IT Ethics in the Internet Age: New Dimensions

Sanjeev Phukan
Bemidji State University, Bemidji, USA

sphukan@bemidjistate.edu

Abstract

Issues of IT Ethics have recently become immensely more complex. The capacity to place material on the World Wide Web has been acquired by a very large number of people. As evolving software has gently hidden the complexities and frustrations that were involved in writing HTML, more and more web sites are being created by people with a relatively modest amount of computer literacy. At the same time, once the initial reluctance to use the Internet and the World Wide Web for commercial purposes had been overcome, sites devoted to doing business on the Internet mushroomed and e-commerce became a term permanently to be considered part of common usage.

The assimilation of new technology is almost never smooth. As the Internet begins to grow out of its abbreviated infancy, a multitude of new issues surface continually, and a large proportion of these issues remain unresolved. Many of these issues contain a strong ethics content. As the ability to reach millions of people instantly and simultaneously has passed into the hands of the average person, the rapid emergence of thorny ethical issues is likely to continue unabated.

Keywords: Ethics, Internet, Proliferation, Technology, Issues.

Introduction

The area of Information Systems (IS) ethics has received, deservedly, a fair amount of attention in recent times. IS Professionals generally agree that we need adequate ground rules to govern the use of present day Information Technology (IT). We have also recognized for many years the need to incorporate ethics into IS curricula [Couger, 1989, Cohen & Cornwell, 1989]. Current mechanisms which attempt to make IS professionals and students more sensitive to the ethical concerns within IT and IS may, however, be too tightly focused in terms of both issues and audience, especially in the light of the rapid proliferation of Internet use.

To properly analyze the impact of the Internet on IS ethics, we would need to establish the appropriate context. To this end, this paper explores several aspects of computer ethics that are relevant to today's users of IT. For example, who are the people that need to be educated on these issues? What *are* the issues, and what has been the impact of the Internet on these issues? What are current attitudes, perceptions, and behavior in situations involving computer ethics, and again, what is the effect of the Internet? Do we have guidelines and codes that provide assistance for these ethical situations? What else needs to be done to help address some of the problems in this important area?

The People

Solomon and O'Brien (1990) found that software piracy didn't seem to be much of a problem until

microcomputers made their first major corporate and home appearance about 20 years ago. Rapid proliferation of inexpensive technology certainly does provide an ample arena for an increase in the unethical use of this technology. Today, the pervasiveness of microcomputer and technology use is not limited solely to IS professionals and students [Wood, 1993]. As early as 1984, in his testimony before the US Congress, computer security expert Robert Campbell (1984) accused the computer industry of failing to develop the necessary ethical framework for IT use. He went on to say that the technology had already breached the boundaries of the professional arena and proliferated into the public domain. Today, technology use spans the widest possible range of activities and often begins at home at an early age. The Internet promises to push this trend forward at a rapid pace. In spite of this growth in use, many people who use technology at home and at work still find it to be a new and rapidly changing phenomenon. As a result, for many users of IT today, just learning how to use this volatile technology is the most important, and often the only, consideration; ethics and other related concerns are relegated to the distant background [Kallman & Grillo, 1996].

In her study of IS ethics attitudes, Kievet (1991) examined the differences between IS majors and non-majors in responses to a number of computer ethics related scenarios. She observed significantly different responses in four of the seven scenarios tested. This could very well mean that the need for computer ethics education is greater outside the IS related fields than within them.

Small businesses that have acquired computers within the last two decades may possess only a few micro-computers. In many of these businesses, the responsibility for buying and managing microcomputers often rests upon a person with no formal education in IS. Furthermore, this purchasing and supervisory role may form only a small part of their day to day duties. Although most people in this situation will be aware of piracy laws, exposure to the broader ethical issues of IT use is likely to be limited.

It is obvious that the number of people who use IT on a day to day basis, at home and at work, is growing explosively, especially as the penetration of the Internet increases. The target audience for discussions of ethical issues is certainly larger than we may have previously imagined. This expanded audience is also more difficult to reach since many of its members may never be exposed to a college level IS class. There is a very real possibility that unless appropriate steps are taken, many of these people may never receive the kind of exposure to the ethical concerns that should go hand in hand with the responsible use of computers and technology.

