Ethics and Information Technology **5:** 49–61, 2003.

Trends and patterns among online software pirates

Sameer Hinduja*
School of Criminal Justice, Michigan State University, 560 Baker Hall, East Lansing, MI 48824-1118
E-mail: hindujas@msu.edu

Abstract. Computer crime on the Internet poses a significant threat to the well-being of businesses and individuals, and none are immune from the repercussions that can result. One type of this unethical and unlawful activity is online software piracy. In this work, the significance of piracy as a topic for academic inquiry is first presented, followed by a summary of the conflicting stances on this issue. Then, a review of scholarly literature previously conducted in this area is given to provide a backdrop for the current research. Univariate and bivariate findings from a quantitative study of students are used to demonstrate the incidence, scope, and associated correlates of Internet piracy in a university setting. Technological and ethical policy solutions that an institution might implement are suggested and discussed in conclusion.

Key words: academic, business, computer, copyright, ethics, intellectual property, Internet, piracy, software, students, university

Introduction

For two decades, information technology has progressed exponentially, and most Americans have seen computers become a vital part of their daily lives (International Review, 1994; Sieber, 1998). Computers benefit us individually as well as collectively. Not only are they used extensively to perform the industrial and economic functions of society, but are also utilized to accomplish many tasks upon which human life itself depends (e.g., medical treatment and air traffic control) (International Review, 1994). With these prosocial benefits of the technology have come a variety of antisocial consequences, particularly in recent years. To be sure, unethical and criminal activity involving computers has existed for some time. We have witnessed an explosion in the frequency and variety of such miscreance, however, with the burgeoning of the global networked environment. A computer can be the subject of a crime by being stolen or damaged; the site of a crime, such as when a child is solicited for sex in a chat room; or the instrument of a crime, such as when it is used to store information illegally (Friedman and Bissinger, 1997). Other forms of computer criminality include the propagation of copyright infringement through software piracy, Internet fraud and marketing scams, identity theft, the creation and transmission of child pornography, and the compromise of network security by hackers (Denning, 1996; Jefferson, 1997; Wolf and Shorr, 1997).

The current study focuses on software piracy by university students – specifically with regard to its occurrence over the Internet, as opposed to the duplication and dissemination of software on physical media such as floppy disks and CDROMs. First articulated are reasons why software piracy is deserving of academic inquiry and consequent policy response. A summary of the various types of software is then given to provide an understanding of this form of intellectual property. Next is presented a brief overview of extant copyright law, which serves as the platform for those individuals who consider it unethical and illegal. The opposing views and notions of those who condone participation in software piracy are subsequently provided to depict the controversial nature of the subject matter. A review of prior piracy research then follows, along with a description of the scope, objective, and methodology of the current work. The relationship between online software piracy and independent variables measuring demographic characteristics, proficiency of Internet use, and variety of Internet use is then statistically examined. Finally, technological and ethical policy solutions to aid in combating the activity are recommended.

The significance of piracy

There are a host of reasons why this phenomenon merits the attention of academics and researchers. To a notable extent, piracy by students can prove quite detrimental to universities in many ways. For instance,

* Sameer Hinduja is a doctoral candidate in the School of Criminal Justice at Michigan State University. His research interests include computer crime, corporate security, and criminological theory.

litigation can arise as software manufacturers seek to thwart the theft of their commercial product. Aside from financial considerations, the negative publicity that can ensue from this situation is often more damaging than a monetary loss (Rahim, Seyal and Rahman, 1999). Additionally, an increase in software prices by corporations to compensate for lost revenues is likely to result from the unauthorized duplication of software.

Another relevant issue is endemic to the study population of this paper (further described below) – if students are not sanctioned for unlawful computing behavior, it is presumed that the behavior will continue when they leave the relatively sheltered milieu of higher education and venture out into the working world – where it is seemingly more difficult to inculcate moral principles. University students are targeted for analysis and subsequent policy application because school is where honorable ethical values must be instilled and strengthened. Piracy undermines the integrity of the educational institution in which it takes place. The failure to satisfactorily address piracy and generate in students an internal insistence on ethical computing behavior may be misperceived as a condoning or even a silent endorsement of the activity. This particular discordant value may then be reinforced and incorporated outside of an academic environment upon graduation.

Finally, perhaps software piracy will inevitably precipitate additional forms of unethical and unlawful computer and network usage, such as the sale of bootlegged copyright material, hacking, Internet stalking, and even dabbling in child pornography. While it may seem that downloading a few programs to one's computer without paying for them cannot be equated to – and is not indicative of – an inclination towards seedier behavior, the existence (or lack) of a correlation remains to be determined and warrants analysis in future longitudinal studies. These factors collectively underscore the importance of studying software piracy among university students in order to effect the development of initiatives to curtail its salience.

Varieties of software

Software products can be classified into two groups: public domain software (shareware and freeware) and commercially-produced software. Shareware products allow individuals to copy and distribute an evaluation version of the program, but demand payment of a registration fee from those who deem it suitable for use after a specified "trial" period (Classification of Software, 1999). Freeware products allow individuals to copy, distribute, modify, reverse-engineer, and develop derivative works as long as they are not sold for commercial profit and remain designated as freeware (Classification of Software, 1999). Commercially-produced software are what most computer users are familiar with, where a license to use the program is purchased from the manufacturer through retail channels prior to installation of the application or game. Shareware, freeware, and commercially-produced software are protected by copyright law aside from the stipulations specified above.

The form of software theft analyzed by this work in a university setting includes the act of transferring:

1. Unauthorized "full-version" software
2. Serial numbers for registering shareware
3. "Keygens" (Software Key Generators) – also for registering shareware
4. "Cracks" (small executable files to modify program code in shareware and consequently unlock "full version" capability)

These files – informally known as "warez" – are available on various web and archive sites and in the personal collections of some Internet users, and accessing and executing them constitute software piracy.

Conflicting positions

Whether the act of software piracy deserves a deviant identity has been contended for years. Copyright law presents a seemingly incontrovertible position, but collectives of critics loudly assert a conflicting argument. Each stance is briefly presented here to serve as a backdrop for the current research. It appears evident that the disagreement is not with the legal definition of software piracy, but with various philosophies concerning the distribution of intellectual property. Legislation governing these products is ostensibly unassailable, but this has not discouraged dissenters from championing beliefs and assumptions in support of their perspective.

