protect themselves against liability, they also help their students, through the faculty, to develop a sense of ethical responsibility which will overflow onto other areas of their lives.

SECURITY: HACKING AND CRACKING

Hacking generally describes the activity of computer aficionados who become absorbed with the challenge of pushing computer technology to the limits of its capabilities. The term "hacker" is not per se pejorative. Indeed, it started out as a term of endearment to describe lovable and often "nerdy" individuals who were recognized as benefactors to society because of the innovative computer-based solutions which they created. Hackers were programmers and visionaries. In the mid-1970s these benevolent hackers formed an informal association called the Home Brew Society which included in its membership people like Steve Jobs and Steve Wozniak who founded Apple Computer Corporation.

Today hacking is generally frowned upon because the term has come to be associated with practices that involve individuals who use computer technology to break the law, specifically to violate the security or privacy of computers and networks. The term that used to describe criminal hacking--**cracking**--was in vogue until "crack" and "crackers" became identified with other social ills not related to computing. In the next several sub-sections we will briefly describe the kind of criminal hacking of which teachers and their students would do well to be aware. Few of our students will ever be guilty of criminal hacking, but many of them will be victims of it.

Chapter 13: Educational Computing and Society

Computer Viruses and Other Malware

Computer viruses are programs created by hackers. As their name implies, viruses infect other computer systems by attaching duplicate copies of themselves to legitimate operating system or applications software with which they come into contact. They are carried from computer to computer either indirectly by way of disks or tapes, or directly by way of e-mail attachments and downloaded software.

Any computer virus should be taken seriously. Most viruses are designed to do some kind of damage to a system either by destroying data or otherwise compromising a system's operations in such a way as to make it unusable. Other viruses might appear to be "harmless," perhaps causing a funny face or announcement to appear on the screen at some programmed date and time. But "harmless" is a relative term. Anything that interrupts normal computer operations is cause for alarm because there is no telling what else might be going on in the background, unseen on the computer screen.

Computer viruses are activated in various ways. **Time bombs** are so-called because they are programmed to "go off"--start doing the damage they have been programmed to cause--at a certain time on a certain date (a popular date is Friday the 13th). **Logic bombs**, on the other hand, are usually less predictable because they are triggered when some specific set of switches (bits) inside the computer's memory become electronically set to a predetermined value.

There are now hundreds of decidedly harmful computer viruses capable of anything from changing or destroying data, slowing down or even immobilizing a system, or interfering with the system's interaction with peripheral devices such as the screen or printer. One common and annoying virus attacks the Macros that run inside of many Microsoft documents. They may, for example, make all subsequently opened files "Read Only" or "invisible" to Word itself. Such viruses spread quickly from home to school and hence throughout a school's network.

Malware: Worms and Trojan horses

Malware refers to malicious computer programs that are run on your computer without your knowledge. A special type of malware, called a **worm**, is a program designed to duplicate itself not only from machine to machine, but also *within* each machine, effectively overwhelming primary memory with copies of itself and leaving no room for any other programming activity. As it does so, it deletes targeted file extensions or causes a program to overwrite its own code with nonsense code, often targeting those programs that are essential for the operation of the system itself. Moreover, a worm will often reply to unread messages in an e-mail reader (Outlook Express or Microsoft Exchange, for example), spreading itself quite handily and looking like messages from YOU. Worms will often masquerade as .zip files, media files (.mp3, .gif) or other file attachments. They are activated, or "installed," by opening the attachment.

An infamous worm called the Slammer was launched at 12:30 am EST on January 25, 2003. Within 15 minutes it "brought down the Internet," causing significant damage to the targeted SQL mega-databases that coordinated global digital commerce. The identify of the hacker is not known, but the effects of the Slammer are known: over \$1 billion in lost revenue worldwide. (Boutin)

Chapter 13: Educational Computing and Society

Another specialized category of malware is the **Trojan Horse**, named after the innocent-looking giant wooden horse built by the Greeks to gain covert entry inside the walls of Troy. The computer version of the Trojan Horse is a program which looks innocent enough--perhaps a computer game made available on the Internet and often an e-mail attachment--but which has code built into it which inflicts damage of one kind or another once installed on a computer system. This can range from destroying files to altering the appearance of your Desktop. Trojan Horses that are designed for e-mail distribution will generally then attach themselves to messages you send by way of your Address Book.

