2004

Ethics In Information Systems: Student Performance In Evaluating Ethical Dilemmas

Charletta F. Gutierrez
Northern Illinois University

Recommended Citation

Gutierrez, Charletta F. (2004) "Ethics In Information Systems: Student Performance In Evaluating Ethical Dilemmas,"
Communications of the IIMA: Vol. 4: Iss. 1, Article 7.
Available at: http://scholarworks.lib.csusb.edu/ciima/vol4/iss1/7

Ethics in Information Systems: Student Performance in Evaluating Ethical Dilemmas

Charletta F. Gutierrez

Department of Operations Management and Information Systems, College of Business, Northern Illinois University, Dekalb, Il 60115 USA
(815) 753-6377, Fax (815) 753-7460, Cgutierrez@niu.edu

ABSTRACT

The explosion in information technology in the last 20 years, and in particular, data communications networks, has had a major impact on ethical thinking and ethical issues. This has been manifested in the recent accounting and business scandals, as it is becoming apparent that the ethical dimensions of information systems-related business decisions cannot be safely ignored. It is important for business educators to introduce students to relevant ethical situations that they may face in the business world. This paper discusses the Information Systems ethical environment and students performance on business ethics cases in a telecommunications course. The results of this evaluation show that more exposure to ethical situations is needed, as students are not prepared to make sound ethical judgements.

INTRODUCTION

Over the last 20 years, the progress in ethical thinking relating to information technology has not matched up with the explosion of the technology itself. This gap has manifested itself in cyberspace as well as in various Information Systems (IS) corporate initiatives aimed at improving efficiency, effectiveness or a strategic advantage for the firm. In the last three years, there has been an abundance of issues related to business ethics in the news, from the Enron scandal to the very recent case involving Martha Stewart. Additionally, the Association for the Advancement of Collegiate Schools of Business (AACSB) has been emphasizing ethics in its accreditation process. As such, ethics is a priority in many business programs. AACSB accreditation promotes continuous quality improvement in collegiate schools of business and is a voluntary program of accreditation. Therefore, Schools of Business that are AACSB-accredited or actively seeking AACSB-accreditation are looking for ways to include ethics into their curriculum. Additionally, the expanded use of Information Technology (IT) raises a variety of ethical dilemmas in business decision-making. Thus, it is important to emphasize the necessity of teaching business ethics in Information Systems courses. According to Verschoor (2003), MBA students are not sure that they are being prepared for the ethical challenges and conflicts that they may have to face in their business careers.

A discussion of previous research on ethics and information systems is presented reviewing many of the management theories of ethics as they relate to information systems. This is followed by a discussion of promoting ethics in information technology courses and the business environment, including a review of the codes of ethics and/or privacy codes of professional organizations. The paper concludes with a discussion of the how students perform on an ethics assignment.

ETHICS DEFINED

Ethics is derived from the Greek word meaning "custom." Ethics are the values and moral standards that guide an individual in his/her interactions with others. Individuals interpret ethics differently, and as such, the difference in ethics can be a hindrance especially with the expansion into global businesses and the increase of information technology and communications (Whitman, Towsend and Hendrickson, 1999). These differences in ethical values are manifested in religion, race, environment or nationality. As a matter of fact, something considered ethical to some, may be illegal, or vice versa depending on the country or environment. An example of this is the duplication of software or software "piracy". While illegal in this country, it is considered ethical in some Asian countries to duplicate software at will, and even distribute such software (Swinyard, Rinne and Kau, 1990). Another example is the ability to download music. When polling the students in a telecommunications course, very few saw a problem with this example.

IS RESEARCH INTO ETHICS

It is becoming apparent that the ethical dimensions of information system-related business decisions cannot be safely ignored. Many professional conferences and major information systems journals are placing an increasing emphasis on ethical issues (Smith and Hasnas, 1999). Various authors have addressed many subsets of IS ethics. Some by looking at behavioral patterns of various subjects who perceive actions as either ethical or unethical (Langford, 1996). While still others have developed or inferred theoretical frameworks which have guided ethical assessments in either laboratory or field settings (Cappel and Windsor, 1998; Smith and Hasnas, 1999; Walsham, 1996). In addition, increased attention is being paid to ethics in information technology curriculum, particularly in Schools of Business (Couger, 1989; Kock, 1999).

The emphasis on ethical decision-making in is has been on the evaluation of is ethical scenarios in corporate business environments. In these scenarios the decision-maker is forced to make an ethical decision not as a individual but, instead, as an agent of a corporate body. However with this in mind, it still leaves a major gap in which there are often no explicit or agreed-upon rules with respect to appropriate and inappropriate behaviors (Banerjee, Cronon and Jones, 1998; Johnson 1989, Smith and Hasnas, 1999). According to Saia (1998), ethical issues are not placed on meeting agendas, or discussed by the water fountain, but they are ever present in the advent of information systems. Even though is developments are enabling an increasing number of

corporate initiatives or efforts aimed at improved efficiency, effectiveness, or providing a strategic advantage for the firm (Cash, McFarland and McKenney, 1992), many of these developments or applications do not address ethical guidelines. This lack of ethical guidelines, as they relate to information technology within the business environment can be a hindrance especially with the global expansion of businesses.

