# Structuring ethical curricula in the information age

## For restructuring ethical curricula in the information age

By Sarah Gordon

## Introduction

According to experts in the field of Information Technology, one of the most pressing need facing students in computer related fields is a lack of understanding of the social and ethical implications of computerization. In "Integrated Social Impact and Ethical Issues Across the Computer Science Curriculum" [Holz, Martin 92] we read:

"Computer technology is particularly powerful due to
its potential to change how we think about ourselves
as human beings, how we make decisions in
governance and social policy, and how we save and
pass on knowledge …

This challenge is particularly difficult given the
traditional mindset of technically trained
professionals who view social impact and ethics
issues as topics auxiliary to the foundation material
in computer science.

Technical issues are best understood (and most
effectively taught) in their social context, and the
societal aspects of computing are best understood in
the context of the underlying technical detail…"

This paper will address what is often said to be the most serious problem there is in implementing the sort of approach suggested in 1992 by Holz and Martin and still valid:

"The most serious problem in implementing this
integrated approach across the computer science
curriculum is the lack of familiarity that most
professors have in locating and preparing materials
to deal with the social and ethical issues."

We will identify some major ethical issues as they relate to computer based interactions, and provide a compact guide which educators can use to guide them in quickly obtaining materials needed for a more thorough exploration of these issues.

## Definitions

One of the first things we must recognize is the lack of familiarity students may have with some terms we may take for granted; even people in computing sciences may be unfamiliar with some of the terminology used in discussion of the ethical issues relating to technology. While they may have familiarity with the technology and with ethics, they have not been exposed to many of technological implementations which help create ethical conflicts. Additionally, since the computing sciences are so new, it is possible that students and educators are not sufficiently aware of the end-result of some computer based interactions. In some cases, people may be using different terminology or analogies which may not be conducive to a thorough discussion and understanding of the topics at hand. For this reason, a beginning course in social and ethical implications of technology must define terms - even those which may appear obvious. Some suggested terms are: e-mail, Internet, software, privacy, property, virus, world wide web, html, virus, copyright, shareware, IRC, ftp. These terms are used frequently in discussion of ethics and technology; however, some of the terms (privacy, property) are subject to interpretation. Others, (html, www, ftp), are not as widely known. The instructor may wish to let students list terms they are familiar with, to build a list of key words for future classes.

Once there are some definitions, (and in some cases, a decision that there are no adequate definitions that are generically applicable), traditional ethical terms and concepts can offer a solid base for exploration of modern technology. A discussion of Duty and Rights is a good place to start. Such a discussion can refresh the concepts of duty and rights; the instructor may wish to present in concise form a overview of "ethics" including deontology, utilitarianism, aristotlean and other ethical models of choice. From this point, issues related to duty and rights become clear as we explore some of these concepts.

## Duty and Rights

Traditionally ethics are viewed as how we behave in our interaction with other people, or in our behaviours which affect people. There are some basic rules:

Don't lie (to other people)

Don't steal (from other people)

Don't hurt (other people)

These rules are, of course, based on principles, which are in turn based on ethical theories of the varying types discussed above. The premise of these theories and their applications appear to be how we relate to other people and how our actions affect others as well as ourselves. The introduction of computing technology introduces an "interface". This interface is, of course, the computer. When we communicate electronically, we can forget there are people involved. This becomes more likely when we spend a lot of time in computing environments, away from other human beings. These computing environments are called "cyberspace" by some. In these environments, depersonalization and desensitization can and do occur. This depersonalization effect can manifest itself in various ways, from withdrawal from "real life", to abberant social behaviours. However, it is important to remember that what we may consider "wrong" may be considered "right" in the cyberspace environment, or it may even be considered a "non-issue". What sorts of behaviours and concepts exist in this environment? We will examine those which exist, and attempt to define some of the issues which we must address if we are to overcome our ambivalence on standards for judging the ethical status of a given situation.

### Hacking Issues: Damage, Ownership, Breaking in

The first concept we will examine is "hacking". Much formal written work has been done on hacking. There are books available at most libraries which tell the stories of hackers breaking into computers, and of the subsequent chases by law enforcement. Some even discuss the successful arrest and prosecution of these 'bad guys'. [Sterling, 1992] [Stoll, 1989] However, there are people who question the validity of some of the more conservative views toward computer hacking. Some serious issues need to be raised in a discussion of hacking. Denning [Denning, 1991] discusses the curiousity, peer pressure and thrill that contribute to some hackers motivations. When we examine the psycho-socio makeup of any group of young people, we find this is not at all an abnormal set of motivations. We hear from many persons called hackers that damage is wrong. This is not so far from our own perception of what is wrong. We would all agree that damage is generally wrong. This is a generic social principle.

"Leave only footprints, take only memories" is one slogan some members of the hacking community adhere to. "We don't hurt anyone" is a common claim of hackers. These claims lead us to some issues, such as what is hurting? What is damage? Is reading your electronic files "damaging" you? What is the importance of intent and motivation? Do people have a right to "equal access" as many hackers claim? What part do freedom and creativity, espoused by many hackers, play in the general development of computing technologies? Is creating new accounts damage? Is reading a password file damage, and if so, what kind of damage is it? Damage to who? Is exploring a system damage? Is it true that we would not be as technologicially advanced today if not for hackers? What constitutes breaking into a system? If a system is on the Internet and it is left "open", is it breaking in if you log in without specific authorization? If you can log in as guest, are you breaking in if you do? If you are not specifically invited to access a system, are you breaking in if you access that system? What are the responsibilities of the adminstrators of systems? Is it helping administrators to break into systems and tell them how you did it? How should we define and assess penalties for electronic crimes. What -are- electronic crimes? What -is- damage? Who defines it? We come full circle.

