This is to certify that the

thesis entitled

Broadband Connectivity and Software Piracy in a University Setting

presented by

Sameer Hinduja

has been accepted towards fulfillment
of the requirements for

M.S. degree in Criminal Justice

N. Marc Uhn

Major professor

Date Fall 2000

DATE DUE	DATE DUE	DATE DUE
MAR 1 3 2002		

BROADBAND CONNECTIVITY AND SOFTWARE PIRACY IN A UNIVERSITY SETTING

By

Sameer Hinduja

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

Department of Criminal Justice

2000

ABSTRACT

BROADBAND CONNECTIVITY AND SOFTWARE PIRACY
IN A UNIVERSITY SETTING

By

Sameer Hinduja

Software piracy has become a significant problem for businesses and educational institutions, and as computer crime continues to proliferate in our information age, its causes and roots merit academic inquiry. This paper attempts to determine whether, and to what degree, high-speed Internet access in a university residential setting facilitates the transferring and distribution of unauthorized software packages. Additionally, it seeks to apply neutralization theory to software piracy to obtain a greater understanding of the factors that influence the commission of this high-tech crime. The study utilized a survey instrument in its methodology, which gleaned valuable information on the motives, rationalizations, and behaviors of software pirates. Independent Samples T-Tests, ANOVA, Correlations, Two-Way ANOVA, and Ordinary Least Squares Regression were utilized to empirically evaluate relationships between variables. A significant relationship was found in that high-speed access is positively related to increased online piracy. Past experience with traditional piracy through the creation and duplication of programs on CDROMs was also found to be a significant predictor of Internet pirating. Finally, neutralization theory was found to be an applicable framework in which to view the deviance. The results of the study are used to suggest policy aimed at combating the onset and perpetuation of unethical and illegal computing activity among students.

To m

To my parents and sister, this work is dedicated.