THEORIES USED TO EXPLAIN BUSINESS ETHICS

Normative Theories of Business Ethics

According to Sankaran (2003), no unified model or framework exists for explaining or capturing all the possible factors that may influence ethics in the business world. However, the Normative Theories of Business Ethics (NTBES), created for businesses and adopted for use in Information Systems, is a group of three theories focused exclusively upon interactions that involve business relationships. NTBES allow ordinary business people to apply ethical principles expressed in business language to concrete moral problems and questions that come up in everyday business transactions (Smith and Hasnas, 1999). The NTBES define the obligations of managers and focus on what they should do to fulfill their moral or ethical responsibilities.

The three leading NTBES are the stockholder, stakeholder, and social contract theories. Each specifies a different set of responsibilities for managers, and these accounts of one's ethical obligations are usually incompatible. Thus, no more than one of them can be correct at any one time. In explaining these three theories the following business case will be incorporated.

Typically many businesses sell information on their customers and engage in what is commonly referred to as cross-marketing or cross-selling. Cross-selling means offering related items when a customer places an order, while cross-marketing means sharing information on customers with other providers, with which the company has a strategic alliance. That is, allowing business partners to target market to your customer base according to specific customer preferences. In the airline industry, companies keep records of each individual transaction in their databases. Examining the purchasing habits of consumers may allow airlines to offer specialized trips or add-ons, like car rentals or hotel stays, to increase revenues. However, this practice creates some ethical issues relating to privacy.

Stockholder Theory

According to this theory, the manager acts as an agent for stockholders. They are responsible to spend corporate funds only in ways that have been authorized by the stockholders and are obligated to maximize the financial return on the stockholders investment. The managers are socially responsible to do so, so long as it is without deception or fraud and engage in an open and free competition with other business.

The stockholder theory also obligates managers to increase corporate profitability only through legal, non-deceptive means and the stockholder theory is generally viewed as having a long-term orientation. It directs managers not to seek short-term gains at the expense of the firm's long-

term financial health but to maximize corporate profits in the long run. According to Smith and Hasnas (1999), when applying this theory, if it was the only theory governing that industry, they would not only be ethically permitted to sell the information on customers' purchases, but obligated to do so. That is, using our case of an airline, if the transaction is legal and will increase the airline's profits, management is obligated to follow through with the sale. However, because the stockholder theory is looking at long-term financial health, maybe the public view of this practice should be included in the equation. Thus, public opinion, even though intrinsic, can eventually cause a decrease in profits, if the public views the practices of the corporation as unethical.

Stakeholder Theory

The stakeholder theory focuses on the corporation's stockholders and also stakeholders. Stakeholders are individuals and/or groups that are either important to the survival and success of the corporation and/or their interests are significantly affected by the corporation. Stakeholders can be customers, employees, suppliers, vendors, and local communities. Ideally a stakeholder is entitled to participate in a corporations' decision making processes. However, it is impossible for a company to take into account every stakeholder's statements or ideas. Therefore, the manager is obligated to consider the stakeholders' legitimate interest and adopt corporate polices that will produce the optimal balance among them. While doing this, the managers have to respect and treat every stakeholder differently and equally, a very delicate balance indeed. Thus, managers must give equal consideration to the interest of every stakeholder.

Airline management must look at the particular benefits and costs that the sale will impose upon each of the stakeholders. That is, the ethical quality of the decision to sell the customers information will depend upon, the nature and intensity of the costs the sale imposes on the airline's customers, relative to the nature and intensity of the benefits it provides to the stockholders. Additionally, the benefits it provides to any strategic alliance partners who purchase the information must also be considered (Smith and Hasnas, 1999).

Social Contract Theory

This theory covers the social responsibilities of corporate managers to meet the conditions stipulated by a society or its members, as if the corporation did not exist in the first place. Some of the conditions that have to be met are to show respect for their workers as human beings, avoid any practice that worsens the situation of a given group in society (discrimination) and enhancing the society as a whole, including the environment, consumers and employees. The idea is to look at how society can be enhanced through the creation of the corporation. If society is hurt in any way then the corporation should not exist. The two most important terms to be considered under social contract theory are *social welfare* and *justice*.

