PART OF THE PICTURE: Ethics and Issues

BY ANNE MARCHANT, GEORGE MASON UNIVERSITY

To be good is noble, but to show others how to be good is nobler, and no trouble.

Mark Twain

Ethics and Society

What will the future bring? Will we live a life of leisure with all our tedious chores performed by intelligent machines? Perhaps we will live instead in an “information prison” with all the details of our lives recorded and analyzed by government or by corporations that exist solely to buy and sell information. To a large extent, the future will be driven by the choices we make now.

Computers permeate every aspect of our lives. In addition to making businesses more productive, they also perform many life-critical tasks such as air-traffic control, medical diagnosis and treatment, and emergency communication. The field of computer science is largely unregulated. Programmers are not required to pass proficiency exams or obtain state licenses to practice their art. In an effort to protect society from the obvious dangers, the field is regulating itself. It does this by encouraging the study of ethics and by demanding the highest level of integrity from its members. Some companies are instituting ethics training for their employees and ethics web sites are appearing where professionals can debate ethical concerns. Professional organizations such as the Association for Computing Machinery (ACM) and the IEEE (Institute of Electrical and Electronics Engineers) have adopted and instituted a Code of Ethics. Students are encouraged to join these organizations and familiarize themselves with these codes. Most colleges and universities also have policies governing the responsible use of computers. Students are encouraged to read these carefully and to develop their own personal standards.

Computer Crime and Security

Some computer crimes are old crimes that simply make use of computer technology. These include harassment, stalking, child pornography, fraud and embezzlement. Other crimes, such as the release of rogue programs, are new forms of crime. “Rogue software” is a class of software designed with some malicious intent. “Viruses” are programs that “infect” software in order to replicate. They usually do something harmful as well. A virus may corrupt or erase information on your disks. “Worms” are self-replicating programs that repeatedly propagate until they overwhelm the computer’s resources. Although they may be spread across a network, viruses tend to create problems on PCs. In general, worms create problems on networks. “Trojan horses” can occur anywhere. These are programs that appear to do something useful while secretly doing something malicious. An example might be a program that appears to be a space war game that secretly transmits the user’s login, password, and user privileges to someone else.

In recent years, macro viruses and email viruses have become a more serious threat. Macro viruses attack macros in office documents. A macro is a short program used to automate frequently performed tasks. If your office software has a "macro virus protection" option, you may wish to enable it. Viruses may also be sent as attachments to email. Be wary of mails sent from anyone unknown to you. Instead of double clicking on an attached document, save it to disk and scan it before opening it.

"Denial of service attacks" are becoming a serious problem on networks. A denial of service attack occurs when there are so many requests for a network service that the targeted machine becomes overwhelmed and service to others is effectively denied. Coordinated attacks by groups of hackers can be especially difficult to thwart.

The term “hacker” has undergone a semantic shift in recent years. Originally the term meant someone who wrote poor programs (a “hack”). It then came to mean a computer enthusiast. Now it has come to mean a computer criminal (sometimes also called “crackers”). Hackers often justify their actions by claiming that they are just trying to learn about computers. Would-be hackers might consider that computer security is a rapidly expanding field. There is a tremendous need for “computer enthusiasts” with creative ideas. Recently, "happy hacker" web sites are starting to appear. These are groups that encourage constructive and legal ways of learning. If you are looking for a challenge, creating a secure system is a much more challenging problem than breaking security. Students who put their energy into learning about computer security may well be on the way to a rewarding career!

How can we protect ourselves against (destructive) hackers and rogue programs? The first line of defense is to use passwords that are not dictionary words and to change passwords frequently. Better means of user authentication are starting to appear. These include biometrics (e.g. fingerprint or retinal scans) and the use of encryption certificates. Backups should be kept of any information that is precious. It is very important to have at least two copies of every file at all times. It is also wise to keep backups at separate locations and in different media.

Users should keep antiviral software on their computers and be sure that they are familiar with how it works. Antiviral software needs to be updated periodically, at least every several months or so. Encryption should be used when transmitting any information that needs to be kept secure, including passwords, credit card numbers, or other confidential information.

Firewalls are systems that monitor traffic between networks to ensure that all network traffic is legitimate. Every network connecting to the Internet should have a firewall in place. System administrators should keep operating system and network security patches up to date, watch for security advisories, keep detailed logs, and use software tools (port scanners) designed to uncover system weaknesses.