and C

cours

work

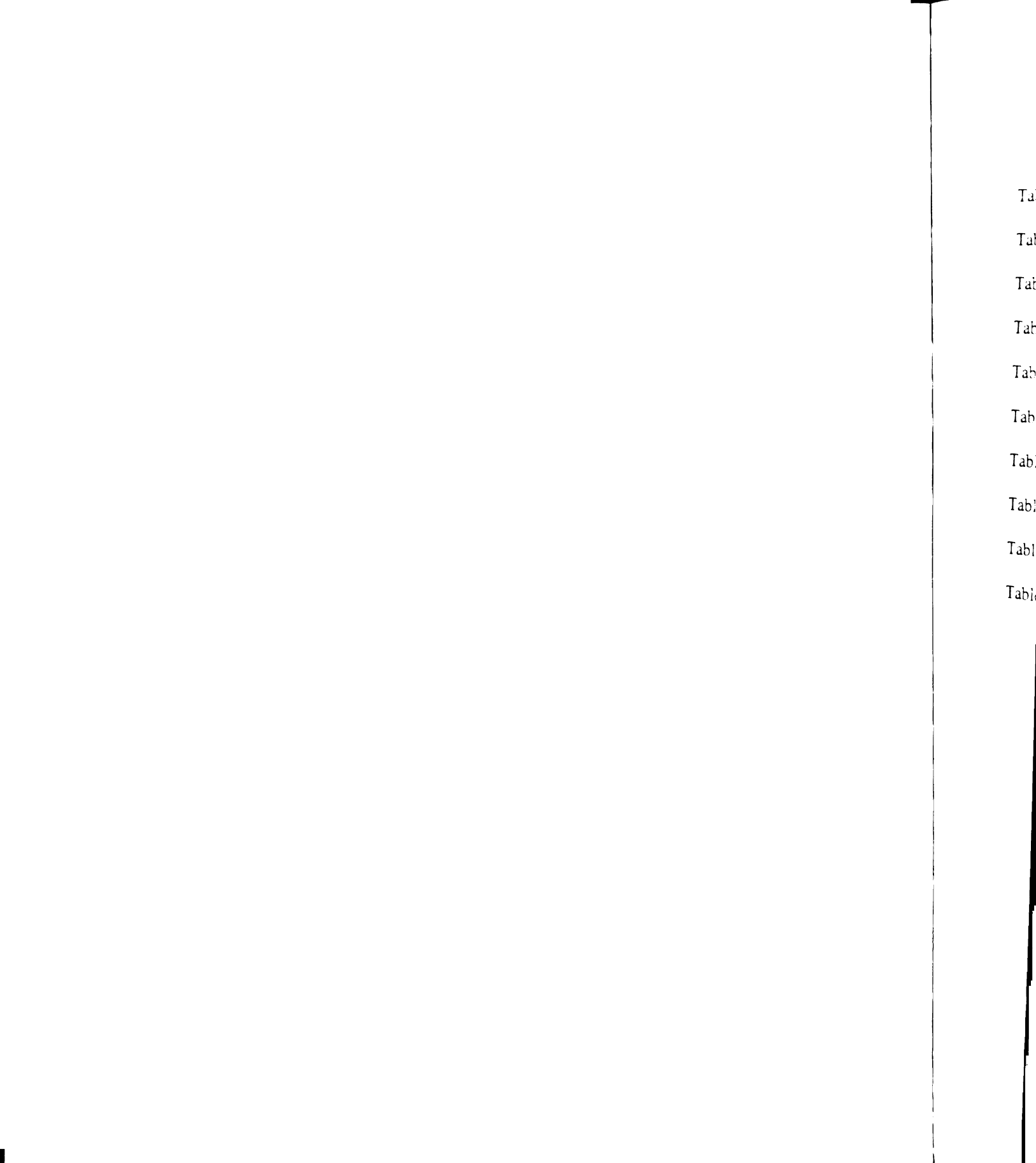
like t

impor

ACKNOWLEDGEMENTS

I would like to thank my committee members, Mahesh Nalla, Christina DeJong, and Christopher Maxwell, who offered valuable guidance and feedback throughout the course of this project. They were always happy to discuss the progress of the research work and bring to my attention inconsistencies that necessitated addressing. I would also like to thank my family and friends for their support and encouragement. Most importantly, I'm grateful to God for the peace that He grants.

TABLE OF CONTENTS



LIST OF TABLES

INTRODUCTION

Premise

Computers have become an increasingly integral part of our lives in the past two decades, playing a significant role in both the industrial and economic functions of society. The exponential growth in information technology (IT), while introducing unheralded improvements in productivity, commerce, communication, entertainment, and the dissemination of information, has precipitated new forms of antisocial, unethical, and illegal behavior. As more and more users have become familiar with computing, the scope and prevalence of the problem has grown. Computer fraud, child pornography, hacking, and software piracy have all achieved notoriety and prominence due to technological advances. These categories fall under a broader heading of a deviance currently receiving deeper examination and unprecedented focus and interest from state, national, and international entities, as well as the general public. This phenomenon is computer crime, defined as "any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime" (Computer crime, 2000).

The Internet has also taken on unprecedented importance since the mid-1990s. It includes email, chat servers, file servers, and web servers that provide vast amounts of information and opportunities for interactive communication to millions of people through the use of a computer. This "Information Superhighway" is a nascent, rapidly diffusing technology that promises to become the economic underpinning for all successful countries in the new global economy. Concomitant with the benefits of

computers and the Internet, however, have arrived new possibilities for criminogenic behavior unique to the "virtual" environment in which it occurs. Software piracy is one such non-traditional crime birthed by digital innovation, and is defined as the unauthorized use or illegal copying of a software product without explicit permission from the copyright holder (Global Software Piracy Report, 1997; Gopal & Sanders, 1998). As the focus of the current study, some of its unique characteristics bear mentioning. For one, when piracy occurs over the Internet (or through an online medium rather than through the duplication of physical media), it is extremely difficult to detect. This is due in part to the power of computers to process and disseminate electronic information rapidly, and the fact that many people have access to the Internet at universities, businesses, libraries, and homes (International Review, 1994). Over the Internet, duplication of intellectual property is extremely simple, and software files online can be copied from a remote hard drive to a local hard drive or piece of removable media by a simple "drag and drop" mouse maneuver that takes mere seconds. Furthermore, there is no loss in quality or degeneration of features or functionality through the reproduction of programs.

On an individual level, data communications often take place at high speeds without personal contact, leaving very little time for users to consider the implications of their actions online. Undeniably, Internet social exchanges are less emotional and relational than interaction in a tangible setting, and this feature has the effect of distancing people from the behaviors committed and reducing inhibitions about participating in immoral activities. Cumulatively, these factors allow individuals to circumvent the purchasing of programs from retail markets, and permit them to use illegally downloaded

software without cost or obligation - software which might have cost millions of dollars to research, develop, write, package, and distribute (Ellis, 1986).

Regardless of the cost of production, however, software piracy is the theft of an intellectual product that belongs to someone else, for which s/he has a genuine and unequivocal right to be compensated. Online piracy occurs not only at the expense of software engineers, programmers, and the IT industry, but also represents a further manifestation of society's ever-widening severance with convention. Unarguably, deviants have adapted and incorporated supreme technological advances that have enacted an overall positive change, such as the Internet, to accomplish the commission of crime.