Under the social contract theory, an airline should not sell the information to direct marketers because it provides no benefit to society as a whole. While the selling of the information would generate additional revenue for the airline, there is no material benefit to its' customers or employees. However, its employees may benefit from increased sales and thus, increased salaries or bonuses. In addition, it could be argued that individuals are target-marketed with only

the products that would interest them, thus, cutting down on the unnecessary information overload and reducing overall "junk mailings." However, this remains to be seen.

Agency Theory

Agency theory, while not one of the NTBES, can still be used to examine information technology and ethics. Agency theory indicates that conflicting interests and information asymmetries affect investors' and firm managers' abilities to make changes, should they want to (Eisenhardt, 1989). Agency theory addresses incentive and information problems inside and outside the firm. Agency theory is a management theory that puts the principal agent dilemma in the forefront and may be a good way to understand the software development process and how to improve it. In agency theory, one person, the principal, wants to induce another person, the agent, to do something that the agent does not want to do (Bowie and Freedman, 1992). Also, the agent has hidden information or a hidden agenda, which exists because it is hard or expensive for the principal to monitor the agent. Often in agency theory, principals and agents have different attitudes towards risk (Eisenhardt, 1989; Salani, 1997). All of these factors can create an ethical dilemma. That is, which of the agendas, either the agents' or the principals', are the best for the firm and which is best for the consumer. Agency theory can be used in conjunction with NTBES to help clarify these issues.

PROFESSIONAL CODES OF ETHICS AND GOVERNMENT STANDARDS ON PRIVACY

There has been an increasing awareness of ethical issues related to information systems among both professionals and academics. Mason, Mason and Culnan (1995), state that individuals resolve ethical questions by referring to rules and codes of ethics. These codes of ethics are grounded in principles which are then grounded in ethical theories. A number of computing professionals' organizations like the Association for Computing Machinery, Institute for Certification of Computer Professionals, the Information Technology Association of America, and the Association for Information Technology Professionals, have established formal ethical and professional codes (Walsham, 1996). An individuals' general code of ethics is a set of guidelines, usually unwritten rules, that the individual follows to judge the rightness and wrongness of what that individual sees and does. Formal policies provide guidelines for members of a particular group to follow. Furthermore, corporate codes of ethics are any written corporate statement of ethics, law, or policy that define standards, for that particular organization (Harrington, 1996).

Software Engineering Code of Ethics and Professional Practice

The IEEE Computer Society (IEEE-CS) and the Association For Computing Machinery (ACM) set up a joint task force that created general guidelines and made formal policies or rules for ethical IS practice. This effort became the Software Engineering Code of Ethics and Professional Practice (Gotterbarn, Miller and Rogerson, 1999). This code is intended as a standard for teaching and practicing software engineering. It documents the ethical and professional obligations of software engineers. In addition, it provides practitioners with

guidelines regarding the standards society expects them to meet. The code also informs the public about the responsibilities that are important to the profession.

The code of ethics has eight principle categories, with each category governing a particular part of information systems development. The code states:

"Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety, and welfare of the public, software engineers shall adhere to the following eight principles:"

1. Public: Software engineers shall act consistently with the public interest.

2. Client and employer: Software engineers shall act in a manner that is in the best interest of their client and employer, consistent with the public interest.

3. Product: Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4. Judgement: Software engineers shall maintain integrity and independence in their professional judgment.

5. Management: Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6. Profession: Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7. Colleagues: Software engineers shall be fair to and supportive of their colleagues.

8. Self: Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

In addition to the code of ethics there are a number of examples where ethics are incorporated in business. Business ethics are concerned with proper corporate and individual conduct in business situations. Since much of information technology these days seem to evolve around the internet, one of the major problems surrounding ethical issues is the exchange of data between companies and the security of such data.

Information Technology Association of America Code of Ethics and Privacy

ITAA is already a leader in privacy protection. As a founding member of the online privacy alliance (OPA) http://www.privacyalliance.org/, it is committed to protecting individually identifiable information in an online or electronic commerce environment. The principles that it suggest for the member organizations are:

Adoption and Implementation of a Privacy Policy: An organization engaged in online activities or electronic commerce has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information.

Notice and Disclosure: An organization's privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested. The policy must state clearly what information is being collected, the use of that information, possible third party distribution of that information, the choices available to an individual regarding collection, use and distribution of the collected information, a statement of the organization's commitment to data security, as well as, what steps the organization takes to ensure data quality and access.

Choice/Consent: Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to "opt out" of such use.

Data Security: Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability. Additionally, they should take reasonable precautions to protect such information from loss, misuse or alteration. They should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.

Data Quality and Access: Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used.

When looking at the above guidelines, online services should offer users an "opt-in" or "opt-out" choice, and the default should be to "opt-out." Basically this will allow users to choose whether they want their information to be included in a database that might be sold to third parties. Even though customers are "opting-out" some online companies are going against their own privacy policies and selling customer information because of the massive profits to be made. A few of the companies that have been charged for illegally selling data on their customers are Amazon.com, Toysmart, Inc. and Toys R' Us (Anonymous, 2000; Rosencrance, 2000).

