

An MBA Course in Ethics, Security, and Privacy

David J. Kroger¹

Mark P. Sena²

Information Systems Department, Xavier University
Cincinnati, OH 45208-5161

Abstract

Ethics is a topic of increasing importance in today's business world. One major area of ethics that is often overlooked in business curricula is that of information technology. This study provides a background on computer ethics in higher education and profiles a new MBA-level course in computer ethics, security, and privacy.

Keywords: Ethics, Security, Privacy, Computer Information Systems, Information Technology, Higher Education, MBA Curriculum

1. INTRODUCTION

Scandals such as those involving Enron, Arthur Andersen, and Worldcom have transformed the issue of business ethics into front-page news. While much of the recent news has focused on unethical accounting practices, the importance of computer ethics has also increased. The proliferation of personal computers, corporate networks, and the Internet have introduced many new computer-related ethical situations that businesses must confront. Issues such as computer crime, Internet privacy, intellectual property controversies, consumer trust, censorship, and other factors are in the forefront of business today. These issues have a great impact on the growth of E-business, which, in turn, has had a dramatic impact on the whole economy.

Computer ethics is not a new topic in higher education. Many universities have offered courses in various disciplines for the past 15 years. However, the coverage seems to be rather inconsistent across university curricula. In searching for information on courses dealing with computer ethics, one would find courses offered in Information Systems, Computer Science, Philosophy, Law, Communications, and other areas. The topics covered in such courses, as one would expect, tend to vary in conjunction with the department that offers the course. As a result, there is not a clear,

common set of resources for educators to utilize in courses dealing with ethics and related topics.

As ethics become a focus in business, it is important for business schools to examine how the topic should fit in the graduate business curriculum. While it is common for a core MBA information systems course to offer a limited amount of content dealing with computer ethics, it is rare to find an MBA-level course focused specifically on ethics and the related issues of security and privacy. The remainder of this paper will review the background of computer ethics including a brief history of the field, the diverse course offerings related to computer ethics, and the various textbooks on the subject. We also present a profile of new course offered at the MBA level focusing on ethics, security, and privacy.

2. BACKGROUND: COMPUTER ETHICS IN HIGHER EDUCATION

History of Computer Ethics

The foundation of computing ethics dates back to the years following World War II. Bynum (2000) credits MIT professor Norbert Wiener as the founder of computer ethics as a field of study. Wiener, in a 1948 book entitled "*Cybernetics: Control and Communication in the Animal and the Machine*", viewed the capabilities of computers as a "presence of another (in addition to the nuclear bomb) social

¹ krogerd@xu.edu

² sena@xu.edu

potentiality of unheard-of importance for good and for evil.”

This early work in computer ethics did not lead to significant progress in the field until the mid 1960s, when the important social and ethical consequences of computer technology became apparent (Bynum, 2000).

In 1973 the Association of Computing Machinery (ACM) adopted its first code of computer ethics. Later in the decade, a professor of medical ethics, Walter Maner, recognized the unique considerations of situations involving computers leading to a separate branch of applied ethics, which he dubbed “computer ethics.” Maner eventually published “*A Starter Kit for Teaching Computer Ethics*.” Building on the foundations of this work, in 1985, Deborah Johnson, published the first major textbook in the field “*Computer Ethics*.” Since that time, the field has grown rapidly with various courses, research centers, conferences, journals and textbooks devoted to topic.

With the popularity of the Internet and advances in science and technology, new issues in computer ethics continue to emerge, ensuring that this field of study will continue to evolve and draw substantial interest from scholars from various disciplines.

Courses in Computer Ethics

As previously mentioned, courses in computer ethics can be found in multiple subject areas. Courses in computer ethics likely evolved from programs focused on 1) computers or 2) ethics. Of course, computer courses have long been found in Information Systems, Computer Science, and other programs such as Telecommunications and Library Science. Any of these disciplines have a legitimate interest in computer ethics.

From the other end of the spectrum, the study of ethical behavior has been examined by educators in Philosophy, Psychology, Law, and Management. Thus, it should not be surprising to learn of the varied interest in computer ethics. As an example of the multidisciplinary nature of the topic, consider the course “Ethics and Law on the Electronic Frontier” offered jointly by MIT and Harvard (2002). The course is offered as a Masters of Engineering elective by MIT and a law course by Harvard and includes instructors from Law, Computer Science, Anthropology and Science Technology Studies.