Issues and Concerns: How They've Grown and Changed

No discussion of computer ethics could be complete or meaningful without a brief examination of the broader definition of ethics. In everyday life, "Ethics is the practice of making a principle-based choice between competing alternatives" [Kallman & Grillo, 1996, p.3]. The issues in IS ethics would certainly fit comfortably within this larger umbrella. We ought to be able to assume that to use IT ethically, a person would first need to possess appropriate ethical standards for day to day living. It comes as a surprise, therefore, that, that many people who consider themselves ethical have less stringent standards when it comes to using computers and related technology [Solomon & O'Brien, 1990, Cohen & Cornwell, 1989].

Many people feel that using a computer to do something that is illegal or unethical is somehow not as "wrong" as other "real" criminal or unethical acts. For others, the term "IS ethics" refers just to issues of software piracy and unauthorized access to computer systems. Neither perception is correct. Criminal or unethical acts performed with the help of a computer are just as criminal or unethical. They usually just take less time or are harder to trace. Ethical concerns in IT actually encompass much more than just software piracy and computer hacking. Wood (1993) states that generalizations from many studies on IS ethics have been limited because most studies have concentrated solely on software piracy problems rather

than a broader definition of IS ethics. Malone (1993) argues that ethical concerns in IS must go beyond behaviors that are considered illegal. He includes such topics as computer crime, software reliability, privacy and matching, employee displacement, and artificial intelligence. Hall and Hamilton (1992) find the issues even more extensive. In their recommendations on the ethical concepts that should be integrated into the MIS curriculum they include the issues of privacy, security, ownership of property, race, equity in access, the environment, internal control responsibility of IS personnel, misuse of computers, artificial intelligence and unemployment and displacement. In their discussion of what constitutes unethical computer use, Kallman and Grillo (1996) include social and economic issues, issues of individual practice, development process issues, issues involving managers and subordinates, processing issues, issues relating to the workplace, issues of data collection, storage, and access, issues about electronic mail, resource exploitation issues, vendor-client issues and issues of computer crime.

The rapid growth of Internet access and use seems to have made many of these issues more significant and pervasive. This growth has also spawned a host of new issues. Issues involving intellectual property rights, ownership of data, copyright laws and violations, and plagiarism now affect millions of people rather than just a few. From perhaps an opposing standpoint come the issues of free speech and censorship.

It is obvious that the issues that are usually lumped together under the common area of "IS ethics" are in reality many and diverse. They extend far beyond the bounds of just criminal behavior. Perhaps more importantly, IS ethics issues affect a wide variety of people. Most people today are touched by IT in some way or another. To deal with the growing problem of unethical use of IT, we need a widespread awareness of the depth and breadth of these issues.

In the final analysis, I believe that there is no real difference between IS ethics and "regular" ethics. Issues of IS ethics usually arise in ordinary ethical situations where Information Technology happens to be involved [Kallman & Grillo, 1996]. Ordinary ethical dilemmas involve a wide variety of circumstances and situations, and the involvement of computers in day to day human activity is becoming increasingly commonplace. It follows that the issues of computer ethics are likely to be as diverse as those of ordinary human activity and will be encountered as frequently. They will just be more difficult to recognize because many of the situations may be new or unfamiliar.

There are many reasons for this difficulty. Many people actually do find it difficult to perceive ethical issues in their use of IT. For instance, people who wouldn't dream of reading someone else's mail browse through others' computer files with little or no feeling of guilt. Many of the hackers that break into someone else's computer systems would perhaps never consider breaking into someone else's home. Others copy software with aplomb, but are horrified when it is suggested that they are stealing. Kallman and Grillo (1996) point out that many of those who are unethical in their use of IT don't really perceive the ethical implications of their actions. Often, people who misuse computers and technology don't really feel that they are doing anything wrong because there isn't an easily identifiable victim.