Federal Trade Commission Privacy Standards

The Federal Trade Commission (FTC) has made inroads into updating legislation on privacy. Specifically, it has been instrumental in bringing forth the Gramm-Leach-Bliley Act, signed into law on November 12, 1999, which safeguards non-public personal information in financial institutions (Appraisal Foundation, 2001). According to the Appraisal Foundation (2001), the privacy regulations require that three types privacy notices must be provided to all customers. Such notices (intial notice, annual notice and opt-out notice) must be clear and conspicuous in understandable language. In addition, the FTC recently recommended the adoption of four fair infomation privacy principles (FIPPs) as the basis of new Internet legislation. These principles

are: notice, choice, access and security (Ippolito, 2001). Much of this was brought about by the Children's Online Privacy Protection Act (COPPA), which is the only legislation to cover privacy issues on all Internet Web sites (Garon, 2001).

The FTC uses the guidelines in the Health Insurance Portability and Accountability Act (HIPAA), to govern privacy and security of data. Under HIPAA, a Chain of Trust Partner Agreement must be in place with all parties that share consumers' data (Garon, 2001). Under this agreement all parties will protect the data, monitor compliance of all parties with the agreement, report all security failures to the FTC, and take any necessary steps to remedy breaches of the agreement (Garon, 2001). Futhermore, according to Dreyer (2001), the FTC is charged with establishing standards relating to the administrative, technical and physical safeguarding of customer records. These include insuring the security and confidentiality of such records, protecting against threats and hazards to the security and integrity of the customer records and finally, protecting against any unauthorized access or use of customer information which could ultimately result in substantial harm or inconvenience to such customer (Dreyer, 2001).

Cybercitizen Partnership

In 1999, Janet Reno, Attorney General in the Clinton administration, created an alliance between the public and the private sector called the "cybercitizen partnership." This alliance was formed to help support "computer ethics and civic responsibility" (MacMillian, 1999). The Justice Department and the ITAA, along with a number of other non-member ITAA companies, funded a public campaign to promote awareness on ethical behavior online. In addition, a directory of information security providers was published to aid organization in effectively protecting their data. This "cybercitizen partnership" is in the forefront of establishing a set of standards for computer ethics on the internet.

According to Smith (2002), some private firms provide guidance to employees, while others assume they employees will "do the right thing." At MCI, employees are given an ethics test which involves a fictitious employee named Julie (Pappalardo, 2004). In each situation where ethical issues are to be resolved, employees are continuously challenged to ask "What would Julie do?". At Pella Corporation, employees are put through ethics training soon after they are hired. In a survey of IS professionals, Hilton (2000) discovered that employees believed that their company's ethics guidelines were well known. However, if this is the case, the question remains "Why are there so many ethics issues in the news?" The following analysis of student performance may provide some insights to this question.

STUDENT PERFORMANCE AND ATTITUDES TOWARD ETHICS

In many examples, students are given straightforward cases of wrongdoing or negligence. According to MacLagan (2003), these cases discuss issues that seem obvious as to the right course of action. However, many of the ethical situations that the students will face in the workplace are situations similar to those encountered daily in the course of doing business (MacLagan, 2003). According to Marrifield (2003), exposure to and discussion of particular

cases allows students to project themselves into the situation, while exploring difficult circumstances without fear. Therefore, the students were given cases that required problematic situations in practice. The students were introduced to a case in which they were to consider the problem, determine if an ethical issue actually existed, and asked to provide different alternatives to avoid the ethical dilemma.

To set the stage for the ethics case, a business professional came to class and discussed the importance of business ethics. Additionally, before the students were given the individual ethics cases, they were provided with "codes of ethics" from several of the above professional organizations and given several in class ethics situations. Students taking telecommunications in the first semester were asked to consider the case of Cyber City, USA (Appendix A). Students in the second semester were given a case where Microsoft was being sued by an individual because of identity theft while using software developed by Microsoft (Appendix B).

Both undergraduate and graduate students were given the cases and required to discuss them using a threaded discussion board online. Most of the undergraduate students were MIS or Operations Management majors, with a few Computer Science majors taking the course. The graduate classes contained a much more diverse group not only in the student majors but also in background. Graduate students were from Accounting, several were MIS, and others came from Computer Science, Engineering, Marketing and general MBA.

Students were evaluated on providing constructive comments during the online discussion (individual grade) and on the final paper (group grade). The intent of the assignment was to develop critical thinking skills, while considering an ethical quandary as suggested by Marrifield (2003). Students were not graded on the outcome of the discussion, as there is not always a right and a wrong answer. However, students lost points if they never took into consideration or discussed the "codes of ethics" from any of the IT associations.