Traditional security is especially important. Physically restricting access to computer systems can prevent many problems. The majority of computer crimes are not committed by hackers, but rather by employees or former employees of organizations. This means that employers need to screen applicants carefully, monitor employees’ behavior, encourage a positive work ethic, and reward integrity. Grievance procedures should be in place to resolve work-related problems and diffuse hostilities when they arise. Secure audit systems should be in place to track fraud.

In 1996, President Clinton established a Commission on Critical Infrastructure Protection. The mission of this commission was to identify weaknesses in critical systems, such as communications, banking, energy, etc., and to propose defensive strategies. Cyberterrorism and cyberwarfare were identified among the potential threats. In response to these concerns, the National Infrastructure Protection Center was formed within the FBI. No doubt both defensive and offensive information warfare capabilities are being developed by governments and organizations around the world. A discussion of warfare is beyond the scope of this chapter, but the ethical implications of this new form of warfare are profound. Will civilian casualties be increased or reduced? As information warfare develops, will the world be a safer place or a more dangerous place? Finally, can information technology be used in such a way as to increase the socio-economic bonds between peoples around the world, making the need for such tactics less likely?

Health Concerns and the Environment

Today, our economy is based largely on information-related jobs. This means that many of us spend long hours behind the computer staring at monitors. The most obvious problem this creates is lack of exercise. We need to remember to make exercise a regular part of our lifestyle. A more insidious problem is a class of injuries known as repetitive stress injuries (RSIs) that result from performing the same actions repeatedly without taking breaks. Carpal tunnel syndrome is one such injury that may result from typing for many hours. These injuries can be incapacitating and may require surgery.

Questions have been raised as to whether computer use can cause problems such as miscarriages, birth defects, and cancer. These are still controversial. Some have suggested that stress and lack of exercise may be more harmful than electromagnetic radiation.

Staring at monitors for long periods of time may cause one to lose the ability to focus prematurely (“farsightedness”). One should reduce glare when possible and use the highest resolution screen possible. It is also advisable to look away from the screen and focus on distant objects periodically.

The ethical employer will insist on ergonomic work station design, encourage employees to take regular breaks and exercise, and watch for signs of excessive stress in fast-paced information-related jobs.

"Internet addiction" is now a recognized obsessive-compulsive disorder. This is the inability to leave the computer for any length of time especially to the extent that it interferes with personal relationships, academic or job performance. Individuals may use "chat rooms" or news groups as a way to escape other problems. Or they may develop obsessions with on-line gambling, web surfing, or pornography. Parents may want to limit their children's access time to the Internet, just as they set limits on TV or other activities.

We think of the computer industry as being relatively friendly to the environment, but there are a number of serious concerns. The manufacture of computer chips can involve some chemicals that need to be carefully managed and disposed of. The ethical manager will see to it that paper and laser printer toner cartridges are recycled. Beyond that, each programmer and engineer needs to address the question: “Will my contributions make the world a better place or will my work cause harm?”

Information Ownership

Congress is granted the authority to "promote the Progress of Science and useful Art, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. Constitution, art. 1, section 8, cl. 8

Copyrights protect the original expression of ideas. You can't copyright a fact or the idea itself, but you can copyright the expression of an idea once it is fixed in a tangible medium. (This may be written text, recorded sound, or software stored on a disk.) A phone call can not be copyrighted (unless taped), but email or on-line chat may be copyrighted if it is saved to disk. (Note that some company contracts co-opt their employees' email copyrights.) Under today's laws, a copyright notice © is not required to secure a copyright, nor need it be registered with the Library of Congress. However, these precautions will help to protect your work and support your case should you try to prove infringement. In 1989, the United States signed the Berne Convention, an international copyright agreement. With the growth of the Internet, international protection for intellectual property is a rising concern. The 1997 NET (No Electronic Theft Act) specifies harsh penalties for both commercial and non-commercial infringement of the copyright of electronic materials. This law does not specify "fair use" of a limited portion of copyrighted materials for educational, research or journalistic purposes. Therefore, unless work is specifically identified as being in the public domain, it's safest to get permission of the copyright holder before using someone else's work.

A copyright grants the copyright holder exclusive rights to the work's duplication, any derivative work, and the right of distribution or display. The integrity of the work must be maintained and the work must be properly attributed to the copyright holder. Copyrights may last up to 100 years depending on the date and nature of the work.

Students should be aware that it is an infringement to copy pictures or text from other web sites onto your own web page unless the copyright holder has granted permission. Creating a link to another page is legal (although this too has been challenged in court!). Similarly, it is illegal to scan in images to use on your web page without permission. You are essentially "publishing" someone else's work. Note that this is different from quoting something in a written paper that you submit as class work. As long as you include only a small portion of the work and properly attribute it to the author, this is considered "fair use."