Another factor that makes it difficult to pin down the issues involved in computer ethics is the newness of the technology. Some criminal and unethical practices involving computers would either never have occurred or would have been very rare without the recent massive proliferation of inexpensive computing power. Many radically new opportunities for crime would be impossible without computers [Neumann, 1991]. It is, after all, difficult to rob a train had trains not been invented. It is likely that software piracy would not have reached current epidemic proportions if microcomputers had not multiplied so rapidly [Solomon & O'Brien, 1990]. Hackers' bulletin boards would probably be rare. Computer viruses wouldn't cause such widespread consternation. The potential for IT misuse would be limited to far fewer users of this technology. Most of these users would be IS professionals with a greater awareness of the ethical issues involved [Wood, 1991]. The novelty of the technology also often creates situations with ethical im-

plications that have no precedent. Obviously, people or organizations have no previously developed mechanisms to help them deal with these new situations, and previously established codes, policies and procedures may have gaps in them that prevent them from pointing out the ethically correct way.

There is reason to believe that the ethical management of IT poses some special difficulties as well. Parker, Swope and Baker (1990) point out several reasons for this. For instance, information created and stored using IT is more easily altered, destroyed or accessed without authority or permission. Privacy, unauthorized access, and the theft of information become increasingly relevant concerns. Also, the use of computers and technologically advanced communications equipment changes the way people communicate with each other. Personal, face to face contact is reduced, decisions are made more quickly and less thoughtfully, and the potential for unethical use is increased simply because not enough time is devoted to careful consideration of all the ramifications of a particular act. Information sharing often conflicts with concerns of confidentiality and privacy, and the lack of access security can often make unethical use far too easy.

A natural tendency to depersonalize complex systems, remote and impersonal computer access, and an increasingly less stringent notion of corporate morality make it easier for some to rationalize their unethical behavior [Neumann, 1991].

The interaction of people with this new technology can create problems too. Because the tremendous growth in computing power has been coupled with a similar decline in costs, many more people today have ready access to enormous quantities of information and the inexpensive means to manipulate it. Even a decade ago, the situation was dramatically different and far less hazardous. The potential for unethical computer use has increased along with this growth in accessibility [Kallman & Grillo, 1996].

The Internet has probably had the greatest impact in the areas listed immediately above. As previously mentioned, the capacity to place material on the World Wide Web has rather suddenly been acquired by a very large number of people. Rapidly evolving software has gently hidden the complexities and frustrations that had been involved in writing HTML in its raw and nasty form. As an inevitable result, an increasingly large number of web sites are being created by people with a relatively modest amount of computer literacy, and who often have no ethical concerns whatsoever regarding the use of the technology.

Simultaneously, once the initial reluctance to use the Internet and the World Wide Web for commercial purposes had been overcome, sites devoted to doing business on the Internet mushroomed and e-commerce became a term that is now definitely part of common usage. Following closely behind the commercial sites were sites dedicated to informing the whole or part of the public about a variety of matters, not all of which were particularly appetizing. Consider, as an example, the web site maintained by one of the teenaged killers responsible for the April 1999 shootings at Columbine High School in Denver, Colorado.

The assimilation of a new and sometimes revolutionary technology is almost never entirely smooth sailing. The employment of the Internet and the World Wide Web for the many and diverse purposes that they are used for today is certainly no exception. As the technology begins to grow out of its infancy, a multitude of new issues surface continually, and a large proportion of these issues remain unresolved. Many of these issues contain a strong ethics content. As the ability to reach millions of people instantly and simultaneously has passed into the hands of the average person, the rapid emergence of thorny ethical issues is likely to continue unabated.

There is little argument regarding the power of the Internet to inform. As a media, it has far more potential than radio or television ever did, and both of those have permanently changed the world we live in, although not always for the better. One enormous difference between traditional mass media (radio, television, print) and the new media of the Internet is accessibility. The former were domains of the well heeled:

a relatively small number of people controlled radio, television, or the print media. On the other hand, almost anyone can place something on the Internet. As the use of web technology accelerates, and I have little doubt that it will, we need a greater awareness of the ethical issues and problems involved in the use of this tremendously powerful media tool.

Finally, to further confuse the situation, IS professionals often find it difficult to agree on what is ethical use of IT and what is not. As a result, many of the legal and ethical issues regarding the use of IT still remain cloudy. Although many countries now have laws to deal with the possible criminal use of IT, almost every new case brings to light ethical and legal aspects that have not previously been encountered or examined. Many of these situations find IS professionals confused about the issues and at odds with others in their profession [Samuelson, 1993, Denning et al, 1991].