Copyright law

All creative works with which we are traditionally familiar – such as academic papers, books, songs, trademarks, slogans, images, motion pictures, paintings, and sculptures – are the exclusive intellectual property of their author – the copyright owner. While the digital duplication and dissemination of intangible property is a relatively new phenomenon stemming from thriving Internet capabilities, it does not fall outside the bounds of relevant legislation. Copyright protection laws stipulated in the United States protect software from the point of its inception, and are

primarily in place to guard against misappropriation by others and to encourage and reward innovation.

Copying software without appropriate authorization is a violation of the Copyright Act of 1976 (17 U.S.C. §106), as amended by the Computer Software Act of 1980, which grants exclusive rights to reproduce, distribute, and modify programs to the authors of the package (Im and Koen, 1990; Im and Van Epps, 1992a; Peace, 1997). The law protects these rights for a lifetime plus 50 years for individuals and plus 75 years for corporations. To reiterate, only the copyright owner can reproduce, distribute, and create derivative works of the software, and has the exclusive right to authorize others to do so (The Copyright Act and Fair Use, 1999). Three exceptions occur – the first allowing for the program to be copied onto the purchaser's hard drive for use (allowing faster access time and convenience as compared to running the program from the floppy disk or CD), and the second providing the right to make a copy for archival purposes (Ellis, 1986). The third exception, the doctrine of "fair use", allows a user to duplicate the program or copyrighted work for educational or research purposes such as criticism, news reporting, teaching, or scholarship, as long as the program is not used for profit and its potential value is not negatively affected (Ellis, 1986; Im and Koen, 1990; Im and Van Epps, 1992a).

Another legal mandate, aside from the aforementioned intellectual property protections, falls under Title 17 of the United States Code and is commonly referred to as the "shrink-wrap law". It states that once the purchaser breaks the seal of a software package, s/he has, in effect, accepted the terms of the license and must abide by its directives (Im and Koen, 1990; Peace, 1995; Software Piracy and U.S. Law, 1998). Much like the Computer Software Act, these terms state that the software has only been *licensed* for use and that *ownership has not been transferred*; that the product must only be installed and used on one computer system; that duplication, distribution, and modification is expressly forbidden; and that any warranty protection is thereby disclaimed (Im and Koen, 1990; Im and Van Epps, 1992a).

Copyright infringement may render the perpetrator liable for damages incurred by the copyright owner and/or statutory damages resulting in fines for every instance of piracy (Malhotra, 1994a; Peace, 1995). If the infringement was performed for pecuniary gain, the fines can increase up to $250,000 and five years in prison (Peace, 1995). Two other legal mandates are worthy of mention. The No Electronic Theft (NET) Act was signed into law in December 1997, and allows for criminal punishments in addition to civil penalties to be doled out to those who pirate software even if a profit motive is absent (Software Piracy and U.S. Law, 1998; Warez, 1998). In December 1999, the Digital Theft Deterrence and Copyright Damages Improvement Act was approved, increasing the penalty for intellectual property theft such as software piracy from $100,000 to $150,000 per infringement (Press Release, 1999).

Piracy rationalizations

Many justifying defenses can be asserted by those desiring to pirate software. In a theoretical piece on this phenomenon, Hinduja (2002) asserts how techniques of neutralization can be employed by software pirates to reduce stigma and normalize unethical and illegal behavior. Some of these techniques include blaming the relatively high prices of software for inducing their misappropriation, or faulting the greedy profiteering motives of software corporations. Perceiving the situation and circumstances in this way, then, unbridles the individual from any ethical harnesses, freeing him or her to participate in the activity. Denying that fiscal harm is exacted upon a manufacturer through the sporadic copying of software is also a cognitive mechanism which can be used as a justification. In addition, the intangible and remote characteristics of a software company on the Internet renders difficult the identification of an actual "victim". Moreover, the boundless nature of cyberspace often preempts any formal or informal repercussions from befalling software pirates. These factors likely contribute to an increased incidence of pirating behavior.

Other proponents of piracy argue that software creators who fail to implement copy protection schemes actually *deserve* to have those vulnerabilities exploited or "cracked". Additionally, pirating software for a "higher" purpose, such as earning better grades, helping a friend, or supporting the cause of a group is another means to normalize the unethical activity (Hinduja, 2002). Finally, many of those who endorse piracy also subscribe to the notion that "information should be free". The rationalization for this mantra is that the free-flowing exchange of information and programs stimulates progress by allowing others to modify and improve upon what has previously been created, rather than develop programs from the outset. The Free Software Foundation (FSF) is one such organization that advocates these principles, and is dedicated to eliminating restrictions on the copying, redistribution, understanding, and modification of computer programs (What is Free Software, 1999). These justifications attest to the fact that specific ethical guidelines concerning propriety in the use of information technology resources are sorely lacking, or are largely impotent. This dearth or ineffectiveness

of ethical boundaries appears to facilitates the liberation of an individual from constraining formal and informal norms of propriety. As a result, the prevalance of software piracy is conceivably augmented.

Prior research

Many of the previous studies conducted in the Management Information Systems, Business Ethics, and Organizational Management fields have sought to elicit a profile of the individual most likely to engage in software piracy. Some consistencies among demographics are worthy of note: pirates tend to be male, younger, and comfortable and experienced with computer systems (Rahim, Seyal and Rahman, 1999; Sims Cheng, and Teegen, 1996; Solomon and O'Brien, 1990; Wood and Glass, 1995). Other studies contradicted the legitimacy of such trends in demographics by determining that these individual and personal variables are not influential factors in piracy participation (Harrington, 1989; Sacco and Zureik, 1990; Wong, Kong and Ngai, 1990). These works were solely based on the duplication of software on floppy disks, and did not consider piracy conducted over a network connection.

Other items included as potential predictors of software piracy in previous research include parental income, geographical location of the educational institution, type of institution, faculty remarks, and the presence and awareness of copyright laws. Christensen and Eining (1991) studied the effects of computer attitudes, material consequences, peer norms, socio-legal attitudes, and affective factors on pirating behavior, and found that individual perceptions concerning computers and the benefits of piracy were related to the possession of illegal software by business students. In a follow-up study, the same authors discovered that perceptions of authority figures' approval or disapproval significantly affect piracy, while prices of programs do not (Christensen and Eining, 1991). In similar research endeavors on the subject, however, software prices were shown to be positively related to pirating activity (Cheng, Sims and Teegen, 1997; Harrington, 1989). Studies by Leventhal, Instone, and Chilson (1992) and Wong (1995) found that when a profit motive was absent from the reasoning behind engaging in piracy, students were generally able to perceive the activity as acceptable. As long as the copied software was not used for fiscal gain, money was not involved, and stealing had not taken place, it was not perceived as wrong to duplicate the program for personal purposes.