Each thread in the threaded discussion was read and evaluated by the instructor. The assignment was graded for relevant comments, non-relevant comments (i.e., 'can we meet to start the paper'), first student to post a message, first student to mention the code of ethics, best comment, and best attitude. Furthermore, students were given additional points if they participated in authoring the report. Half of the total assignment grade was given for the group report and half of the grade came from the student's individual contributions. Therefore, if a student did not contribute to the online discussion, that student could only earn a maximum of 50% of the points alloted to the assignment. Grades ranged from 49% to 110% (several students capped at the maximum grade with 10% extra credit). In addition, if a student did not participate until the day the paper was due, the comments were considered "too late to contribute." For example, one student signed in and made several comments in the 10 minutes before class started on the day the paper was due.

Cyber City Case Results

In evaluating this assignment, it was found that undergraduate students have lower ethical standards than graduate students. That is, the graduate students agreed that an ethical dilemma existed, while several of the undergraduate groups believe no ethical issue existed at all. Some

of the undergraduate students, as soon as they thought that no ethical issue existed, stopped participating in the group discussion. Such students tended to earn lower overall grades on the assignment than those students who kept an open mind and joined the discussion. For instance, these student groups commented that "technology should move forward at any cost." That is, if some are left behind because they don't have the technical knowledge or funds to obtain systems, so be it, just don't hold back the others in the community that do.

The students who believed that there was at least one ethical issue in the case, identified a minimum of four themes. These included accessibility to the network (children with parents that have access will have a clear advantage over their peers), technical knowledge imbalance, economic imbalance, and security. Security is not necessarily an ethical issue, but many groups suggested that user's personal information must be secured. Students came up with a variety of solutions for these problems. Some of these proposals were very innovative whereas others almost impossible to implement. According to the comments on one student report, "a majority of the population is low-income and don't have a lot of technical expertise or computer access, therefore, the proposal will require more adjustments before continuing." Some of the suggestions are as follows:

Training courses offered by volunteers and/or training videos/PC software.

Supply more computers at various sites so that all residents would have access.

Subsidize computer purchases or make special arrangements with businesses for donations for the needy.

Charge a fee for usage.

Make sure that an equal number of slots for children's teams are available for those with no access.

Provide a 7/24 hotline for questions/technical support and sign-up for any programs/services offered over cyber city's network.

Provide a newsletter for all citizens, describing all features and locations for access.

In regards to the security and privacy issues, students suggested that the proposed system would expose the users to potential harms such as inappropriate use of parent/teacher interactions, security of information regarding children and confidentiality of individual and organizational information. Specifically, anything can be altered during the transmission of data regarding children's school schedules, or when a business is registering for a city permit. Sensitive information will be transmitted over the internet, stored in databases and handled by city employees, therefore, the students suggested the following:

Household identification numbers and passwords should be used.

Assign different levels of access to different members of the community.

Do background checks on all employees.

Train employees in ethical issues.

Encrypt all information traveling over Cyber City's network.

Inform users of the importance of proper usage.

Install anti-virus software and firewall protection.

In meeting with guidelines from the FTC commission rulings on privacy, Cyber City should implement policies regarding the information handling and storage, as well as, provide the required privacy notices to patrons of the system.

Students cited several sections from the Code of Ethics of the ACM in their discussions. They applied the following sections from the code:

Section 1.1: Contribute to society and human well-being, "Computing professionals should prohibit the use of computing technology in ways that result in harm to any of the following: users, general public, employees and employers. In addition, they are required to make users aware of any problems that may occur due to the system."

Section 1.2: Avoid harm to others.

Section 1.4: Be fair and take action not to discriminate. "In a fair society, all individuals would have equal opportunity to participate in or benefit from the use of computer resources, regardless of race, sex, religion, age, disability, or national origin." That is, inequities between different groups of people may result from the use or misuse of information and technology.

Section 1.7: Respect the privacy of others "To ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals."

Section 2.1: Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.

Section 2.5: "Provide a comprehensive and thorough evaluation of any computer system and its' impacts, including analysis of possible risks."

Section 2.7: Improve public understanding of computing and its consequences. "Computer professionals have a responsibility to share technical knowledge by encouraging understanding of computing, including the impacts of computing systems and their limitations."

Section 2.8: Access computing and communications resources only when authorized to do so.

Section 3.4: Ensure that users and those that will be affected by a system have their needs clearly articulated during the assessment and design of requirements.

Section 3.5: Articulate and support policies that protect the dignity of users and others affected by a computing system.

Section 3.6: "Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems."