Spyware and Spam

Although there is some disagreement about when viruses leave off and malware begins, it is generally agreed that **spyware** are hidden malware that sit on your computer and gather information about your computer use, preferences and data **without your consent**. Although often created by paid or contracted programmers, spyware programs are of questionable legality. They can also be sinister, establishing a sort of "remote control" over your computer or browser, or logging, and communicating, all of your keystrokes (and thus your passwords and credit card numbers). Spyware presents a serious threat to individual and network privacy and, as such, is currently one of the most actively combated forms of hacking. Spyware also causes problems on the host computer, generally slowing performance, due to the large information files that they create and distribute behind the scenes. *Adware* is another pest, a subset of spyware, causing pop-up advertisements to appear even when you are not actively surfing. These are the result of a spyware application that communicates your Internet searching and computer activities to advertisers and others interested in such data, who send you pop-up ads geared to your "interests." There are numerous other forms of malware. They are well logged at PestPatrol Pest Research Center (<http://www.pestpatrol.com/pestinfo>).

Spam is another form of malware that is becoming more of a problem than a pest. This unsolicited e-mail is often advertisements, but can also be "pornspam." Clearly, schools want to block both categories. Although there is new federal legislation to reduce and, to some extent, monitor spam, this is malware virtually impossible to police by policy. Keeping alert to and reporting spam (but not opening it!) is yet another responsibility of the computer-using teacher.

Trespass of Computer Systems

This is one of the seemingly innocuous yet potentially most devastating activities carried on by modern day hackers. Skilled hackers are able to obtain the access codes and passwords of institutional computer systems ranging from the local hospital or university to the Pentagon and beyond. The networked world is an open door to hackers determined and skilled enough to get around the various levels of security designed into the systems. Some hackers are motivated purely by the thrill of being able to gain access to these systems; they have no intention of damaging the data stored in them, and no particular interest in the data per se. But the activity is still illegal because it is trespass, an invasion of privacy, and an infringement of peoples' rights.

Chapter 13: Educational Computing and Society

Other hackers go further, altering data, stealing data, destroying data, or adding data¹. Sometimes the objective is sabotage, sometimes espionage, sometimes thrill-seeking vandalism, and increasingly it is **identity theft**. *Sniffers* are programs written by hackers for the purpose of capturing id names and passwords as the data packets travel across a network. Criminal prosecutions have been brought against a number of such hackers in the last few years.

When the hacker is working from a foreign base and infiltrating US government computers via satellite, the potential for disaster is real. Such was the case in 1988 when a hacker in West Germany tapped into NASA computers. Fortunately a NASA computer scientist discovered the intruder early on and, in order to track him down, set up elaborate monitoring procedures which kept NASA apprised of his every move. Eventually the hacker was traced back to West Germany. No serious damage was done.

But it is not only outsiders that breach the security of networked computer systems. Kabay (1992) reminds us that "75% to 80% of all attacks on data confidentiality and integrity are by employees authorized to use the systems and networks they abuse." Much of this in-house hacking, even when detected, goes unreported because companies fear loss of reputation and credibility in the eyes of the public in much the same way as banks are loath to report that they have been victims of electronic embezzlement.

Similarly, schools will often deal with hackers quietly and in-house. It is helpful, therefore, for a school or district to have a strongly worded, legally viable, and clearly stated policy spelling out the consequences of hacking by students or employees.

Money Theft (Embezzlement)

The bill paid by banks for electronic fraud runs into the billions of dollars per year. The banks, of course, pass the bill on to the consumer. If the bank goes under, the tax payer picks up the tab. What Kabay (1992) has to say about network infiltration applies equally to electronic fraud: most of the theft involves company insiders--"white-collar criminals." The last thing the banks used to want was that their vulnerability to financial loss through credit card fraud and illegal transfers of funds should become public knowledge. Thus much of this kind of crime used to go unreported. Today, however, electronic embezzlement is so rampant that financial institutions are openly and diligently investigating cases when they are detected.

STEPS SCHOOLS SHOULD TAKE TO SECURE NETWORKS AND COMPUTERS

As long as computer networks are vulnerable, hackers will attempt to breach them. The responsibility lies with the designers, builders and managers of these systems to make them as secure as possible against unauthorized entry. This is a mammoth task because networks are communications systems; access is the key to their success. Moreover, even the best computer system and productivity software leaves "holes" through which hackers can gain entry.

¹ In schools, this is often salary, grade and testing data!

