SELECTED FACTORS IN STUDENT EVALUATION OF ETHICAL AND LEGAL ACTIVITIES RELATED TO COMPUTER USAGE

Richard Aukerman, Texas A & M University at Kingsville, rickaukerman@hotmail.com
Dennis L. Mott, Oklahoma State University, dmott@okstate.edu

ABSTRACT

Student attitudes about the ethics and legality of various internet-related activities appears to be quite diverse. This project determined student beliefs about selected activities. The data were then analyzed to establish if a relationship exists between student background and attitude about those selected activities.

Keywords: Ethics, computer crime

INTRODUCTION

Can (or should) professors include the teaching of ethics as an integral aspect of the educational experience? As early as 1867, Robert E. Lee, then President of Washington College (now Washington and Lee University) in Virginia, stated in a letter to Professor J. B. Minor that "Education embraces the physical, moral and intellectual instruction of a child from infancy to manhood." (1)

Professional educators generally agree that there exists a need for determining the beginning basis (knowledge, skill, understanding, etc.) of our students--if we wish to ultimately help them advance from knowledge point "A" to knowledge base "B" as shown by the frequent application of the pretest-posttest concept. Knowledge of student beliefs related to the legality and morality of various uses of the computer assist in determining how students value various computer activities. The purpose of this study was to determine whether or not selected demographic items could be considered as determining factors in student beliefs about the legal and ethical use of computers.

Student Discussion Scenario

A computer science graduate student decided to demonstrate the inadequacies of internet security. This student released a worm designed to spread while drawing little attention to itself. However, it replicated faster than expected. As a result, many computers crashed. The student then sent an e-mail message with instructions for killing the worm and preventing re-infection. The message could not get through because of a clogged network, caused at least partially by the panic related to the worm. This negatively affected 6,200 computers at universities, military sites, and medical research facilities. The costs of repair exceeded $98 million. (2)

Do college students think this activity was illegal? Do they think it was morally wrong (unethical)? Or do they perhaps believe it was a good way to prove the point: a lack of security on the internet?

The use of this scenario for a class discussion found some students pointing to the relatively small number of computers affected as a factor to consider. Some indicated a belief that the creation and release of the worm was unethical, but would only reach the level of illegality if a greater number of computers had been harmed.

At that time, it was indicated that the case being discussed was an actual event and that it had occurred in 1988. The amount of damage this would cause in 2002 would probably be exponentially greater. The students were asked if this additional information changed any opinions. The discussion of this issue showed that student opinions with respect to ethical versus unethical, legal versus illegal, and acceptable versus unacceptable behavior for computer usage varied greatly and were strongly held values.

WHAT CONSTITUTES A COMPUTER CRIME?

The United States Department of Justice states that computer crime is any illegal act for which knowledge of computer technology is essential for either its perpetration, investigation, or prosecution. (2) Of course, this presupposes knowledge of whether or not an act is illegal.

On February 8, 1999, a Sheriff in North Carolina pled guilty to wiretapping and recording a high school teacher's telephone calls, which the teacher made from his home on a cordless phone. The case was prosecuted by a North Carolina Assistant United States Attorney and a Trial Attorney for the *Computer Crime & Intellectual Property Section, Criminal Division of the United States Department of Justice.* (5)

On December 9, 1999, a federal grand jury charged Kent Aoki Lee with selling Viagra over the Internet without a prescription. Lee was also charged with wire fraud and trademark violations growing out of his operation of a separate pirated Internet website. (4)

On February 8, 2000, Jay Cohen was convicted in Manhattan federal court of operating a sports betting business that illegally accepted bets and wagers on sporting events from Americans over the Internet and telephones. Cohen is the first defendant to stand trial in a serried of Internet offshore sports gambling cases that were the first prosecutions brought under the federal Wire Wager Act. (3)

On January 29, 2001, two South Carolina residents were charged in a federal indictment with trafficking in luxury goods (Rolex, Cartier, and Tag Heuer watches, Mont Blanc pens, and Oakley sunglasses) that bore counterfeit trademarks, in violation of Title 18, United States Code, Section 371, the federal conspiracy statute, and Section 2320, the trademark infringement statute. (7) On March 6, 2001, a guilty plea was entered. *Assistance in prosecuting the case was provided by the Computer Crime and Intellectual Property Section, Criminal Division of the United States Department of Justice.* (6)

What do these four examples of government prosecution of computer-related crimes have in common? They are all cases that may not have been prosecuted successfully prior to the

enactment of federal laws regarding computer crime. After all, one of the primary concerns of prosecution of computer crimes prior to federal legislation was jurisdiction.

Assistance in investigating and prosecuting these cases was provided by the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice. CCIPS was founded in 1991 as the Computer Crime Unit, and became a section of the Section of the Department of Justice in 1996. The staff includes about two dozen attorneys who focus exclusively on the issues raised by computer and intellectual property crime.

The internet has had a major impact on the concept of computer crime because some acts are solely a product of the internet. For example, a domain name that was originally used by a religious organization was given up when the group decided to no longer maintain a web site. The domain name was then sold to an international organization promoting pornography. Many users were unaware of the change and were quite shocked when they attempted to access the religious materials! When this scenario was introduced during an academic discussion of computer ethics, it immediately generated a discussion of whether this constituted a crime, was unethical behavior, or was simply an acceptable business transaction.

These are examples of situations that caused the researchers to attempt to determine if there was a consistency of background that resulted in specific evaluations of activities as illegal, unethical, or ethical.

RESEARCH QUESTION

This research is an attempt to determine what, if any, role student background plays in the classification of an activity as:
>   a.   illegal versus legal
>   b.   unethical versus ethical

Students were asked to evaluate 30 activities as either illegal, legal but unethical, or ethical. They were also able to indicate if they did not know what an activity involved and therefore could not evaluate it.