Identity Theft Results

The second semester students were asked to evaluate a case taken from the newspaper concerning legal action brought against Microsoft for identity theft. While the case against Microsoft is argued in the legal system, the students were given the responsibility of determining the ethical issues involved in the case. Several overwhelming themes emerged during the student discussions:

Many students took the stance that the suit was frivolous and just brought against Microsoft, because Microsoft has "big pockets."

Microsoft has a monopoly on much of the business software market.

Microsoft had a duty to its consumers to make their software as secure as possible.

The end-user license agreement (EULA) explains the terms of service, however users cannot read this until they have opened the product, and by then it is not returnable. EULAs have been the target of criticism on two fronts. First, because it is written in "legalize" and secondly, because it removes any liability from software manufacturers arising from the usage of such software.

Anyone using the Internet for business transactions should be aware of the dangers of identity theft.

Microsoft provides automatic patch updates and it is up to the consumer to authorize the updates and use the patches. However, the number of patches or updates in any given period is too high.

Neither party is at fault, a third party should be responsible.

Unfortunately, during the discussion, the students could not manage to get the term "legally responsible" out of their minds. However, students thought that Microsoft was ethically responsible according to the ACM's Code of Ethics, Section 1.2 "avoid harm to others." According to the students, harm as defined by this case, is injury or negative consequences, such as undesirable loss of information and loss of property. In order for Microsoft to avoid unintentional harm to users, the company must consider every possible use and abuse of their products as they make design decisions, considering all potential impacts on the users. According to one group, in the event that Microsoft's products leads to unintended negative consequences, Microsoft is ethically bound to undo or mitigate these negative consequences. Additionally, students suggested, that at the time of release, if Microsoft was either aware of or to later learn of any security problems with their products then they are ethically obligate to

develop a solution to the problem. Furthermore, Microsoft must make sure the solution can be understood and implemented by all users and that the solution is accessible to all users. They commented that maybe the release of the products is premature, without the required testing.

Another problem with this case was that several students took either a pro-Microsoft or an anti-Microsoft stance. It was not the intent of the case to address student opinions of the company, and thus, guiding the students to the ethical issues was a constant challenge. However, in the end the students believed that both sides were ethically irresponsible, Microsoft for not properly testing the software and warning customers of the security vulnerabilities. And the plaintiff for looking for restitution from the wrong party, while not having the proper training in the use of the Internet and the products for online business transactions. One student put it this way, "unfortunately, when ethics is the issue people tend to ignore the end-user side of the story, focusing solely on the side with money. So who is being ethical here?"

In addition to the obvious parties as described above, the students identified a third responsible party, the owner of the Web site where the plaintiff was doing business. Students noted that, using the ACM code of ethics, "it is the responsibility of computer professionals to maintain the privacy and integrity of data describing individuals." Therefore, students didn't believe that the Web site developers took the proper precautions to ensure the accuracy of the data, as well as, protecting it from unauthorized access. Furthermore, students commented on "what about the hacker", this is where is the ultimate responsibility lies.

Overall Results

Students had mixed feeling about having an ethics case in a telecommunications course. The undergraduates particularly did not see the relevance of the cases, particularly the Cyber City case. This was a major factor in using the Microsoft case for the second semester students. By using a real case rather than a hypothetical case, students seemed to relate more to the issues. Many undergraduates just took the stance that no ethical issues were present and didn't bother to discuss the cases. Graduate students put forth more effort and thought into the case reports and ultimately gained valuable insights into some ethical dilemmas that may emerge in the work environment. However, one issue with the Microsoft case was that students couldn't seem to get past the legal issues. Therefore, a number of the student papers focused on the legal responsibilities rather than the ethical issues of the case. Additionally, in the Microsoft case none of the groups looked into the FTC rulings of privacy, specifically the Chain of Trust Partner Agreement, requiring that all parties protect the users data and report all security failures.

CONCLUSION

In this paper, several theories with respect to ethical behavior and information technology have been reviewed. Which of these should be used in any given situation is up to the individual. Many professional organizations have adopted some form of ethical and/or privacy standards, as have many private companies. However, many members do not follow those standards. Business students, especially those in the undergraduate program, do not seem to have a firm grasp of what to do in ethical situations. However, the graduate business students are able to

identify the issues more thoroughly, even if they are not able to focus on just the ethical situation. Ethical dilemmas are confusing for business students. Therefore, it is up to business educators to help students work through such dilemmas by enhancing courses with everyday cases and relevant practice scenarios.

APPENDIX A

THE CASE OF CYBER CITY'S NETWORK

The city council of Cyber City, USA, is debating a new program, the Cyber City Network (CCN). This service would allow residents access to a wide variety of municipal and school services from their home computers. If the program is approved, residents will be able to scan the city's job listings, apply for building permits, ask questions of the police department, or get their children's homework using the Internet.