Software is usually copyrighted. The holder of the copyright does not sell the software itself, but rather sells licenses to use the software. It is worth taking a minute to read the license that comes with software you purchase commercially. In general, it is illegal to make copies of commercial software except for the purposes of making a backup. As a rule, you must purchase a legal copy of the software for every machine you intend to install it on (although there are exceptions in some cases). Large companies and educational institutions will often purchase "site licenses" that allow them to install the software on a network file server. Duplicating software without paying for it is called "software piracy" or "bootlegging."

Sometimes software may be distributed as “shareware.” Usually, shareware may be freely duplicated and distributed, but the author will require you to register the software and pay a fee if you decide to keep the software. Freeware is software that the author has placed in the public domain and may be duplicated freely.

Inventions, processes, and algorithms may be patented. An idea must pass a rigorous set of tests in order to be patented. The concept must be a new idea, it must be useful, and it must be “non-obvious” to other professionals working in the field. A patent may be held for 20 years and grants the patent holder the right to control sale of the invention and the right to royalties.

The legal system is struggling to manage the protection of electronic intellectual property. Does it make sense to grant an individual exclusive rights to an idea for 20 years in the rapidly changing field of computer science? As the use of computerized information continues to increase, society will need to adapt by making new laws and by changing existing laws. Exciting careers await those who combine the study of law and the study of computer science!

“Netiquette” and hoaxes

On-line “chat,” newsgroups, and email create a new realm for social interaction. In one sense, the lack of face-to-face interaction has a leveling effect on society. We make judgments based on a person’s ideas instead of on their age, race, social standing, religion, ethnicity, or appearance. On the other hand, there is a disturbing lack of accountability that leads people to engage in inflammatory exchanges. These “flame wars” are usually viewed by more experienced users as a sign of immaturity and inexperience.

Chain mail is disallowed by many institutions and may be illegal in some instances. Be suspicious of mail that encourages you to forward the message to many other users. These messages may try to play on your emotions with such statements as: “Little Johnny is dying of cancer and would like your email messages before he dies. . . ” or “Forward this mail to as many people as you can and it will bring you luck. If you don’t, some serious harm will come to you.” Such “chain mail” propagates quickly and overwhelms network resources. Don’t be taken in!

Virus warnings are often hoaxes. Be especially leery of email viruses such as the “Good Times” virus. (This is a very old hoax!) Check with CERT (the Computer Emergency Response Team) to verify virus alerts (see CERT’s web address provided at the end of this section).

Should anonymous email be permitted? Should we be accountable for the things that we say? On the one hand, we instinctively want to have the ability to “blow the whistle” anonymously—especially in cases where negative repercussions are likely. Anonymity may also protect such people as AIDS patients, abuse victims, and other folks who need to get information or support. On the other hand, anonymous email makes it easy to harass other users or make libelous statements. Before sending anonymous email, ask yourself why you need to send it anonymously. Is it really because you may be unfairly punished or is it really just a way to say something you are not brave enough to take responsibility for?

While most folks feel that free speech is an important right, few are willing to support "spam." Spam is unsolicited, bulk email, usually selling a product or service. While spam may just be a nuisance for the average user, spam can cause a serious loss of productivity to large corporations. There have been attempts to legislate against spam, and a number of court cases have not supported the idea that spam is a protected form of speech. We are beginning to see a whole line of anti-spam products and services appear.

Internet Content and Free Speech

The vast quantity of information now available world-wide is bound to have profound, long term ramifications. Information that was formerly only available within the walls of academia or published in obscure journals is now easily accessible to people of all classes, as long as they are computer literate and have access to the Internet. The problem is that the Internet is a reflection of society at large. The information on the Internet includes hate, doctrines of violence, a lot information that is wrong, and information that may be harmful to children.

Should Internet content be regulated? If so, how do we effectively regulate an international medium? Whose standards do we implement? There have been two major attempts at legislation, the Communications Decency Act (CDA), struck down by the Supreme Court in 1997 as a violation of the First Amendment, and the Child Online Protection Act (COPA), which is currently facing challenges in court.

Some argue that filtering software may provide a solution. Such software can be used by schools and libraries to prevent children from gaining access to undesirable material. Others argue that this is censorship and question the standards used in setting up filtering guidelines.

This is a topic that will continue to be hotly debated. What seems to be lost in the debate is a realization that with freedom comes responsibility--a responsibility to use the Internet appropriately, a responsibility to teach children to use the Internet in a constructive manner, and a responsibility borne by all of us to make judgments about the information we use and the sites that we patronize.