Each student was asked to indicate current major, selecting from management information systems, business but not management information systems, and non-business. They also indicated an age range, sex, and whether or not they had completed a course in business law. These demographic data were then statistically assessed to determine any relationship to the selected evaluation (illegal, unethical, ethical) of each of the 30 activities on the list.

FINDINGS

The three primary groupings of respondents were
>   1.   MIS majors,
>   2.   business majors other than MIS (referred as non-MIS), and
>   3.   non-business majors.

The respondents were also divided by sex for all groups except non-business majors. The number of non-business majors responding was too small for this breakdown to be of any statistical concern. Only four of the activities included on the questionnaire will be discussed in this paper.

SPAMMING

The first item on the questionnaire asked for an evaluation of spamming. Nearly 40% of all non-MIS majors responded that they did not understand the term. Of those who understood the term, 54.5% felt it was unethical. Two-thirds of the non-business majors claimed to understand the term, and 80% of them felt the activity was unethical. Eighty-two percent of the MIS majors understood the term and 60% of those considered spamming an unethical activity. Thus, non-business majors overwhelmingly believe that spamming is unethical. Business majors and MIS majors agree that spamming is unethical, but at a significantly lower rate.

SENDING PERSONAL MESSAGES VIA E-MAIL

An interesting situation arose with respect to the issue of sending personal messages via company e-mail. Sixty percent non-business majors felt that it was unethical to send personal message via company-email while only 33% felt it was ethical. Among business majors, 52% of the females and 46% of the females thought it was unethical, while 32% of the females and 42% of the males felt it was ethical. Looking at female MIS majors, 44% considered it an unethical practice, while 50% said it was ethical. Among males, 36% considered it unethical and 32% considered it ethical. Interestingly, 24% of male MIS majors had no opinion about this issue.

SELLING INFORMATION ABOUT REGISTERED USERS

Selling information about registered users also showed some differences between the groups. 60% of the non-business majors considered that to be an unethical activity while only 13% thought it was illegal. 56% of the business majors thought it was illegal, with another 40% considering it unethical. Among MIS majors, 40% considered the activity illegal and 42% thought it was unethical. It is interesting to note that approximately 50% of the business and MIS majors thought it was illegal to sell information about registered users, while a very small percentage (13%) of the non-business majors considered it to be an illegal activity.

BROWSING THE INTERNET WHILE AT WORK

The activity of browsing the internet while at work showed some interesting differences of opinion. 47% of the non-business majors and 42% of the MIS majors felt the activity was unethical, while 62% of the business majors considered it unethical. Interestingly, 18% of the MIS majors registered no opinion about this activity. One reason this result may be considered unusual is that both MIS and business majors are housed in the college of business administration.

ON-LINE SALE OF REPRODUCTIVE EGGS

Using the internet for the sale of reproductive eggs was a "hot" news item for a while. It was interesting to note that the gender of the respondent seemed to play a major role in the opinion expressed about this issue. Female MIS majors and business majors considered it unethical at a 56% rate. Another 25% thought this was an illegal activity. Twenty-seven percent of the males in these two groups also thought the activity was illegal. However, 40% considered this to be an unethical activity. Although the non-business majors were not categorized by sex, as a group only 27% considered the on-line sale of reproductive eggs to be unethical.

CONCLUDING REMARKS

On those issues where there was general agreement regarding the legality of an activity but a difference of opinion with respect to its ethics, in almost all instances a higher percentage of the females classified the activity as unethical. There was no consistency of agreement or disagreement among the three groups of MIS majors, business majors, and non-business majors. This limited study seems to imply that female students have higher ethical standards than male students. The relative lack of agreement about the status of many internet activities also seems to indicate that unless, or until, society in general reaches agreement about ethical uses of the internet, any attempts to teach ethical uses of the internet would only be the imposition of the standards of belief held by each specific instructor.

REFERENCES

1.   Fellman, M., (2000) *The Making of Robert E. Lee*, New York: Random House, Inc.

2.   Ferrera, G. R., Lichtenstein, S. D., Reder, M. E. K., August, R., and Schiano, W. T. (2001) *Cyberlaw: Text and Cases.* Cincinnati: South-Western College Publishing.

3.   Jay Cohen Convicted of Operating An Off-Shore Sports Betting Business That Accepted Bets from Americans over the Internet. U.S. Department of Justice Press Release, February 28, 2000. Retrieved February 27, 2002 from http://www.cybercrime.gov/cohen.htm

4.   Kent Aoki Lee Charged by Federal Grand Jury with Wire Fraud, Trademark, Violations, and Selling Viagra Over the Internet Without a Prescription. U.S. Department of Justice Press Release, December 9, 1999. Retrieved February 27, 2002 from http://www.cybercrime.gov/kaokilee.htm

5.   North Carolina Sheriff Pleads Guilty to Illegal Wiretapping High School Teacher's Phone Calls. (n.d.). Retrieved February 27, 2002 from http://www.cybercrime.gov/sheriff.htm

6.   Operators of www.fakegivts.com Web Site Plead Guilty to Selling Counterfeit Goods Over the Internet. U.S. Department of Justice Press Release, March 7, 2001. Retrieved February 27, 2002 from www.cybercrime.gov/Dipadova_plea.htm

7.   Two Indicted and Arrested in South Carolina for Trafficking in Counterfeit Luxury Goods over www.fakegifts.com Web Site. U.S. Department of Justice Press Release, January 29, 2001. Retrieved February 27, 2002 from www.cybercrime.gov/fakegifts.htm