Other scholars have sought to understand the phenomenon by focusing on individual beliefs from the perspective of an ethical decision (Gopal and Sanders, 1998; Im and Van Epps, 1991; Kievit, 1991; Wong, 1995). That is, researchers endeavored to discover whether the decision to participate in piracy was related to the individual's awareness of the community's norms of legally and morally acceptable conduct. Cohen and Cornwell (1989) found that many college students find software theft and other forms of unethical computing behaviors acceptable, and even condone them as normative activity. In fact, most inquiries have found a prevailing social consensus with regard to the acceptability of intellectual property theft among university students, likely due to peer norms and the lack of a threat of disciplinary repercussions (Cohen and Cornwell, 1989; Oz, 1990; Rahim, Seyal and Rahman, 1999; Reid, Thompson and Logsdon, 1992; Solomon and O'Brien, 1990; Wood and Glass, 1995). This is likely related to a silence and passivity on the part of university personnel to recognize and address the problem. Such a display of indifference may be interpreted as an attitude of general tolerance or leniency towards the activity, and may consequently further its preponderance. As mentioned earlier, Christensen and Eining's (1991) work supports this contention in finding that perceptions of disapproval from authority figures was correlated with decreased participation in software piracy.

Principal issues

Through this analysis, answers to two important questions are sought.

1. What is the demographic makeup of university students who engage in online software piracy?

The demographic composition of respondents can be analyzed and used to determine whether a certain age, gender, race, employment status, age, year of study, or choice or major makes a difference in the collective profile of individuals that pirate software over a networked connection. This can be used to support or refute previous studies of this phenomenon which intended to educe an outline of the typical software pirate. Additionally, the current work improves upon prior research by examining the student body as a whole, rather than taking convenience samples of students in introductory Business, Management Information Systems, and Computer Science classes (Buckley, Wiese and Harvey, 1998; Im and Van Epps, 1991; Kievit, 1991; Rahim, Seyal and Rahman, 1999; Sims, Cheng and Teegen, 1996).

2. How deep are students' immersion in the software pirating scene, and what are their general sentiments towards the act?

The level of involvement in piracy among the study sample can be ascertained through a variety of closed-ended questions. These will ideally help determine recipients' frequency and collective beliefs towards piracy, their extant knowledge of particular concepts in the piracy scene, and their perceptions of the efficacy of threatened sanctions.

3. How are levels of Internet proficiency and variety related to software pirating activity by students?

Proficiency of Internet use will be measured with a list of 10 constructs that range in their degree of difficulty.[1] Variety of Internet use – the breadth of activities the respondent has performed on the Internet – will be measured with a list of 13 items.[2] In accord with intuition, it is predicted that the larger the count of items in which the respondent has participated, the greater the scope of his/her usage of the Internet.

Two primary dependent variables are employed in the current work. The variable of "Degree of Hardcore Pirate" was developed to aid in measuring the level of immersion in the software pirating scene.[3] It is important to determine the degree of piracy participation among students to differentiate between those who have dabbled in the activity and those who are heavily involved in it. "Overall Online Pirating Behavior" was a variable created to measure general involvement in software pirating activities, and was utilized in bivariate statistical analysis to determine the contributory role of proficiency and variety of Internet use on software piracy.[4] Secondary dependent variables employed in the univariate analyses were simply those items that comprised "Overall Online Pirating Behavior" and "Degree of Hardcore Pirate".

Methodology

An anonymous and voluntary questionnaire was developed to collect relevant data for the study, and was pretested among a selection of five colleagues. Their helpful suggestions and comments about clarity, composition, structure, and interpretation were taken into account and incorporated into a revised version. The sampling frame consisted of a random selection of classes at a large Midwestern university, and a pronounced attempt was made to include students of all class standings (i.e., freshman, sophomore, junior, senior, graduate level) – by surveying different types and levels of courses. Some classes selected were core classes which the university requires all students to take, while others were restricted to those in a particular discipline. Seventy were initially selected; however, the final total was thirty as less than half of the instructors and professors could spare class time for the administration of a survey. The questionnaire was subsequently administered to 507 students in 30 classes during the summer semester of 2000. After listwise deletion of missing cases, the final number of respondents equaled 433.

Concerning the study population, college students are arguably impressionable individuals seeking to discern their true identity, abilities, and skills while attempting to carve out a niche for themselves before leaving the sheltered academic environment to make their living. Since they lack extensive life experiences from which to draw and reflect upon, they perhaps are

[1] These 10 items used to measure *Proficiency of Internet Use* included: "changed my browser's 'startup' or 'home' page"; "made a purchase online for more than $100"; "participated in an online game"; "participated in an online auction"; "changed my 'cookie' preferences"; "participated in an online chat or discussion (not including email, ICQ, or AOL Instant Messenger)"; "listened to a radio broadcast or music clip online"; "made a telephone call online"; "created a web page"; "set up my incoming and outgoing mail server preferences".

[2] These 13 items used to measure *Variety of Internet Use* included: "Email", "Chat/IRC"; "Research for school work"; "File Transfer"; "Using the Newsgroups"; "Product and Travel Information"; "Online Stock Trading"; "Online Shopping"; "Online Auctions"; "Online Games"; "Online Banking"; "To collect information related to news, sports, or the weather"; "To collect information related to personal interests and hobbies"; "Web Design".

[3] The *Degree of Hardcore Pirate* variable was constructed using an additive scale comprised of eight items: "I know what warez is"; "I know what an .nfo file is"; "I know what 0-day means"; "I have set up an FTP server on my computer system in order to allow others to log in and upload/download pirated software to/from me"; "the majority of my file transferring takes place at night (11pm to 7am)"; "I leave my computer on for extended periods of time (i.e., overnight) to transfer files"; "I have a personal account on one or more FTP sites"; and "I can find almost any piece of commercial software I might need on the Internet, either through friends or searching/browsing through file archives". These items – containing arcane terms and examples of behavior endemic to the phenomenon – are generally only answerable in the affirmative by those significantly immersed in piracy. Since these questions were all dichotomous, an additive model resulted in a range from 0 (representing no knowledge of, and no participation in, the software pirating scene) to 8 (representing complete awareness of, and participation in, the software pirating scene).