Scope and Objective of the Research

Some statistics might prove useful in sketching a rudimentary picture of the scope of software piracy. The worldwide market for software in 1997 was $122 billion, with the United States (U.S.) holding 70% of this market (Global Software Piracy Report, 1997). In 1998, 38% of business applications loaded onto computer workstations were illegally copied (Global Software Piracy Report, 1998). A hefty $11 billion dollars in software revenues were lost worldwide in 1998, with piracy in the U.S. making up 25% of that figure – a $2.9 billion dollar loss to the software industry. In the U.S. alone, software piracy cost 109,000 jobs in 1998, as well as $4.5 billion in wages and nearly $991 million in tax revenue (Colorado, 2000). It suffices to say that the gargantuan sums of money involved alone should warrant closer and immediate scrutiny by criminal justice practitioners, researchers, educators, and society as a whole. Another factor is that the venue for the retail distribution of software is moving from traditional "brick and

mortar" establishments to online storefronts (with estimates of 66% of software being distributed online by 2005) as the Internet aids companies in their goal to reach a wider customer base and promote their products with lower overhead (Clausing, 2000). This, coupled with the continual increase in Internet users, augurs a steady rise in the trend of piracy.

It is important to stipulate that stealing over an Internet connection is no different than stealing from a traditional retail outlet. Piracy incurs significant damage on the IT industry not only by depriving corporations of billions of dollars in financial returns, but also by eliminating jobs and by stifling innovative enterprise, new research, and product development - fundamental elements for a continued burgeoning of our information-based society. Another relevant issue is endemic to the study population of this paper (further described below) - if college 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. Piracy also undermines the integrity of the educational institution in which it takes place. Perhaps software theft will inevitably precipitate additional forms of illicit 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 unlicensed programs from the Internet to one's dorm room computer cannot be equated to, and is not indicative of, an inclination towards seedier criminal behavior, the existence (or lack) of a correlation remains to be determined and warrants analysis in future longitudinal studies.

This exploratory work focuses on a particular type of computer crime seemingly fostered by broadband connectivity granted to students who reside in university residential facilities. Software piracy has been the subject of previous studies in the business ethics and management information systems fields, but these inquiries have been primarily descriptive in nature. Prior research has provided us with an undeveloped sketch of the prevalence of this particular form of deviance among specific study populations such as business and computer science students, but has failed to satisfactorily determine possible sociological or situational causes of the crime. Moreover, previous exploration has not applied a criminological perspective to guide and steer the investigation.

The primary goal of the current study is to determine whether software piracy among college students is engendered through the availability and inherent rapidity of high-speed link to the Internet. This determinant has not previously been addressed, but is deserving of investigation as network pipelines and consequently online data transfer speeds are continually upgraded and augmented to meet the usage requirements of a growing population of wired individuals. Moreover, by soliciting demographic information from the respondents, the findings of previous research that intended to extract a profile of the "typical" software pirate can be corroborated, refuted, or modified. Piracy through traditional means – the duplication of programs from CD to CD, computer to CD, or CD to computer is also analyzed as a predictor of Internet piracy. Finally, this work attempts to ascertain whether and to what extent students use techniques of neutralization to free themselves from the binds of a normative value system in order to effectuate the unauthorized duplication and dissemination of software. I hope that after

determining the extant level of this crime on a college campus, and by identifying the *a priori* rationalizing processes that occur behind the scenes, competent policy initiatives can be constructed and developed to reduce, if not completely eliminate, the amount of illegal software that is being transferred and distributed through the university's high-speed Internet connection.

Value and Contribution of the Research

This study makes several useful contributions to the areas of criminal justice and computer crime research. For one, the examination applies a criminological theory to software piracy. It extends the research of criminal justice into an area little studied, and works to fill the void of inquiry into deviance resulting from technological advances (in this case, the Internet). Further, the work strives to engender useful policy solutions that universities can implement in order to curb high-tech crime on campuses, an issue that has failed until now to merit examination. Finally, a latent objective is to spark additional interest in, and subsequent research of, all aspects of high-tech crime.

To a notable extent, piracy by students can prove detrimental to the university in many ways. For instance, litigation can arise as software manufacturers seek to thwart the theft of their commercial product. Aside from financial considerations, the negative publicity that can arise from this situation is often more detrimental than a monetary loss (Rahim, Seyal, & Rahman, 1999). Additionally, to make up for lost revenue, an increase in software prices by corporations is likely to result from the unauthorized duplication of program files. Lastly, a failure to satisfactorily address pirating behavior 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, and may even possibly contribute to a substantive rend in the moral fabric of society. University students are targeted for analysis and subsequent policy application because school is where honorable ethical values must be instilled and strengthened, before the individual enters the working world where it will be more difficult to inculcate moral principles. These factors collectively underscore the importance of studying software piracy on college campuses in order to effect the development of initiatives to curtail its salience.