These factors all contribute toward making it difficult, to say the least, to develop a clear and concise definition of what constitutes ethical use of IT. Implementation of ethical codes is only really possible if we can clearly define the territory that these codes should cover. We now know that a list of relevant concerns will not be short or simple. Neither will it be complete. As IT becomes increasingly more complex and widespread, we can expect ethical concerns to keep pace.

Current Attitudes, Perceptions, and Behavior

Unethical and often illegal behavior in the use of IT seems to be commonplace. Software piracy and unauthorized access to computing facilities are illegal acts in most countries. Yet, many users of IT violate these laws with little or no concern. If so many people are willing to act in ways that are patently unethical, what kind of attitude might we expect when the issues are a little more blurred?

Today, the Software Publishers Association (SPA estimates that as much as 20% of all personal computer programs in use are illegal copies [Weise, 1992]. With estimates of software sales today in the neighborhood of US$50 billion to US$60 billion, that could represent as much as US$12 billion each year. The SPA also contends that a large number of organizations buy only one copy of a piece of software that they intend to use, and then load it on as many computers as they own. The SPA has brought suit against several companies and at least one university because of this practice.

Many writers in the area of computer ethics paint an equally disturbing picture of current day business and computer ethics. Bloombecker (1991) finds reasons for despair, although he also finds reasons for hope. His contention, however, that software piracy and hacking remain largely offenses of the young may be too sanguine. Stark (1993) suggests that part of the problem of business ethics as a whole may exist because of the gap between "academic" business ethics and professional management. Machan (1991) agrees, pointing out that many classroom approaches to business ethics are little more than sessions of 'business bashing'.

Other writing and studies that focus more specifically on computer ethics show that the present situation is disappointing. In her study of software copying policies, Athey (1990) found a dismally poor attitude towards software copying at universities. She also discovered that university faculty were some of the worst offenders in this regard. Im and Van Epps (1991) found that respondents in 75% of the 241 business schools that they surveyed agreed that software piracy occurred at their schools. A study of college students showed that a significant proportion believed it was acceptable to pirate software [Cohen & Cornwell, 1989]. This was reinforced by a study carried out by Reid, Thompson, and Logsdon (1992), who found that software piracy was a significant problem among microcomputer users in general, but especially among university students. A similar study of university faculty [Wickham, et al, 1992] concluded that an intensive program is necessary to educate both students and faculty about copyright law. Peace (1997) reached similar conclusions for professionals that use computers.

Davis and Vitell (1991) suggest that ethical standards in IS may be on the decline, in sharp contrast to ethics in other business areas. Their study also revealed that a large minority of respondents believed that unethical IS behavior could actually help them to be successful.

Wood (1991), in his study comparing the computer ethics standards of managers and students found that the students tended to have lower ethical standards than present day IS professionals in nonacademic settings. This, he felt, was a reason for some concern since many of those students surveyed would soon be part of the business world. In another study [Wood, 1993] he concluded that the number of years of computer use had little to do with responses to scenarios involving computer ethics. This meant that there was no reason to believe that experienced IS professionals would exhibit more ethical behavior than those without the benefit of such experience. Somewhat heartening, however, was the fact that his study showed computer professionals as a rule tended to be able to recognize a computer crime when they encountered one.

The results of the many studies that have researched attitudes and perceptions regarding computer ethics show no reason for complacency. Perceptions of what is ethical and what is not vary widely. University students and faculty appear to have regrettably lax ethical standards when it comes to using computers. This bodes ill for the future, especially as Internet use becomes increasingly more prevalent. The arena, and therefore the potential for unethical IT use just keeps increasing. Even more disconcerting is the fact that although studies indicate that people seem to have a grasp of what constitutes unethical use of IT, their actual behavior often seems to ignore these very same ethical standards that they claim to possess [Wickham, et al, 1992, Athey, 1990]. That is, they know it's wrong, but they do it anyway.

Information Technology and Codes of Ethical Behavior

Codes of behavior for IS professionals have been in existence since the 1960's. Why then, the sudden fuss over IT ethics? Several factors have contributed to the situation.