[4] The *Overall Online Pirating Behavior* variable was created via factor analysis from the following variables: "How frequently do you upload/download pirated software to/from others (on average)"; Number of mediums used to pirate software; Degree of Hardcore Pirate; "How often in the last month have you pirated software?"; "How often in the last year have you pirated software?". These items are jointly considered a solid and appropriate measure of the construct (alpha = 0.76).

generally less grounded in their ethical standards and mores. As a result, this may augment their susceptibility to participation in controversial activities such as software piracy. Further, researchers have pointed out that colleges and universities are breeding grounds for piracy, many times due to the lack of vigorous rule enforcement governing computer ethics by academic officials, as well as higher levels of curiosity and questionable behavior among students (as compared to persons at lower levels of education or the "working world"). This is evidenced by research findings on the subject of cheating and plagiarism (Agnew and Peters, 1986; Buckley, Wiese and Harvey, 1998; Crown and Spiller, 1998), as well as on software piracy (Cheng, Sims and Teegen, 1997; Eining and Christensen, 1991; Im and Van Epps, 1991; Im and Van Epps, 1992b; Sims, Cheng and Teegen, 1996; Temple, 2000; Wong, Kong and Ngai, 1990).

Analyses

Univariate statistics

Descriptive findings are now provided to paint a broad picture of the respondents' demographic characteristics and their participation in online software piracy.

As illustrated in Table 1, the majority of respondents were female (53.1%), white (71.8%), 21 years of age or older (70.6%), seniors (59.8%), and either majoring in Business (23.5%) or a discipline of the Social Sciences (34.3%). Also, a sizable three-fourths (74%) of the study population worked at least ten hours a week. Six singular piracy measures were included to determine how these demographic variables differentiated individuals in their participation in software piracy. They included: "I have uploaded/downloaded at least one piece of pirated software to/from someone"; "How frequently do you pirate per week? "; "Number of mediums used to pirate software";[5] "Degree of Hardcore Pirate"; "How often in the last month have you pirated software? "; and "How often in the last year have you pirated software?". For each of these variables, the mean scores for males were higher than that for females – in accord with intuition that men would engage in piracy with greater frequency and intensity than women.

More Asian respondents have transferred at least one piece of pirated software to/from someone and pirate more software per week than any other race. Asians also used the most mediums to pirate software online, and ranked highest on the constructed measure of "Degree of Hardcore Pirate" – indicative of significant immersion in the software pirating scene. The number of hours a respondent worked each week was not correlated with pirating activities or the level of immersion in the piracy scene. This intimates that the financial status of a student – if measured by their willful participation in the workforce – is unrelated to the practice of software piracy. Furthermore, the demarcation between ages 17–20 and ages 21–older did not seem to evince any striking differences in pirating behavior. Perhaps if the sample's age were more evenly distributed, a specific age range would have loaded higher on one or more of the piracy means.

Concerning educational level, freshmen loaded highest in the sampling means measuring Internet piracy participation; however, this statistic is not reliable as only four freshmen were surveyed. Comparing juniors and seniors, it is apparent that more seniors have uploaded or downloaded at least one pirated application or game, pirate more frequently per week, month, and year, and use more transmission mediums than juniors. Juniors, however, appear more significantly immersed in the piracy scene. Finally, those who did not major in either Social Science or Business ranked higher on the mean number of times per week, month, and year they pirated software, as well as the scope of piracy mediums utilized and their level of immersion in the pirating scene.

The findings of some ethical questions from the survey instrument are presented above in Table 2. Almost half (41.3%) of the students were cognizant of, and concerned about, copyright infringement online, and 16.6% believed that information, graphics, and files posted to the Internet cannot and should not be used by anyone. In a question that speaks volumes about perceptions of ethical computing behavior, 49.6% revealed that they would not feel guilty about pirating software, and one-fourth (25.9%) chose "Undecided" – a group perhaps more susceptible to drifting towards participation in piracy rather than refraining from it. Reinforcing a general lack of an inculcation of computing ethics is the finding that 51.3% of all respondents do not regard piracy as improper or intrinsically wrong. This percentage is somewhat disquieting, particularly when considering the possible deterrent effect of news reports on the controversy surrounding the online distribution of intellectual property in the form of digital music files. Another finding along the same lines, and indicative of the perceived power of sanctions to dissuade or deter pirating behavior, was that 35.3% of those surveyed do not believe they will ever be disciplined for their copyright infringing activities. Moreover, the threat of legal repercussions and fines are – according to

[5] Software piracy mediums include the World Wide Web, the USENET newsgroups, instant messaging programs, chat programs, and FTP programs (which are used both to serve and to retrieve software).

Table 1. Demographics of software pirates (n = 433)

Demographic statistics	Total sample percentage	Piracy measures (means)					
		1(%)	2	3	4	5	6
Gender							
Male	46.5	42.1	1.58	1.60	1.77	1.26	1.45
Female	53.1	26.8	1.38	1.15	0.98	1.12	1.22
Race							
White	71.8	32.5	1.40	1.24	1.31	1.16	1.28
Asian	10.3	46.2	1.66	1.89	1.57	1.13	1.30
Other	17.9	32.2	1.57	1.43	1.31	1.29	1.43
Employment (hrs)							
40	14.4	38.4	1.47	1.47	1.49	1.23	1.27
30	17.4	23.9	1.47	1.05	1.32	1.08	1.16
20	28.8	39.6	1.53	1.41	1.40	1.27	1.44
10	13.4	29.4	1.42	1.25	1.05	1.17	1.26
0	26.0	34.1	1.44	1.51	1.39	1.17	1.38
Age							
17–20	28.5	34.6	1.42	1.55	1.28	1.15	1.32
21–older	71.5	33.5	1.48	1.26	1.36	1.19	1.30
Educational level							
Freshman	1.8	50.0	1.83	2.83	3.00	1.33	2.00
Sophomore	4.7	29.2	1.62	1.95	1.10	1.29	1.57
Junior	30.6	32.3	1.42	1.20	1.42	1.16	1.23
Senior	59.8	35.1	1.45	1.34	1.27	1.17	1.31
Graduate	3.2	25.0	1.64	1.18	1.55	1.36	1.45
Discipline							
Soc. Science	34.3	29.3	1.47	1.20	1.18	1.09	1.22
Business	23.5	36.4	1.37	1.21	1.08	1.14	1.25
Other	42.2	36.2	1.51	1.54	1.61	1.27	1.42