### Ownership Issues: Who owns data about you? Should software be free? Who owns the Internet?

Some of the questions we ask about hacking seem to be based on our lack of true understanding and definition of various forms of ownership; of systems and of the Internet in general. Classical definitions of IP aside, there appears to be in our computing community some dissension as to who actually owns (or who SHOULD own) "things" on the Internet. The Internet itself is not owned by anyone, although small parts of it seem to be getting swallowed up by commercial interests. There are people who feel that software itself should be free. Reasons such as the encouragement of social cohesiveness and enhanced development capability are usually cited by those taking this position. [Stallman] SPA (The Software Publishers Association) and other business oriented groups work to combat software piracy (which would not exist if software were free). [SPA] Piracy is rampant, depriving developers of huge revenues. Why do people feel it justifiable to copy software and use it without paying for it? These issues are worth discussion. Do people have a right to try software first? Do developers have a duty to let them? What about the argument that without copyright, there is little (if any) incentive for innovation?

### Privacy Issues: Who should be able to read your mail? Who owns information about you?

"Who owns what" also applies to concepts like E-Mail. Based on our traditional concepts of mail, we consider electronic mail to be private; however this is not necessarily the case.

It is not only trivial to read someone's mail, but many companies do it as a matter of routine. There are other questions we must consider when we move from paper mail into electronic mail. Who owns your electronic mail? Do companies have the right to read it? Does your service provider have the right to read it? Do they have a duty to inform you if this is their practice? Can a University rightfully decide what is an appropriate topic for you to discuss in public forum or e-mail? These issues are complex.

There are others. Privacy and ownership of information are not only up for discussion in broad generic philosophical terms, but in real life impacting terms. Information on you is collected routinely. Who owns this information? Some of the types of information include your health records, driving records, neighbors, employment history. What ethical conflicts arise in the gathering and accessibility of this kind of information? Is a computer a good place to store this information? What, if any, safeguards should be required? What can you do to protect your privacy? What is the governments role in providing privacy. Is there a right to privacy in cyberspace? To answer some of these questions, we must first initiate informed discussions.

### Anonymity Issues: Does anonymity change behaviour? Is anonymity ever justified? What are your rights in electronic transactions?

Anonymity in life (specifically, in non-computer based) has been shown to change behaviours. In experiments throughout history, people have been shown to be less responsible in a group situation or where their indentity is not known. Computers can encourage and facilitate anonymity, and multiple or fake (not necessarily fradulent) identities. What sorts of ethical issues arise due to this process? Do you have the right to know who you are talking to? Do you have the right to hide who you are? Anonymous mailers and anonymous remailers add more depth to the discussion. It is possible to be totally anonymous on the internet, although total anonymity requires some effort. In what situations is anonymity justified, if it is ever justified at all? What are the affects of anonymity on electronic communications?

### Cryptography Issues: Who owns the code?

Privacy, some say, can only be ensured by cryptography. Some people say strong cryptography is needed to ensure the government cannot read private individual communications. Some cryptographic products are on the lists of things that cannot be exported, and are seen as 'weapons'. What are the issues surrounding cryptography and who are the cypherpunks? What is PGP? What is PEM? This information is also available from various electronic sources.

### Viruses Issues: Do you have a "right" to pass out viruses? Do you have a "duty" not to? Are computer viruses artificial life?

Viruses are another new concept in computing. The debate surrounding them seems to center around several issues: is virus writing a right? should virus distribution be made illegal. These questions are usually met with a variety of arguments from both sides, ranging from "Viruses are constitutionally protected" to "Viruses are Artificial Life" research. Neither of these has been proven and the debate goes on.

There are various mailing lists and newsgroups dealing with the topic: comp.virus, alt.comp.virus are two of the more used ones. FTP sites with information about viruses include ftp.informatik.uni-hamburg.de (login anonymous, username as password), and ftp.datafellows.com.

Other sites which are easily accessible via the Internet contain live viruses and viral source code. It is the opinion of this author that such distribution of viruses constitutes irresponsible action on the part of the account owner and should be discouraged. However, it is not illegal in some countries to make this information available, so discouraging will probably take the form of peer and societal pressures.

## Conclusion

The resources provided by this paper can provide instructors and students with information sufficient to begin a discussion on ethical issues related to computing. This list of resources is, however, by no means exhaustive. It is our hope that by encouraging the student to explore these issues, we are at the same time encouraging an evolution in the computing community's approach to these dilemmas.

Websites
www.2600.com
ftp.2600.com
www.acm.com
www.etext.com
ftp.etext.com
www.faqs.com
www.greatcircle.com
www.vortex.com

Denning, Dorothy: The United States vs. Craig Neidorf, Communications of the ACM, Nr. 3, Bd. 34, März 1991.
Elsevier Science Publishers, North Holland 1992, S. 137-143.
NET (Nationwide Electronic Tracking): "For Sale, Data About You", Harper's Magazine 1992.
Forrester, Tom und Morrison, Perry: Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing. MIT Press, 1990.
Holz, H.J. und Martin, C.D.: Education and Society, Information Processin 92, hrsg. Von R. Aiken, Band II (Proceedings IFIP 12th World Computer Congress, Madrid, Spain. September 7-11, 1992).
Stallman, Richard: Why Software Should Be Free. Free Software Foundation, April 1992.
SPA (Software Publishers Association): Is it O.K. to copy my Colleague's Software? SPA 1994.
Sterling, Bruce: The Hacker Crackdown: Law and Disorder on the Electronic Frontier. Bantam Books, 1992.
Stoll, Cliff: The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Doubleday Books, 1989.
The Knightmare: Secrets of a Super Hacker. Loompanics Unlimited, 1994.