Students will need to make judgments about the web sites that they use as source material for course work and research. Is a given page from a reliable, unbiased source? Is the author selling a product or service? Is the author knowledgeable? Then too, there are web sites that offer students papers and homework solutions. What effect will these have on the development of each student? What will be the effect on society in general?

Privacy

While the US Constitution does not specifically guarantee a right to privacy, several of the Amendments have been interpreted as implying a right to privacy. (One example is the Fourth Amendment, which protects citizens against unreasonable search and seizure.) Do you feel that a right to privacy is important in a free society?

Database technology and the Internet make it very easy to store and transmit large quantities of information. Everything from our medical histories to our driving records are routinely bought and sold. As a society we need to come to terms with what information should be stored, how its accuracy can be verified, how it should be protected, and when it should be destroyed.

Ask yourself how you would feel if you were turned down for a loan because your credit history had been accidentally (or deliberately!) swapped with someone else's. When it is your word against the computer's, where is the burden of proof? Now imagine a worse scenario. Imagine that your name and social security number is very close to that of a convicted felon. Might this affect your ability to get a government job? On the other hand, law enforcement needs to maintain extensive databases to assist them in preventing and solving crimes.

Recently, there has been discussion about the implementation of routine "profiling" of airline passengers and subjecting those with suspicious profiles to extra searches. Profiles are generated by matching information in different databases to try to identify "suspicious" persons. Is safety more important than civil liberty? Should you have the right to know what information about you is being stored?

Concerns have been raised about information that is gathered about us online. Be aware of the information you supply to online retailers or when filling out online petitions or other forms. Imagine how this information might be used. Children should be cautioned against giving out personal information over the Internet. Many businesses publish a privacy policy that clearly indicates how information about clients will be used. A non-profit organization, TRUSTe, certifies that online businesses are adhering to fair information practices. If this sort of self-regulation is unsuccessful, congress may be forced to regulate business practices that infringe on consumer privacy.

Does your employer have the right to monitor your email and Internet usage? As long as this is disclosed, they probably do. How does this make you feel about your work? If you know that you are being monitored, are you likely to change the way you behave at work? Should all employees be monitored or only those in particularly sensitive jobs?

With world populations continuing to rise, governments and economies become increasingly dependent on computerized systems to function. The danger is that if we do not make careful choices, we will be ever defined and controlled by data files. Worse, in the wrong hands, information systems can become the tools of oppressors.

As computer professionals, you can do your part to protect privacy by observing security precautions, restricting access to information, and by encouraging professional behavior among your colleagues. When information is gathered, procedures and policies must be in place to define how it will be used, to ensure its integrity, and to determine how and when it will be destroyed. Remember that email should be treated as if it were a "post card," and not a sealed letter. Information that needs to be kept private should be encrypted and important documents should be digitally "signed." You should become familiar with the Electronic Communications Privacy Act (ECPA) of 1986 that protects private communications.

Quality Control and Risk Reduction

As you are beginning to learn, writing good software is extremely difficult. Software needs to be carefully designed, carefully developed, and tested as thoroughly as possible. Commercial software is routinely put through in-house testing (“alpha” testing) and then testing by select clients (“beta” testing). Some managers will even plant bugs in their products knowing that in the process of finding these bugs, their programmers will uncover other errors. Standards for software in life-critical applications need to be extremely high. Interfaces must be easy to learn and must be “bullet proof.” They must anticipate user errors and safeguard against potentially serious mistakes. Documentation and user training need to be part of the overall product plan, not afterthoughts. If serious flaws are detected, there should be some mechanism in place to report problems, correct them quickly, and notify users.

Computers are powerful tools. This means that when we make mistakes with computers, they tend to be large scale! As students you should learn to do “back of the envelope” approximations to develop a sense when results are wrong. You should develop a style of coding that is readable. Remember that the person writing the code may well not be the one to maintain it! Even when code appears to work, make use of debuggers, the assert statement, or simply print out the values of variables to make sure that code is correct. Finally, document your code thoroughly with comments, “help” or “readme” files, manuals, or whatever system is required by the application.

The recent Y2K issue has drawn attention to our increasing dependence upon computer technology. (This problem occurred because historically, programmers used only the last two places to store a date. In other words, 1999 would have been stored as 99. This meant that computers could not differentiate between 1900 and 2000.) While there was a great deal of hype, and a certain amount of fraud, many experts feel that forcing society to implement a thorough testing of systems and to develop backup systems and procedures has had many benefits and prevented many problems. The lesson to be learned from Y2K is to plan ahead!