City council agendas would be posted, and citizens could testify at council meetings from offsite computers. Recreation department schedules would be available on the network, and parents could register their children for city sports teams on-line. In addition, parents could also communicate with teachers through e-mail and a electronic bulletin board system. Businesspeople who require city permits and licenses could apply for them via the CCN.

Only about one-fourth of Cyber City's 60,000 residents own computers equipped with modems, which would allow them to log on to the network from their homes. DSL and cable modems are not available at this time in Cyber City. In addition, there is a large number of low-income, as well as, non-technical families living in Cyber City. The city has promised to provide a limited number of additional computers (3 at each location) at elementary schools, senior citizen centers, and libraries for those who do not have access at home.

Please identify the ethical implications, if any, of this proposal. If ethical implications exist, identify appropriate alternative measures to remedy such concerns.

Source: http://www.nd.edu/~rbarger/cybercity-cse.html

Copyright (c) by Thomas Shanks, S.J., 1996. Dr. Shanks is director of the Markkula Center for Applied Ethics, Santa Clara University. Modified by: Charletta F. Gutierrez, 2003.

In your assigned groups, discuss on-line the problems and concerns identified in this case. Members will be graded upon their participation and the suggestions discussed.

During the discussion, identify the ethical issue(s)/problem(s) and provide at least four (4) alternatives to solving each problem.

Each group will turn in a written summary of the group's discussion, including:

Each ethical issue should be identified together with the alternatives to each, whether, pro or con.

Your group's recommendation(s) and whether Cyber City should continue with the plans to build the CCN or suggest an alternate plan.

APPENDIX B

THE CASE OF THE MICROSOFT AND SECURITY

A Los Angeles woman has filed a lawsuit against Microsoft over security holes in the company's software. The lawsuit is asking the court to certify the action as a class action suit. At issue is an accusation against Microsoft that is commonplace among the company's opponents. The plaintiff, Marcy Hamilton, a film editor, charges that because of shoddy workmanship by Microsoft she became a victom of identity theft. She says her social security number and bank information were stolen online, and she was required to do significant work to fix the problems caused by the thieves. Her financial information was compromised and bank accounts were either compromised or seized to the extent that law enforcement became involved. The Microsoft software was not identified (in the original article), however it should be noted that the software was used by the plaintiff during an online business transaction over the Internet.

Microsoft responded that it would actively defend itself against the lawsuit. A spokesperson for Microsoft stated that Microsoft certainly takes responsibility for its software and recognized the need to build more secure software. The spokesperson also noted that security is a top priority for the company ant thus there is a commitment to build the most secure software possible.

Hamilton's lawyer, Dana Taschner, said that Microsoft advertised that its software is extremely secure. In addition, consumers don't have any practical choices other that using Microsoft products. Furthermore, consumers are not well-informed of the dangers of using these products. Vulnerabilities, patches and other workarounds are well-known to computer professionals, but not to consumers.

Even though this is a legal issue (it may not make it through the court system), identify the **ethical** implications, if any, of this case. If ethical implications exist, identify appropriate alternative measures to remedy such concerns. Identify all parties that may have some responsibility.

Case based on source: http://story.news.yahoo.com/news?story2/cmp/2031004/ Techweb Oct. 07, 2003. It is your responsibility to find additional information about the case.

In your assigned groups, discuss online the problems/concerns identified in this case. Members will be graded upon their active participation in the discussion and the suggestions discussed.

During the discussion, identify the ethical issue(s)/problem(s) and provide at least four (4) alternatives to address each problem identified.

Discuss the professional "code of ethics" handout, and describe why any of the specific items in the codes may apply to the Microsoft case and what you as a member of the profession should take into consideration if asked to participate in the decision making.

Each group will turn in a 5 page (double-spaced) written report of the group's discussion, including: a) each ethical issue identified and the alternatives to each, whether, pro or con. a) recommendation(s) for Microsoft and the plaintiff and what steps should taken.

REFERENCES

Anonymous, (2000). Amazon.Com and privacy: Amazon's change of policy. September 2000. Http://Www.Junkbusters.Com/Ht/En/Amazon.Html

Appraisal Foundation (2001). The Appraisal Foundation white paper: Privacy regulation and the appraiser. June 2001, https://www.appraisalfoundation.org/html/PDF-Images/ASBPrivacyGuidance.pdf pulled June 14, 2004.

Banerjee, D., Cronon, T.P. And Jones, T.W. (1998). Modeling It ethics: A study of situational ethics. *MIS Quarterly*, *22*(1), 31-60.

Bowie, N.E. and Freeman, R.E. (1992). *Ethics and Agency Theory: An Introduction.* New York: Oxford University Press.

Cappel, J.J. and Windsor, J.C. (1998). A comparative investigation of ethical decision making: Information Systems professionals versus students," *The Data Base for Advances in Information Systems*, *29*(2), 20-34.