Examples of course syllabi provided by ISWORLD (2002) reflect this diversity. Material covered in these courses can vary accordingly. The emphasized content is likely a reflection of the foundations of each discipline or the leanings of the instructor. Consider the prototype syllabus offered by David Vance, who maintains aforementioned the ISWORLD ethics site. The syllabus (2002) suggests coverage of:

- philosophical definitions, philosophical thought, sub-fields of philosophy

(metaphysics, pistemology, value theory, aesthetics, logic),

- "rational" and "critical" as they concern philosophical thought, speculative and analytic approaches to philosophy, "idealism" and "materialism"
- topics related to morality (logical positivism, relativism, existentialism, determinism; teleology (hedonism and utilitarianism), deontology
- etc,....

Thus, one approach is to emphasize the philosophical foundations of computer ethics.

For instructors who seek more applied content, Ethics in Computing at North Carolina State University (2002) provides a framework of ethical topics along with links to news and articles for each topic. Topics covered include:

- Basics (principles, codes of ethics, whistle blowing)
- Commerce (anticompetitive practices, auctions, cybersquatting, fraud, gambling, spamming, taxation, free trade, plagiarism (term papers), free trade
- Computer abuse (denial of service, hacking, viruses, spamming)
- Intellectual property (copyright, patents, law, piracy, MP3, etc.)
- Privacy (database privacy, email, privacy on web, encryption, anonymity, spam)
- Risks (artificial intelligence, licensure, network security, software reliability, software safety, computer model reliance)
- Social Justice (equity of access, workplace monitoring, immigration, offshore development (i.e., outsourcing), depersonalization)
- Speech (netiquette, free speech, anonymity, email privacy, chain letters)

While one could argue about the arrangement or topics within this framework, this site provides an excellent resource for organizing and finding content for coverage of computer ethics.

Textbooks

A search of google.com and amazon.com reveals a variety of textbooks related to computer ethics. However, there are relatively few choices for instructors who seek to teach computer ethics to information systems students. Many textbooks have become outdated, or were written by philosophers rather than business or computer professionals. Others contain relevant content but are edited collections of articles instead of an integrated textbook with a comprehensive view of the subject and lack supporting teaching resources (review questions, study guides, presentations,

exam questions, etc.). The appendix following this article contains a list of several textbooks related to computer ethics.

3. COURSE PROFILE: MBA COURSE IN ETHICS, PRIVACY, AND SECURITY

The approach to teaching information systems ethics that we have chosen in our college of business is to combine the discussion of ethical issues with those of privacy and security – privacy because it is one of the primary ethical concerns in information systems, security, because it is the way privacy is protected and ethics are implemented. The course is titled “INFO 930, Ethics, Privacy, and Security” and is offered at the graduate (MBA) level.

We begin by presenting HIPAA as the most significant example of an implementation of ethics, security, and privacy together. HIPAA, the Health Insurance Portability and Accountability Act (also known as the Kennedy-Kassebaum Act) of 1996 mandates that all medical records in the United States will be electronic by a certain date, proscribed by formula. (Currently, that date is October 10, 2003) Recognizing the importance of medical information, the vulnerability of electronically stored and transmitted information, and the ethical basis of the medical profession, the authors put provisions into the legislation directing congress to enact additional legislation defining privacy rights of citizens, particularly in relation to electronically stored and transmitted information. Security measures, based on currently-existing protocols and methods, were also proscribed, making HIPAA a model both of the interdependence of the fields of ethics, security, and privacy, and of future implementations of paperless applications for business. A brief history of privacy legislation and litigation completes this foundational section of the course.

After establishing the importance and interdependence of ethics, security, and privacy, we discuss privacy in greater detail. The legal environment, starting with The Constitution, forms a majority portion of this area. Key legislative landmarks (for example, the Privacy Act of 1974) are presented, with a view to understanding the difficulty in defining privacy, and the conflicting needs surrounding it. For example, the Privacy Act of 1974 said, in essence, that no citizen had to divulge their Social Security Number to anyone other than the IRS; the Internal Revenue Act of 1986 completely reversed that decision, compelling banks and other institutions to require the SSN of depositors for tax reporting, and opening the door for anyone asked to perform any financial transaction (for example, cashing a check) to ask for the SSN for identification. This example serves to illustrate the difficulty that the legal community has in defining a reasonable and enforceable right to privacy, while the HIPAA experience shows the

difficulty of legislating privacy, and recent experience with the Child Protection Act emphasizes the contrasting ethical dilemmas in creating privacy legislation.