The Future

Advances in technology are creating many admirable improvements in the quality of many lives. “Telecommuting” enables new parents to work, improves access for the disabled, and helps the environment by cutting down on traffic. “Distance learning” is making educational opportunities available throughout the world. All sorts of new economic possibilities are being created. Improvements in the speed of worldwide communication and the vast amount of information now readily available has profound implications we are only just beginning to imagine. Yet there are dangerous hazards to be negotiated. Choices we make now will determine how well we will meet these challenges.

- Exercises

Briefly define each of the terms in Exercises 1–16.

1. ACM
2. chain mail

3. copyright
4. fair use
5. firewall
6. hacker
7. IEEE
8. patent
9. piracy
10. rogue software
11. RSI
12. site license
13. telecommuting
14. Trojan horse
15. virus
16. worm
17. Examine recent issues of the New York Times, Time, Newsweek, or other newspapers and news magazines to find an article that describe one of the following:

    (a) A new application of computing

    (b) A problem caused by a computer error, either in hardware or software.

    (c) Difficulties caused by a new computer virus, worm, or Trojan horse

    (d) A break-in by a hacker or a group of hackers to databases containing sensitive information.

    Write a report that summarizes the article and your reaction to it, especially to any ethical and moral issues that are involved.
18. Many of the publications of the professional computing societies contain articles that are of interest to students. Select one or several of the publications in the following list, locate an article dealing with some current ethical issue, and prepare a written summary of the article, the ethical or moral problem involved, suggestions for dealing with the problem, and your reaction.

    Communications of the ACM

    Computers and Society , a publication of the ACM Special Interest Group on Computers & Society

    COMPUTERWORLD

    IEEE Computer

    IEEE Software

IEEE Spectrum

New Scientist

SIGCAPH Newsletter, a publication of the ACM Special Interest Group on Computers and the Physically Handicapped

SIGCHI Bulletin, a publication of the ACM Special Interest Group on Computer & Human Interaction

Software Engineering Notes , an informal newsletter of the ACM Special Interest Group on Software Engineering

19. Create your own “Code of Ethics” for an imaginary company. A good way to start is to think about school or workplace behavior that you find objectionable. Try to think of a code to address these problems.
20. Discuss freedom of speech and the Internet. Should any form of expression be permitted? Should individuals be free to post child pornography, hate, violent material, or materials that might incite others to commit crimes? What happens when different cultural standards collide? Are there technological solutions to these problems?
21. Discuss the gender gap in computer science academic programs. Men outnumber women roughly 3 to 1. Why is this, when parity has been achieved in other top professional fields? A recent study has shown that 95% of hackers are male. Why is this? \
22. Create a web page on one of the topics below and include links to related pages:
    CFAA (1986 Computer Fraud and Abuse Act)
    ECPA (1986 Electronic Communications Privacy Act)
    COPA (1998 Child Online Protection Act)
    FBI NCCS (National Computer Crime Squad. See http://www.fbi.gov)
    encryption
    software piracy
    viruses

For Further Reading

Baase, S. *A Gift of Fire*. Prentice Hall, 1997.

Bowyer, K. *Ethics and Computing* . IEEE Computer Society Press, 1996.

Cavazos, E. & Morin, G. *Cyberspace and the Law*. MIT Press, 1995.

Cheswick, R. & Bellowin, S. Firewalls and Internet Security. Addison Wesley, 1994 (2000 edition due out).

Denning, D. *Information Warfare and Security* . ACM Press/Addison Wesley, 1999.

Hoffman, L. *Rogue Programs, Viruses, Worms, and Trojan Horses* . Van Nostrand Reinhold, 1990.

Icove, D.J. *Computer Crime: A Crime-fighter’s Handbook* . O’Reilly Associates, 1995.

Johnson, D.G. & Nissenbaum, H. *Computer Ethics & Social Values* . Prentice Hall, 1995.

Neumann, P. *Computer Related Risks* . Addison Wesley, 1995.

Parker, D.B. *Fighting Computer Crime.* J. Wiley and Sons, 1998.

Schneier, B. *Applied Cryptography* . J. Wiley and Sons, 1995.

CERT Coordination *Center* `http://www.cert.org`

Computer Professionals for Social Responsibility `http://www.cpsr.org`

Ethics References `http://www.cs.gmu.edu/~amarchan/cs105/ethics.html`

Electronic Frontier Foundation `http://www.eff.org`

The Online Ethics Center for Engineering and Science `http://onlineethics.org/text/index.html`