First, the growth in technology, its complexity and its use, including access to the Internet, has been unprecedented. Ethical codes developed even a decade ago can't possibly address the bewildering range of possible situations involving ethical conflict. Second, because technology use is so pervasive, the majority of the people who should be targeted by these codes of conduct do not belong to the professional organizations that developed them. In fact, many IT professionals do not belong to any professional organizations. As a result, much of the audience remains untouched. Third, different organizations for IT professionals have different codes and guidelines. Although most have similar objectives, the treatment of these objectives differs from one organization to the next. Even if an IT professional were to belong to a particular organization, the standards by which he or she would be expected to live and work by would be different from those adhered to by a member of a different organization. There is no single set of widely accepted codes and guidelines for ethical decision making [Oz, 1992]. Finally, a code of ethical standards is not the law although most codes of ethics do incorporate sanctions to deal with misconduct. Although legislation to deal with a variety of computer and technology related crimes has been enacted, statutes fall far short addressing potential wrongdoing.

In a call for a unified ethics code for IT professionals, Oz (1992) examined the differences between the ethical codes of 5 organizations for IS professionals. The study found similarities as well as differences between these codes when examined in a framework of obligations to society, employers, clients, colleagues, the professional organization and the profession. One flaw in all 5 sets of standards was a lack of guidelines for prioritizing ethical conflicts. A unified code, the study concluded, would better serve IT professionals and would enhance public perception of the profession.

The Association for Computing Machinery (ACM) is the oldest professional organization for IT Professionals. It is also the largest. Recently, responding to the dramatically different computing environment of the present time, ACM members voted to adopt a revised code of ethics and professional conduct. The code consists of 24 imperatives, organized under the four broader headings of general moral imperatives, more specific professional responsibilities, organizational leadership imperatives, and compliance. A set of guidelines supplements this code and is intended to assist ACM members in dealing with the ethical issues addressed by the code itself [ACM, 1992, Anderson et al, 1993].

Anderson et al (1993) tested this revised code of ethics on several scenarios that involved ethical decision points. The cases were intended to illustrate both the broad range of issues that may be encountered as well as how one may use the code to deal with them. In their conclusions, the authors suggested that several ethical topics were either not addressed by the guidelines or were dealt with in insufficient detail. They further concluded that because of the diversity and complexity of present day issues as well the potential for new issues continually coming to light, the guidelines would need to be updated on an ongoing basis.

Summary and Conclusions

I think the most valid conclusion we can reach based on much of the work done in this area is that ethics in the use of IT, especially in the context of Internet use, are not in robust health. We have many reasons for concern.

The number of people touched by and affected by this technology is enormous and is growing rapidly, especially with the increased availability of the Internet. This makes a target audience difficult to define and difficult to reach. The ethical issues themselves are also difficult to define, increasingly complex and diverse, and are growing as rapidly as the technology. Attitudes, perceptions and behavior among users of this technology leave much to be desired. Codes of ethics and professional conduct vary from one professional organization to the next and are incomplete or obsolete. In addition, membership in these organizations make up only a minuscule part of the relevant audience. Classes in computer ethics, when part of an IS or IT curriculum, don't appear to make much of an impact and reach only a small proportion of students who use IT.

Obviously, the importance of IS ethics cannot be overstated in the age of the Internet. There are too many people involved for us to remain unconcerned. It is probably not possible to develop comprehensive ethical guidelines to cover every possible situation of IT misuse. It is possible, however, to realize the pervasiveness and the magnitude of the problem. It is also possible to develop ethical guidelines on an ongoing basis to keep pace with changes in the issues. Finally, it is vital that these guidelines be a part of *all* school and college curricula rather than just IT related disciplines.

References

ACM Code of Ethics and Professional Conduct (1992). *Communications of the ACM*, *35(5),* 94-99.

Anderson, R.E., Johnson D.G., Gotterbarn, D., & Perrolle, J. (1993). Using the New ACM Code of Ethics in Decision Making. *Communications of the ACM, 36(2),* 98-107.

Athey, S. (1990). A Comparison of the Fortune 500 and AACSB- Accredited Universities' Software Copying Policies. *CIS Educator Forum, 2(4),* 2-11.

Bloombecker, J.J.B. (1991). Computer Ethics: An Antidote to Despair. *The Mid-Atlantic Journal of Business, 27(1),* 33-42.