Cash Jr., J.I., McFarland, F.W. and McKenney, J.L. (1992). *Corporate Information Systems Management: The Issues Facing Senior Executives.* 3d Ed. Homewood, Il: Irwin, 1992.

Couger, J.D. (1989). Preparing IS students to deal with ethical issues. *MIS Quarterly*, *13*(2), 211-218.

Dreyer, T. (2000). A lawyer's guide to privacy under G-L-B http://www.complianceheadquarters.com/Privacy/Privacy_Articles/a_lawyer_s_guide_to_privacy_un.html pulled June 14, 2004

Eisenhardt, K.M. (1989). Agency Theory: An assessment and review. *Academy of Management Review 14*(1), 57-74.

Frand, J. (1996) http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

Garon, J.M. (2001). New regulatory definitions may change the business you thought you were in. *Interface Tech News*, http://www.gcglaw.com/resources/tech/interface.html pulled June 14, 2004.

Gotterbarn, D., Miller, K. and Rogerson, S. (1999). Computer Society and ACM approved Software Engineering Code of Ethics. *Computer*, (October) 84-88.

Harrington, S.J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly*, *20*(3), 257-278.

Hilton, T. (2000). Information Systems ethics: A practitioner survey. *Journal of Business Ethics, 28*(4), 279-284.

Information Technology Association Of American, (1992). Privacy Policy. http://www.ITAA.org/about/privacymem.htm

Ippolito, P.M. (2001). Current issues at the FTC: Privacy, subprime lending, and marketing violence to children. *Consumer Interests, 47*, http://www.consumerinterests.org/public/articles/Ippolito--Current_Issues.pdf pulled June 14, 2004.

Johnson, D.G. (1989) A framework for thinking about computer ethics. In J. Robinett and R. Barquin, Eds. *Computers and Ethics: A Sourcebook for Discussions*. Ny: Polytechnic Press, 26-31

Kock, N.F. (1999). A case of academic plagiarism," *Communications of the ACM, 42*(7), 96-104.

Langford, D. (1996). Ethics and the Internet: Appropriate behaviour in electronic communication. *Ethics and Behavior, 6*(2), 91-106.

MacLagan, P. (2003). Varieties of moral issue and dilemma: A framework for the analysis of case material in business ethics education. *Journal of Business Ethics, 48*(1) November, 21-32.

MacMillian, R. (1999). Justice Department gives $300,000 to ITAA for alliance. *Newsbytes*, March 15, 1999.

Mason, R.O., Mason, F.M. and Culnan, M.J. (1995). *Ethics of Information Management*, Thousand Oaks, Ca: Sage Publication.

Merrifield, M. (2003). Teaching right from right. *Baylor Business Review, 20*(1) Spring, 10-14.

Pappalardo, D. (2004). Do the right thing, MCI style. *Network World, 21*(7) February 16, 2004, 1, 16.

Rosencrance, L. (2000). Sharing of personal data by Web sites sparks new privacy controversy. *Computerworld*, August 1st. 2000 Http://Www.Computerworld.Com/Cwi/Printer_Friendly_Version/Frame/0,1212,Nav47_Sto47902-.00.Html

Saia, R. (1998). What would you do?: Ethical dilemmas and ethical decisions. *Computerworld*, March 16th, 1998, 64-65.

Salani, B. (1997). *The Economics of Contracts: A Primer*. Cambridge, Massachusetts.

Sankaran, S. and Bui, T. (2003). Ethical attitudes among Accounting majors: An empirical study. *Journal of the American Academy of Business, Cambridge, 3*(1/2 September), 71.

Smith, H. J. (2002). Ethics and Information Systems: Resolving the quandaries. *Database for Advances in Information Systems, 33*(3), 8-22.

Smith, H.J. and Hasnas, J. (1999). Ethics and Information Systems: The corporate domain. *MIS Quarterly, 23*(1), 83-102.

Software Engineering Code of Ethics and Professional Practice, Copyright © 1999 by the Institute of Electrical and Electronics Engineers, Inc. and the Association for Computing Machinery, Inc.

Swinyard, W.R., Rinne, H. and Kau, A.K. (1990). The morality of software piracy: A cross-cultural analysis. *Journal of Business Ethics, 9*(4), 655-664.

Verschoor, C.C. (2003). Is ethics education of future business leaders adequate? *Strategic Finance, 85*(2), 20,23.

Walsham, G. (1996). Ethical theory, Codes of Ethics and IS practice. *Information Systems Journal, 6*, 69-81.

Whitman, M.E., Towsend, A.M. and Hendrickson, A.R. (1999). Cross-national differences in computer-use ethics: A nine-country study. *Journal of International Business Studies, 30*(4), 673-689.