Chapter 13: Educational Computing and Society

The only way to fully protect a computer is to turn it off and/or disconnect it from the network. However, in addition to adhering to the Software Code of Ethics, there are several things teachers and schools can do to combat these menaces:

- The foremost solution is the purchase and installation of reliable up-to-date anti-virus software, such as that marketed by McAfee and Symantec corporations. In a school, both the network servers and all client machines, including portables, should scan hard drives, external and portable storage devices, all installations, downloaded applications and files, and all e-mail messages without cease. Virus "definitions" are kept up-to-date and made available at the website of the anti-virus producer; they should be automatically downloaded to all computers.
- Select an e-mail service or client that provides a spam and virus filter. These will generally either delete questionable messages, mark them, or route them to a discrete folder.
- Special software exists to detect and remove spyware and trojan horses. It is strongly suggested that a school obtain more than one such application, for none will do the full job. It is also possible to access an online anti-spyware service, which will scan and repair your hard drive via the Internet (with subsequent advertisements for the full version of the software).
- "Cookies," a common and generally benign form of spyware, can be manually deleted from within every web browser. Browsers can also be set to "deny cookies," but this has the consequence of making it impossible to access many of the newer websites.
- The school network should be sure to have an active **firewall**, which will help it to detect and log attacks to its security. Often these take the form of random, or purposeful, flooding of the IP address with requests; if that flood reaches critical, the network server can shut down.
- System and productivity application producers make "fixes" available constantly online. All school computers should be able to download and install these fixes as they become available.¹
- Educate yourself and the school community to a few simple rules:
 - Change passwords often and make them as random as possible;
 - Do not store passwords or financial information on the computer;
 - If you use the computer for financial transactions, do so only from a Secure Site (SSL) option;
 - Because many viruses are spread over e-mail attachments, it is a straightforward solution to **delete without opening any email message and/or attachment from an unknown**

¹ There was a time when Macintosh computers and systems were viewed as "immune" to viruses. This is no longer true. Not even the open source systems are immune these days.

Chapter 13: Educational Computing and Society

source. By setting your e-mail application to "delete attachments with original message" you can further protect yourself;

- Be alert to any sudden change in the performance or appearance of your computer(s). Report anything odd to network services immediately.
- It is wise also for a school's IT staff to keep all members of the school community informed of new viruses. Such information will sometimes be bogus (there are virus hoaxes quite often), but an ounce of prevention is worth it!

Moreover, networked schools of the future will have to implement the kind of steps recommended by Kabay (1992) to protect corporate networks. Here are Kabay's recommendations to network managers:

- Have a message displayed at the network log in that warns hackers that the system is for authorized users only and that intruders will be prosecuted. If you do not use such a log in, consider implementing it.
- Have a written plan of network security procedures describing standard operating procedures including counter measures and defense plans for when the network is under attack.
- Make access controls and event logging (maintaining a record of all use of the network) part of this standard procedure.
- Regularly go over the procedures with personnel responsible for system security.

For wireless networks, it is possible to restrict network access to only those MAC addresses¹ that are logged with the network server. Furthermore, all modern networks can be remotely managed. Network attacks and problems often occur after hours; if the managers can be alerted to attacks and then scan, repair and reboot network servers from their homes or laptops, the institution itself will be more secure.

This might read like overkill for many school teachers and administrators, especially in these early days of networked computing in schools K-12. However, computer managers at any college can relate a litany of horror stories that are the result of abuse of computer systems by that minority of students with a personal or societal axe to grind. Remember, trouble most often comes from inside.

LOOKING BACK

This chapter has briefly examined the impact of computers on society. Computers have been incorporated into every product under the sun. They have been woven into the fabric of our systems of transportation, administration, information, communications, manufacturing, finance and government, to name but a few. They have begun to transform the way we live, the way we work, and the way we play. Inevitably they are being slowly but surely woven into the fabric of our education systems, too, and they will transform the way we teach and learn.

¹ You will remember that each hardware device on a network has a discrete and unique digital address. In this case, the MAC address is on the wireless NIC cards in the laptops.

Chapter 13: Educational Computing and Society

This chapter also has argued the case for incorporating into school curricula the discussion of the computer-related ethical and legal issues raised by new technologies. James Truslow Adams pointed out that "There are obviously two educations. One should teach us how to make a living, and the other how to live." Schools should prepare children to address ethical and legal problems when ignorance of them will leave students vulnerable to victimization of the kinds described in this chapter.

Sanders (1986) observed that we can restrict ourselves as teaching professionals to the narrow task of working within the framework of the narrow academic responsibilities that are assigned to us, or we can extend the scope of that commitment to include the parental, counseling, and leadership roles which our students need more than ever today.

The question every teacher must address is this: "Is it fair that just a few of today's children are already enjoying the advantages that computers, used appropriately, can bring?" The objective of this book is to open a window onto the classroom of tomorrow. This classroom is already available for a privileged few; we must ensure that it is available to all.