Piracy Statistics are measured with the following survey questions:

1. "I have uploaded/downloaded at least one piece of pirated software to/from someone.
2. "How frequently do you pirate per week?"
3. "Number of mediums used to pirate software"
4. "Degree of Hardcore Pirate"
5. "How often in the last month have you pirated software?"
6. "How often in the last year have you pirated software?"

the responses – irrelevant at best and laughable at worst, with 55.4% of all students unconcerned about the law's mandates. In a final measure of ethical standards among students, only 8.8% were plagued by their conscience after pirating software and decided to legitimately purchase the product they had freely downloaded.

Bivariate statistics

One-way analysis of variance (ANOVA) was conducted to see how categorical variables might be inserted into the statistical model as influencers of pirating behavior. As previously mentioned, the dependent variable employed was a constructed measure of "Overall Online Pirating Behavior". Proficiency in Internet-related activities, such as participating in a web-based auction or creating a web page, is expected to be positively related to pirating behavior. Succinctly put, it is presumed that those who are more technologically adept are more likely to possess the knowledge and abilities to pirate software.

As predicted, those who engaged in six or less items of the variable measuring proficiency of Internet use rated lower on overall online pirating (see Table 3). As predicted, those who had performed seven or more items rated higher on overall pirating behavior. Based on the significance level of F, at least one proficiency category significantly differs from the others in its power to influence software piracy. The Bonferroni Post Hoc test found that the alpha level for the category of 9–10 items was 0.00 when compared to each of

Table 2. Ethical standards among students (n = 433)

	SD (%)	D (%)	U (%)	A (%)	SA (%)
I am concerned about copyright infringement	7.9	22.2	28.6	30.71	0.6
Information, graphics, and files posted to the Internet can and should be used by anyone	14.1	46.4	22.9	13.4	3.2
Generally speaking, I would feel guilty for pirating software	7.9	16.6	25.9	32.3	17.3

	No (%)	Yes (%)	N/A (%)
I feel that the distribution of commercial full-version software is wrong.	51.3	29.8	18.9
I don't think I will ever be disciplined or get into trouble for transferring commercial full-version software files.	31.9	35.3	32.8
I am worried about legal repercussions, such as fines of up to $150,000 per program and up to five years in prison, that could result from the distribution of commercial full-version software	55.4	18.9	25.6
I have at least one time felt so guilty that I went and purchased the software that I had downloaded.	56.6	8.8	34.6

SD = Strongly Disagree, D = Disagree, U = Undecided, A = Agree, SA = Strongly Agree

Table 3. ANOVA of proficiency of Internet use and overall online pirating (n = 433)

Proficiency of Internet use	Mean	*F*
0–2 items	−0.35	26.578**
3–4 items	−0.12	
5–6 items	−0.06	
7–8 items	0.28	
9–10 items	1.32	

$\eta^2 = 0.256$
**Correlation is significant at the 0.01 level (2-tailed).

Table 4. ANOVA of variety of Internet use and overall online pirating (n = 433)

Variety of Internet use	Mean	*F*
0–2 items	0.10	13.666**
3–4 items	−0.28	
5–6 items	−0.08	
7–8 items	0.42	
9–10 items	1.02	

$\eta^2 = 0.128$
**Correlation is significant at the 0.01 level (2-tailed).

the other categories; this indicates that the highest level of proficiency differentiates software pirates from non-pirates. That is, those who are highly skilled at Internet-related activities are significantly more likely to be software pirates than those who demonstrate a lower skill level. Eta squared (η^2) was found to be 0.2559; that is, 25.6% of variation in overall online pirating behavior can be explained by proficiency in Internet use. As an assessment of strength, this figure is indicative of a moderate relationship between the predictor variable and software piracy.

ANOVA was also employed to ascertain the relationship between the utilization of a variety of online resources and overall pirating behavior. The sample means depict that those with a higher degree of variety in their Internet activities pirate software with greater frequency (see Table 4).

Furthermore, the significance of F indicates that at least one category mean is different from the others in the population. The Bonferroni Post Hoc comparison test found that the alpha value for the category of 12–13 items was significantly different from 0–2 items ($\alpha = 0.01$), 3–5 items ($\alpha = 0.00$), and 6–8 items ($\alpha = 0.00$), indicating that those who used the Internet in a wider context substantially varied in their pirating activities than those whose online use was more specific and narrow. However, 12–13 items was not differentiated from 9–11 items ($\alpha = 0.094$). Thus, it seems a demarcation can be made between 0-8 items and 9–13 items – with the former grouping categorized as "low variety" of Internet use, and the latter as "high variety". To reiterate, those who use the Internet for a broad range of purposes pirate software to a significantly greater degree than those who only utilize the Internet for a few specialized functions. To note, a relatively small 12.8% of variation in overall online pirating is explained by this predictor.

Discussion and implications

The foregoing analysis clearly expresses that software piracy conducted over the Internet among students is a problem meriting immediate attention and a competent response. What proactive and reactive measures can be taken to impede the proliferation of this form of intellectual property theft? The implementation of technical initiatives at the workstation and network level may go a long way towards this end, and are presented below as practical suggestions. Methods to instill ethical computing behavior among university students also portend much value, and are proposed as well. While some of these policies might not be plausible at smaller universities and colleges, it is hoped that noteworthy potentialities based on these suggestions can be extrapolated, modified, and put to use.

Technological solutions

To begin, at the university where this research was conducted, monitoring is currently being performed to ensure the efficiency and peak functionality of the wide area networks by determining how many packets of data are lost as a result of heavy bandwidth usage, overload, or other network traffic issues (personal correspondence, February 3, 2000). It has been suggested that monitoring of bandwidth and identification of exactly what is being transferred (through a technique called "packet sniffing") is increasingly necessary to address the issue of copyright infringement occurring over university data communication lines. However, there are some issues that preclude the possibility of using this technique.