One of the surprises that we encountered in our first offering of this course was the naïve attitude taken by the non-technical (those whose computer literacy is basically limited to use of prepackaged software) graduate (MBA) students toward privacy and security. Their reaction was almost unanimously along the line of, “What’s the big deal about privacy? If you’re not doing anything wrong, why should you care if someone sees your information?” To facilitate a more informed discussion of the topic, two guest speakers were engaged. The first was a network professional and self-acclaimed non-criminal hacker. He talked about, and demonstrated, how hackers can observe and intercept non-secured Internet transmissions. The second was a professional background investigator who regularly uses web-based data to do his work. His primary tool is a public database which contains the information about every person who has committed any infraction, or who has had any interaction with the county court system. Address, driver’s license number, SSN, disposition of divorce decrees – all available at the click of a mouse button. These experts and their examples of how easily privacy can be compromised over the Internet created a change in most of the students’ attitudes about privacy.

Once the groundwork for privacy as an ethical issue is established, we engage in a presentation and introduction of some of the central ethical issues, both privacy- and other-oriented, involved in the implementation and use of contemporary information systems. Those issues include:

- Who has what information and how do they use it?
- Collection and sharing of personal information in both the public and private sectors.
- Data warehousing and data mining; the creation of new information out of old.
- Data integrity, accuracy, completeness; segmentation issues.
- Identity Theft.
- Ethics as a foundation of trust for the use of knowledge management systems.
- Disinformation, misinformation, and hate groups.
- Ethics of Marketing, including the use of spam e-mail

- The current state of ethics in virtual reality
 - Colin Beardon, Faculty of Art, Design & Humanities, University of Brighton, UK: “What is the likely effect of spending an extended period in a virtual environment where it is possible to completely discount the worth of other people and to deal with them only by means of militaristic or sexual aggression?”
 - Does VR provide adequate skills training?
 - Is over-reliance on computers for training producing “blind spots” in pilots or physicians?
- The current state of ethics relating to artificial intelligence
 - Can we create A.I. that is equal to human intelligence?
 - Is it immoral to replicate the human in something that is not human?
 - Are we playing God?
 - Is that necessarily a bad thing?
 - Should we continue to try to make computers/machines smarter than humans?
 - Where do we draw the line?
- The Digital Divide and cultural differences.
- Cybersex, Cyberpornography, Child Pornography and “near” child pornography
 - On the web
 - In programs/cd-roms/games
- Games and violence, sex, and behavior modeling
 - Lack of consequences
 - Lack of intimacy
- Privacy and the government
 - The FBI, the CIA, and tools like Carnivore
 - Privacy vs. Homeland Security

- Corporate espionage

The course also examines how information systems are evolving and what ethical issues may arise in the future are also topics of interest. Some areas discussed include:

- Information systems in human genome mapping and cloning.
- Marketing via GPS.
- Virtual reality and artificial intelligence in robotics
 - The Harvard research
 - The popular view: AI, Bicentennial Man, and the “rights” of robots

The course also deals with issues regarding the protection of privacy, the support of ethical behavior, and protection from unethical behavior through security methods. Security, defined as protection of information assets based on what you have (a key, a secure token, etc.), what you know (ID, password, etc.) or what you are (biometric measures such as retinal scan, fingerprint, etc.), is presented with some level of technical rigor. We discuss authentication methods such as Kerberos, firewalls, encryption, and web security via SSL and https. Again, guest speakers are brought in to emphasize the importance of strong security. In particular, a web enforcement officer with the United States Air Force presented on intrusion detection tools and methodologies.

Finally, students are presented with an overview of the major professional societies, associations, and trade organizations dealing with the issues surrounding ethics, privacy, and security in information systems. Examples can be found on web sites from University of British Columbia’s Centre for Applied Ethics (2002) and INFOSYSSEC’s Security, Ethics, Policy and the Law site (2002).