Campbell, R. (September 24, 1984). Testimony before Congress on Computer and Communications Security and Privacy. *Committee on Science and Technology, Subcommittee on Transportation, Aviation and Materials, US House of Representatives, 98th Congress, 2nd Session.*

Cohen, E., & Cornwell, L. (1989). A Question of Ethics: Developing Information Systems Ethics. *Journal of Business Ethics, 8,* 431-437.

Cohen, E., & Cornwell, L. (March 1989). College Students Believe Piracy is Acceptable. *CIS Educator Forum,* 2-5.

Couger, J.D. (1989). Preparing IS Students to Deal with Ethical Issues. *MIS Quarterly, 13(2),* 211-218.

Davis, D.L. & Vitell, S.J. (Summer 1991). The Ethical Problems, Conflicts and Beliefs of Small Business Information Personnel. *The Journal of Computer Information Systems,* 53-57.

Denning, D.E. and others. (1991) The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking. *Communications of the ACM, 34(3),* 23-43.

Hall, J.A., & Hamilton, D.M. (Winter 1992-1993). Integration of Ethical Issues into the MIS Curriculum. *Journal of Computer Information Systems,* 32-37.

Im, J.H., & van Epps, P.D. (Summer 1991). Software Piracy and Software Security in Business Schools: An Ethical Perspective. *Data Base,* 15-21.

Kallman, E.A. and J.P. Grillo (1996). *Ethical Decision Making and Information Technology, 2e,* New York: McGraw Hill.

Kievat, K.A. (Fall 1991). Information System Majors/Non-Majors and Computer Ethics. *Journal of Computer Information Systems,* 43-49.

Machan, T.R. (1991). Teaching Business Ethics in an Academic Environment of Mistrust. *The Mid-Atlantic Journal of Business, 27(1),* 59-65.

Malone, D. (Spring 1993). The Ethical Issues of Automated Information Processing. *Journal of Computer Information Systems,* 82-84.

Neumann, P.G. (1991). Inside RISKS: Computers, Ethics and Values. *Communications of the ACM,* **34***(7),* 106.

Oz, E. (1992). Ethical Standards for Information Systems Professionals: A Case for a Unified Code. *MIS Quarterly, 16(4),* 423-433.

Parker, D.B., Swope S., & Baker, B.N. (1990) *Ethical Conflicts in Information and Computer Science, Technology and Business,* Wellesley, MA: QED Information Sciences.

Peace, A. G. (Fall 1997). Software Piracy and Computer-Using Professionals: A Survey. *Journal of Computer Information Systems, 38(1),* 94-99.

Reid, R.A., Thompson, J.K., & Logsdon, J.L. (Fall 1992). Knowledge and Attitudes of Management Students Toward Software Piracy. *Journal of Computer Information Systems,* 46-51.

Samuelson, P. (1993). Legally Speaking: Computer Programs and Copyright's Fair Use Doctrine. *Communications of the ACM, 36(9),* 19-25.

Solomon, S.L. & O'Brien, J.A. (Spring 1990). The Effect of Demographic Factors on Attitudes Toward Software Piracy. *The Journal of Computer Information Systems,* 40-45.

Stark, A. (May-June 1993). What's the Matter with Business Ethics? *Harvard Business Review,* 38-48.

Weise, E. (November 18, 1992). Combating 'Softlifters'. *Minneapolis Star-Tribune.*

Wickham, M., Plotnicki, J., & Athey, S. (Summer 1992). A Survey of Faculty Attitudes Towards Personal Computer Software Copying. *The Journal of Computer Information Systems,* 47-52.

Wood, W.A. (Summer 1993). Computer Ethics and Years of Computer Use. *Journal of Computer Information Systems,* 23- 27.

Wood, W.A. (Winter 1991-1992). A View of Computer Ethics by Managers and Students. *The Journal of Computer Information Systems,* 7-10

Biography

Sanjeev Phukan is a Professor of Business Administration ate Bemidji State University, which is a member of the Minnesota State College and University System. He teaches in the areas of Operations Management and Information Systems. He received a Masters degree in Management Science from the Birla

Institute of Technology and Science, India, and an MBA from Illinois State University, USA. His research interests include ethics in information systems and global information technology