With connection-based traffic such as FTP and IRC, the client computer must contact and establish a connection with the remote computer in order to facilitate the transfer of data, thereby augmenting the challenge of ferreting out information from the packets. Determining the content of transfers through connection-based traffic is an extremely arduous task because each packet of data must be analyzed, which can consume exponentially large amounts of time and hardware resources. Packet sniffing will also compete for the time and attention of network administrators who are usually quite busy tending to other vital day-to-day affairs such as maximizing "uptime" for all systems online and maintaining network connectivity throughout campus. Finally, most transfers of program files occur in binary format rather than plain-text format, and it is therefore extremely hard to detect what an assortment of zeros and ones mean when attempting to deduce the type of files that are being transferred. Most importantly, though, is the issue of whether network administrators on a campus have the legal right and ethical consent to inspect the contents of files being transferred. Many would argue that this is a fundamental breach of individual civil rights, and violates doctrines in place at educational institutions emphasizing academic freedom and complete respect for the privacy of students (personal correspondence, February 3, 2000).

Filtering out certain types of data may also initially seem like a viable solution. At the routing level, where the university network is connected to the Internet, traffic can be filtered so that incoming and outgoing data on certain ports are allowed and disallowed for usage. This would accordingly reduce the amount of throughput that requires monitoring. Nonetheless, this might unintentionally restrict legitimate users in their computing and networking abilities. Persons can also circumvent filters by purposively configuring data transmissions through common ports essential for standard Internet activities such as web browsing (e.g., port 80). Finally, partial filtering of illegal traffic indicates an acknowledgement that restricting certain types of data *is* possible – which then places the onus of continually monitoring, identifying, and addressing potentially proscriptive network activity on the university. Such a task may be impractical and largely impossible to carry out.

Another possible solution results from the existence of a caching server, which is present in each residence hall (or dormitory) as an intermediary node between a student's computer and the millions of Internet servers from which documents and information are retrieved. Some background on this technology is requisite before assertion of a suggested solution. The caching server can be considered a "data liaison" which saves frequently requested data into a collection that is made immediately available to users as soon as a client computer requests it. Rather than venturing outside of the university network to obtain the content and unnecessarily adding to the volume of Internet traffic and congestion, the caching server functionally accelerates the communications flow of the network and reduces latency (transmission delays) by delivering documents and data from its storage repositories rather than from the originating servers.

Caching servers may potentially be used to promote computing ethics. When a student turns on his computer in a residence hall, the network interface card is activated and broadcasts the Internet address it has been assigned, indicating that the port is open and ready for data transfer. Perhaps each time this broadcast stream of data is received by the caching server, it can be configured to push a popup window onto the user's desktop. This small window would then serve to remind each individual of the "Acceptable Use"

policies of the campus network, and would contain an "OK" button which must be clicked (thereby consciously indicating at least surface abidance by ethical computing mores) before the school's Internet connection can be used. It bears mentioning that this procedure is currently in place on many employee computers at the university studied, but has not been designed to function on the computers of students. Perhaps the absence of such an ethical reminder has contributed in some way to software piracy among students.

Software manufacturers are increasingly implementing server-side license verification architectures to reduce the unauthorized duplication of their products. This is when a serial number or license key is sent to an online database upon the execution of the program to confirm that it is legitimate and reserved only to the user who purchased the product. If an individual attempts to utilize a key previously designated to another, the program will shut down and not function until a valid license is purchased. That key will then become "blacklisted", and subsequent individuals who attempt to register the program with it will be stymied.

One of the largest software manufacturers in the world, Microsoft Corporation, has recently enacted such a system to decrease pirating of their office productivity suite. It requires users to register their product through an online process within the initial fifty uses, or the program will cease functioning (Microsoft, 2000). With more and more Internet users obtaining dedicated connections, their computers will perpetually be online and thereby capable of facilitating server-side verification. While this may be countered in some instances by unplugging one's Internet connection before executing a program, such a duplicitous procedure seems too cumbersome for most individuals. It must be noted that through the reverse-engineering of software and the use of hex editors, skilled programmers can manipulate code to comment out the routine that executes the license confirmation process. When considering the entire Internet population, this level of technical proficiency is rare; therefore, it is suggested that all software developers implement such a remote authentication scheme to cross-check user licenses with a list of valid, registered, purchased codes.

Ethical solutions

When the boundaries of lawful and ethical behavior are clearly defined, it will presumably be more challenging for potential offenders to transgress such limits. Deviance may be reduced in severity and frequency, then, with the use of laws, legal sanctions, or threats of sanction (Tittle, 1980). If acceptable and unacceptable computing behavior is plainly spelled out by university administration through the use of ethical codes substantively similar to laws and legal sanctions, the incidence of piracy among students may be reduced. Engendering a respect for intellectual property among students should be an intrinsically essential function of higher learning, particularly when it involves a networked environment where the appropriation of creative works without the author or owner's permission can proliferate with great ease and celerity.

While Acceptable Use Policies (AUP) in university handbooks and codebooks are used frequently to accomplish this end, they are seemingly not enough, as many students do not take the time to read such lengthy administrative discourses. One AUP (Computer and Network, 2001), not from the university involved in the present work, states:

a. [The University] utilizes a wide variety of software, with an equally wide range of license and copyright provisions. Users are responsible for informing themselves of, and complying with, the license and copyright provisions of the software that they use.
b. No software copy is to be made by any User without a prior, good faith determination that such copying is in fact permissible. All Users must respect the legal protection provided by copyright and license to programs and data.

Investigation and criminal or civil actions are the consequences of this activity, as proposed by the school. While such a warning perhaps absolves the college of any legal duty to specifically educate the student body about intellectual property theft, it does not serve to abrogate its commission. Furthermore, the guidelines are likely to be considered "window dressing" and fail to engender a respect for intellectual labor and creativity – seemingly essential to refraining from piracy. Such codes must clearly delineate the unethical and illegal computing behaviors that will not be tolerated, as well as the consequences that will result.