Course work is based on readings from professional journals, trade press, and the organizations mentioned above. Students are expected to research and make a 45-60 minute presentation on one of the major topics of the course. Grading is based on the presentation, a write-up (paper) of the presentation materials one written examination, and participation through BlackBoard.

This course has been presented once, in Spring, 2002, and is scheduled to be presented again in Spring, 2003.

4. CONCLUSIONS

This topic of computer ethics is rapidly changing and draws interest from a broad variety of disciplines. As a

result, one course in the topic can be very different from another. This study provides a brief review of the various approaches that these courses can take and the resources that instructors can use to help in course delivery. We add to this diversity by providing a detailed example of a new course offered to MBA students focused on ethics, privacy, and security.

It is unlikely that we will ever (nor should we) develop a comprehensive set of topics that fits all courses in computing ethics. Nonetheless, the current state in this area is rather disorganized, making it difficult for instructors to find reliable resources and making administration of curricula related to computer ethics difficult. Thus, there is a great need for further research on pedagogical approaches to computer ethics.

5. REFERENCES

Bynum, T. W., A Very Short History of Computer Ethics, *American Philosophical Association's Newsletter on Philosophy and Computing*, Summer (2000).

Computing Ethics Resources on WWW, University of British Columbia Centre for Applied Ethics, <http://www.ethics.ubc.ca/resources/computer/inst.html> (2002)

Ethics and Law on the Electronic Frontier" offered jointly by MIT and Harvard , <http://swissnet.ai.mit.edu/classes/6.805/index.php3> (2002).

Ethics in Computing at North Carolina State University, http://www.eos.ncsu.edu/eos/info/computer_ethics/ (2002)

Ethics at Mississippi State University http://cyberethics.cbi.msstate.edu/eth_syl.html, (2002)

INFOSYSSEC Security Ethics Policy and Law <http://www.infosyssec.org/infosyssec/seceth1.htm> (2002)

ISWorld Ethics Syllabi, <http://cyberethics.cbi.msstate.edu/syllabi.htm>, (2002)

- Ethics and Computing by Kevin W. Bowyer (Editor) 528 pages ; Publisher: IEEE; ISBN: 0780360192; 2nd edition (February 15, 2001)
- Computers, Ethics and Social Values by Deborah G. Johnson (Editor), Helen Nissenbaum (Editor) 656 pages ; Publisher: Prentice Hall; ISBN: 0131031104; 1 edition (February 2, 1995)
- Computers, Ethics, and Society by M. David Ermann (Editor), Mary B. Williams (Contributor), Michele S. Shauf (Contributor) 384 pages ; Publisher: Oxford University Press; ISBN: 019510756X; 2nd edition (April 1997)
- Internet Ethics by Duncan Langford (Editor) 296 pages Publisher: Palgrave Macmillan; ISBN: 0312232799; (July 2000)
- Morality and Machines: Perspectives on Computer Ethics by Stacey L. Edgar 448 pages Publisher: Jones & Bartlett Pub; ISBN: 0763717673; 2nd edition (September 2002)
- CyberEthics: Morality and Law in Cyberspace by Richard A. Spinello 184 pages ; Publisher: Jones & Bartlett Pub; ISBN: 0763712698; 1st edition (November 2001)
- Case Studies in Information and Computer Ethics by Richard A. Spinello, Richard A. Sinello 285 pages ; Publisher: Prentice Hall; ISBN: 013533845X; 1 edition (June 26, 1996)
- Computer Network Security and Cyber Ethics by Joseph Migga Kizza 191 pages ; Publisher: McFarland & Company; ISBN: 0786411341; (October 2001)
- The Fourth Civilization- Technology Society and Ethics, Third (1999-2000) Edition by Richard J. Sutcliffe. Offered Online (<http://www.arjay.ca/EthTech/Text/>)

6. APPENDIX

Textbooks related to Computer Ethics

- Cyberethics: Social & Moral Issues in the Computer Age by Robert M. Baird (Editor), Reagan Mays Ramsower (Editor), Stuart E. Rosenbaum (Editor) 356 pages; Publisher: Prometheus Books; ISBN: 1573927902; (April 2000)