When they graduate from school, our students will function more effectively if they protect themselves against the unfair competition that comes with privacy invasion. On the personal level our students must learn to be conscious of, and give due recognition to, the privacy and equality rights of others. Girls, in particular, must learn to protect themselves against unequal opportunity arising from a prejudicial stereotype that women lack technological competence.

Stealing software is both easy to do and easy to get away with. Hacking is not so easy, but it presents an irresistible challenge to bright, determined, morally-indifferent individuals who need the boost to their egos that comes with the exercise of the power that their computing skills put at their fingertips. Unfortunately they do not feel constrained by a code of ethics that respects others' security and privacy rights.

The more we understand the realities of the computerized world, the more fully we will be able to function in it. This chapter has discussed software piracy and hacking in some depth not simply because they are interesting to learn about. It is part of our role as teachers to make our students aware, on the one hand, of the constraints on their freedom dictated by the rights of others and, on the other hand, of the extent to which their own rights can be infringed upon by the unethical and/or illegal activities of the kind described. Our students almost certainly will be victims of hacking. They may even be among the few who find these activities "bait which [they find difficult to] resist swallowing." The knowledge that you help them acquire by discussing these issues with them will serve both them and society well

LOOKING FORWARD

This concludes our study of the social impact of computing. In the last chapter of the book we will reflect upon the theory and practice of computer-based teaching and learning. Computers have value in schools only to the extent that they reinforce the centrality of the individual student in the educational process while providing opportunities for that individual student to work collaboratively with peers at home and abroad. The cultural change brought on by technology

Chapter 13: Educational Computing and Society

will be as dramatic for teachers as for students. The most successful teachers will take every opportunity to acquire the skills and concepts that are necessary to provide an appropriate and effective learning environment for their students.

What shape that learning environment will take is still largely a matter of conjecture. Cheaply available, wireless notebook size computers may eventually replace paper-based grade books and rosters. A computer weighing a couple of pounds with the power and functionality of an end-of-twentieth century supercomputer and costing no more than a few dollars will find its way into every teacher's brief case and every student's backpack. We will be able to download into it a lifetime of relevant data. We will be able to link to networks which will put us in touch, not only with the entire world of information available at the end of telecommunications lines, but also with our students wherever they may be.

Perhaps much of education will eventually take place from the home—a teleschooling equivalent of telecommuting. Just as many workers now log on to their companies from home-based offices, so tomorrow's children may power up the information center in their room at home to log in to classes which do not require their physical presence at a central learning location.

Student teachers in this first decade of the 21st century will see extraordinary change during the course of their careers. *The key to their survival will be their ability to adapt.* An understanding of reality is the foundation for purposeful adaptation, and an understanding of reality is borne of experience and conscientious study of the wisdom of those who have gone before. Chapter Fifteen tries to capture past and current pedagogical wisdom and apply it to the realities of Education for an Information Age.

Chapter 13: Educational Computing and Society

DO SOMETHING ABOUT IT

Suggestions for exercises and projects

1. There is an appropriate time to bring up specific ethical and legal issues with students. Brainstorm with your colleagues or classmates to define just when and how such a discussion might arise with students, and how it might best be conducted.
2. What are some of the special difficulties experienced by inner-city and rural school districts that result in underutilizing computer-based technology? Brainstorm with colleagues or classmates to come up with strategies for these school districts to optimize their investment in the technology and overcome the difficulties under which schools must operate.
3. "It is impossible to control invasion of one's privacy." Discuss the pros and cons of this argument. In what ways, other than those discussed in this chapter, can you protect your privacy? Is it important to raise this with students? Why?
4. Brainstorm with colleagues or classmates to come up with further strategies for encouraging girls to get involved in computers, mathematics, and science. Then try them out, make a note of the most effective, and publish them in a booklet for distribution to your school's faculty and students.
5. Examine the details of a typical software license agreement and determine to what extent the agreement tallies with copyright law.
6. Invite a guest "expert" from a local software company into your class to discuss the negative effects of unauthorized copying on the software industry. During the class, students should take notes and afterwards write a newspaper-style article about the visit.
7. Brainstorm with a group of other students on the subject of hackers and computer viruses. List the kind of problems computer viruses can cause you, and identify strategies you can implement to avoid becoming a victim of hacking activities such as computer viruses.
8. Download and read over the SPA document, "Is it OK for Schools to Copy Software?" (http://www.sija.net/piracy/policy/edu_copy.asp). Are there any answers that you do not find convincing? Why? What, for you, is the most compelling reason why copying software is unethical? Why?
9. Invite a member of the IT or Network Support staff of your university into your class to discuss the negative effects of unauthorized copying, piracy, and software downloading. During the class, students should take notes and afterwards write a newspaper-style article about the visit.