As a guideline or framework for use, the Software and Information Industry Association (SIIA) provides a Recommended Internet Usage Policy that can be adapted as necessary by universities to suit their interests (Recommended, 1999). Apart from increasing methods of deterrence and awareness of sanctions, universities should inform the student body of the regular occurrence of piracy detection and computer auditing, monitoring, and logging by network staff and administrators. Towards this end, the SIIA and the Business Software Alliance (BSA) provide organizations and individuals with a self-audit

kit at either zero or minimal cost (Software Piracy, 1999; SPAudit Software Management Tools, 1999). Thus, it is hoped that consciousness by students of continually impending "sweeps" by those in charge will serve as a disincentive to participate in the activity.

Some universities distribute CDROMs to every incoming student, containing licensed or freeware copies of Internet software such as Netscape Navigator and Microsoft Internet Explorer, as well as a program which configures the client system (or allows for effortless configuration by the student) to use the Ethernet ports in university dormitories. When the program files on the CDROM are run, shortcuts to web pages such as the university's AUP or organizations such as the BSA or the SIIA can be installed onto the desktop of the user's computer. This not only would facilitate easy accessibility to rules and regulations governing intellectual property and honorable computing practices without having to search for the information, but also increases cognizance and awareness of the university's insistence on – and attention to – lawful use of their network resources.

To preclude software piracy by students, other steps can be taken to increase recognition that software is a tangible product with an assignable value, and that intellectual property theft is a crime. For instance, universities are increasingly requiring incoming high-school students to take a basic introductory course pertaining to computers, general office software applications (word processing, spreadsheet, presentation programs), and the Internet. It is suggested that instructors of these courses incorporate into their lesson plan a time where the distinction between ethical and unethical computing behavior can be clearly defined. Even a brief mention of computer ethics during orientation sessions and campus tours is likely to be helpful in educating students and underscoring the necessity to adhere to institutional and external standards of proper usage of computing resources. Publication of national articles about computer criminal arrests in the school newspaper might also generate a deeper awareness of the seriousness of the issue at hand. In addition, anti-piracy signs and posters in computer laboratories and even heavily frequented school halls or areas would increase sensitivity toward the university policy, as well as to copyright law in general.

Another potentially beneficial solution might involve relational interaction between universities and the IT industry, particularly software development companies. These business entities might send representatives as public speakers to campuses during either the first week of orientation or to a required introductory computing class during the semester. In these venues, representatives could champion their cause by describing the damage that is done to their companies as well as the IT industry, developers and programmers (both by removing financial incentive and through the stifling of innovation and creativity), and ultimately the consumer population. This will plausibly counter rationalizations and justifications that students might employ to facilitate software piracy. Furthermore, by the speaker's presence, the existence of a real and visible victim will be demonstrated, ideally dissuading the perception of software manufacturers as nonhuman, remote, and oblivious entities.

Summary

The implementation of technological initiatives at the network and workstation level and the inculcation ethical standards among individuals may prove fruitful in addressing software piracy. The distinction between right and wrong among certain behaviors birthed by technological advances is often unclear and susceptible to varying interpretations. By extension, there seems to exist a lack of such a demarcation line with regard to piracy, and universities need to step up and address this issue through the specific and conspicuous delineation of appropriate and inappropriate computing behavior. It can be argued that the inability to proactively curtail piracy through technological means or to cultivate cognitive restructuring among populations prone to questionable behavior has in some respects fostered and perpetuated the phenomenon.

The current study has sought to depict the existence of Internet software piracy in a university setting in an attempt to shed light on the problem and to bring attention to the increasing salience of ethical computer and network usage. As illustrated by the statistics, piracy is not unique or rare – it is all too prevalent among students of a variety of demographic characteristics. Proficiency and variety of Internet use were also found to be positively related to online software piracy. As individuals become increasingly experienced and comfortable with computers and the Internet, the theft of various intellectual property likely will grow. The convergence of communications, computing, and unethical behavior has already reaped sizeable fiscal consequences for industry and society, and a subsequent decrease (or even a plateau) of these activities does not seem imminent without substantive effort. Therefore, it is hoped that the current research provides useful technical and ethical policy solutions and serves as a stepping-stone for additional inquiry, so that substantive progress can be made in curtailing

the preponderance of Internet software piracy among students.

Acknowledgements

The author gratefully acknowledges the guidance and mentorship of Drs. Mahesh Nalla, Christina DeJong, and Christopher Maxwell.

References

R. Agnew and A.A.R. Peter. The Techniques of Neutralization: An Analysis of Predisposing and Situational Factors. *Criminal Justice and Behavior*, 13(1): 81–97, 1986 (March).

M.R. Buckley, D.S. Wiese and M.G. Harvey. An Investigation into the Dimensions of Unethical Behavior. *Journal of Education for Business*, 73(5): 284–290, 1998 (May–June).

H.K. Cheng, R.R. Sims and H. Teegen. To Purchase or Pirate Software: An Empirical Study. *Journal of Management Information Systems*, 13(4): 49–60, 1997 (Spring).

A.L. Christensen and M.M. Eining. Factors Influencing Software Piracy: Implications for Accountants. *Journal of Information Systems*: 67–80, 1991 (Spring).

Classification of Software. Software and Information Industry Association, 1999. [Online] Available http://www.siia.net/piracy/programs/share.htm, December 12, 1999.

E. Cohen and L. Cornwell. College Students Believe Piracy is Acceptable. *CIS Educator Forum*, 1(3): 2–5, 1989.

Computer and Network Acceptable Use Policy. Middle Tennessee State University, 2001. [Online] Available http://www.mtsu.edu/misc/policy.html, March 15, 2001.

D.F. Crown and M.S. Spiller. Learning from the Literature on Collegiate Cheating: A Review of Empirical Research. *Journal of Business Ethics*, 17(6): 683–700, 1998.

D. Denning. *Protection and Defense of Intrusion*. Georgetown University, 1996 (February 28–March 1). Paper based on a talk given at the conference on 'National Security in the Information Age' at the US Air Force Academy, Colorado Springs, CO. [Online] Available http://www.cs.georgetown.edu/~denning/infosec/USAFA.html, July 1, 1999.

M.M. Eining and A.L. Christensen. A Psycho-Social Model of Software Piracy: The Development and Test of a Model. In R. Dejoie, G. Fowler and D. Paradice, editors, *Ethical Issues in Information Systems*, pp. 134–140. Boyd and Fraser Publishing Co., Boston, MA, 1991.

D.R. Ellis. Computer Law – A Primer on the Law of Software Protection. *The Florida Bar Journal*, 1986 (April).

R.D. Gopal and G.L. Sanders. International Software Piracy: Analysis of Key Issues and Impacts. *Information Systems Research*, 9(4): 380–397, 1998 (December).

M.S. Friedman and K. Bissinger. *Infojacking: Crimes on the Information Superhighway*. New Jersey Law Journal, 1995 (May 22). [Online] Available http://www.sgrm.com/art15.htm, March 01, 2001.

S.J. Harrington. Why People Copy Software and Create Computer Viruses: Individual Characteristics or Situational Factors? *Information Resources Management Journal*: 28–37, 1989 (Summer).

S. Hinduja. *Neutralizing Piracy*, 2002. Article manuscript under review.

J.H. Im and C. Koen. Software Piracy and Responsibilities of Educational Institutions. *Information and Management*, 18(4): 189–194, 1990.

J.H. Im and P.D. Van Epps. Software Piracy and Software Security in Business Schools: An Ethical Perspective. *Data Base*, 22(3): 15–21, 1991 (Summer).

J.H. Im and P.D. Van Epps. *Legal and Ethical Issues of Software Piracy*. International Association for Computer Information Systems. New Orleans, LA, 1992a.

J.H. Im and P.D. Van Epps. Software Piracy and Software Security Measures in Business Schools. *Information and Management*, 23(4): 193–203, 1992b.

International Review of Criminal Policy – United Nations Manual on the Prevention and Control of Computer Related Crime, 1994. [Online] Available http://www.ifs.univie.ac.at/%7Epr2gq1/rev4344.html, February 12, 1999.

J. Jefferson. Deleting Cybercrooks: Prosecutors Want Tough Laws to Put Internet Hackers, Scam Artists and Pedophiles on Permanent Log Off. *Cyber Law, ABA Journal*, 83: 68, 1997 (October).

K. Kievit. Information Systems Majors/Non-Majors and Computer Ethics. *Journal of Computer Information Systems*, 32(1): 43–49, 1991 (Fall).

L.M. Leventhal, K.E. Instone and D.W. Chilson. Another View of Computer Science Ethics: Patterns of Responses Among Computer Scientists. *Journal of System Software*, 17: 49–60, 1992.

Y. Malhotra. Controlling Copyright Infringements of Intellectual Property: The Case of Computer Software – Part One. *Journal of Systems Management*, 45: 32–35, 1994a (June).

Microsoft Incorporates New Anti-Piracy Technologies In Windows 2000, Office 2000. Microsoft Corporation, 2000. [Online] Available http://www.microsoft.com/presspass/press/2000/feb00/apfeaturespr.asp, April 5, 2000.

E. Oz. The Attitude of Managers-to-Be Toward Software Piracy. *OR/MS Today*, 17(4): 24–26, 1990 (August).

A.G. Peace. *A Predictive Model of Software Piracy Behavior: An Empirical Validation*. Unpublished doctoral dissertation, University of Pittsburgh, 1995.

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

Press Release. Business Software Alliance, 1999. [Online] Available http:/www.bsa.org/pressbox/policy/944837492.htm, December 12, 1999.

M.M. Rahim, A.H. Seyal and N.A. Rahman. Software Piracy Among Computing Students: A Bruneian Scenario. *Computers and Education*, 32: 301–321, 1999.

Recommended University Internet Usage Policy, 1999. [Online] Available http://www.siia.net/piracy/programs/univgd2.htm, November 15, 1999.

R.A. Reid, J.K. Thompson and J.M. Logsdon. Knowledge and Attitudes of Management Students toward Software Piracy. *Journal of Computer Information Systems*, 33: 46–51, 1992 (Fall).

V.F. Sacco and E. Zureik. Correlates of Computer Misuse: Data from a Self-Reporting Sample. *Behaviour and Information Technology*, 9: 353–369, 1990.

U. Sieber. *Legal Aspects of Computer-Related Crime in the Information Society*. University of Würzburg. COMCRIME – Study Prepared for the European Commission, 1998. [Online] Available http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html, April 15, 2001.

R.R. Sims, H.K. Cheng and H. Teegen. Toward a Profile of Student Software Piraters. *Journal of Business Ethics*, 15: 1996, 839–849.

Software Piracy. Business Software Alliance, 1999. [Online] Available http://www.nopiracy.com/intro_c.html, December 12, 1999.

Software Piracy and U.S. Law. Business Software Alliance, 1998. [Online] Available http://www.nopiracy.com/swandlaw_c.htm, December 12, 1999.

SPAudit Software Management Tools. Software and Information Industry Association, 1999. [Online] Available http://www.siia.net/piracy/tools/download.htm, December 12, 1999.

S. Solomon and J.A. O'Brien. The Effect of Demographic Factors on Attitudes Toward Software Piracy. *Journal of Computer Information Systems*: 40–46, 1990 (Spring).

Temple University Pays $100,000 To Settle Software Claims. Business Software Alliance, 2000. [Online] Available http://www.bsa.org/pressbox/enforcement/index.html?/pressbox/enforcement/952007190.html, March 25, 2000.

The Copyright Act and Fair Use. Software Information Industry Association, 1999. [Online] Available http://www.siia.net/piracy/programs/fairuse.htm, December 12, 1999.

C.R. Tittle. *Sanctions and Social Deviance: The Question of Deterrence*. Praeger Publishers, New York, 1980.

Warez: Myth vs. Fact. Business Software Alliance, 1998. [Online] Available http://www.nopiracy.com/warezfaq_c.html, December 12, 1999.

What is Free Software? – GNU Project. Free Software Foundation, 1999. [Online] Available http://www.fsf.org/philosophy/free-sw.html, November 20, 1999.

C. Wolf and S. Shorr. Cybercops Are Cracking Down on Internet Fraud. *The National Law Journal*. The New York Law Publishing Company, 1997.

E.Y.H. Wong. How Should We Teach Computer Ethics? A Short Study Done in Hong Kong. *Computers and Education*, 25(4): 179–191, 1995 (December).

G. Wong, A. Kong and S. Ngai. A Study of Unauthorized Software Copying Among Post-Secondary Students in Hong Kong. *The Australian Computer Journal*, 22(4): 114–122, 1990 (November).

W. Wood and R. Glass. Sex as a Determinant of Software Piracy. *Journal of Computer Information Systems*, 36(2): 37–40, 1995 (Winter).