NEUTRALIZATION THEORY

Sociologists have found that individuals can engage in behavior they know is wrong by disavowing their deviance and presenting themselves as normal (Young, 1988). One framework of this process pertains to neutralization theory. In 1957, Gresham Sykes and David Matza introduced this perspective on social control, which attempted to explain how some juveniles appease and transgress the moral obligation to be bound by the law. To validate their activities of misconduct, individuals learn techniques that they can use as qualifications to extricate themselves from personal responsibility even before the act is committed. This allows them to rhetorically neutralize whatever misgivings they might originally have had about participating in the miscreance (Sykes & Matza, 1957). Then, through these justifications the imperatives of the dominant normative society are dismissed (although not diametrically opposed) for the time being in order to facilitate the commission of the crime. "Social controls that serve to check or inhibit deviant motivational patterns are rendered inoperative", allowing the delinquent the freedom to violate conventions while avoiding negatively labeling oneself as a criminal (Sykes & Matza, 1957:667).

To neutralize internal and external demands for conformity, five types of justification are explicated by Sykes and Matza (1957): *denial of responsibility* ("it is not my fault"), *denial of injury* ("no harm will result from my actions"), *denial of victim* ("nobody got hurt"), *condemnation of the condemners* ("how dare they judge me, considering how corrupt and hypocritical they themselves are"), and *appeal to higher loyalties* ("there is a greater and higher cause"). While an emphasis will be placed on these five techniques that Sykes and Matza promulgated, it bears mentioning that other

scho

inclu

you'

doin

inten

least

(Henr

demo

strate

conde

Denial

respons

one's c

students

because

reasonir

and un

widespr

(FTP) s

others d

buying

scholars have specified and studied four additional *a priori* rationalizations. These include *metaphor of the ledger* ("if you weigh all of my good deeds against my bad deeds, you'll see I'm a decent person") (Klockars, 1974), *claim of normality* ("look, everyone is doing it, so how could it be wrong") (Henry, 1990), *denial of negative intent* ("I had no intention of causing any harm") (Henry, 1990), and *claim of relative acceptability* ("at least I am not a murderer or rapist; people engage in much worse activity than this") (Henry, 1990). These final four techniques will be discussed to a lesser degree to demonstrate that they are also applicable to software piracy. All nine are stigma-reducing strategies used to normalize lawbreaking behavior in the face of disapproval and condemnation by others.

Denial of Responsibility

The technique of neutralization advanced by Sykes and Matza called denial of responsibility involves a perception that deviant behavior is a result of forces beyond one's control. Citing the oft-invoked stipulation of being a "poor college student", students can convince themselves that pirating applications and games occurs only because they cannot afford to purchase the product legitimately. According to this reasoning, if it were financially possible to buy the software (often perceived as overly and unfairly priced by manufacturers), there would be no need to download it illegally.

Furthermore, denial of responsibility occurs when students claim that the widespread availability of the software on World Wide Web and File Transfer Protocol (FTP) sites encourages them to take advantage of the situation. Many contend that if others didn't make "warez" (pirated software) so easily accessible, they would resort to buying the products to meet their needs. Interestingly, many pirates do not use every

product they download; they merely compulsively collect each title they can get their hands on, perhaps in order to brag of their vast collection to online friends, or to be able to offer a large selection to another individual to choose from who has a piece of software they desire. The value of these programs, then, is the prestige of ownership, and can be likened to collecting baseball cards just for the sake of possessing them (Pogue, 1998).

In the realm of commerce and industry, there is a prevailing conflict between optimizing benefits for the sustenance and growth of the company and giving the consumer the most utility and worth with their output (Buckley, Wiese, & Harvey, 1998). Accordingly, many pirates often hold that most individuals and businesses in the software industry are egocentric, greedy, and self-serving, and are trying to make or save a "quick buck" any way they can in order to get ahead, to the detriment of the interests of consumers. In order to thumb their noses at the rapacity of these companies, some pirates believe it is acceptable to resort to underhanded practices, such as avoiding payment for software by pirating it, and assisting others to obtain it non grata as a further "slap in the face". Thus, by resorting to an adolescent battle of one-upsmanship with the program manufacturers, pirates can disaffirm the harmful nature of their actions. This misguided reasoning thus conduces to the perpetuation of the crime.

Denial of Injury

In making their decision of whether to engage in the misbehavior, offenders may focus on the recipient of the harm and the degree that another person or entity is debilitated by their actions. In the case of software pirates, they may feel that software companies reap a sizable profit on all of their products, and that a few bootlegged copies will not put even a tiny dent in their presumably impenetrable fiscal armor. If no tangible

and observable harm occurs, then, it is easier to cast aside any reservations and commit the act. Furthermore, software companies may be perceived as having so much capital that they "will never miss" the relatively few dollars of which pirates deprive them, or that they "can afford it". This is an attempt to redefine software piracy in a more acceptable light.

The belief that "no one is getting hurt" is a dominant but misguided belief in the warez scene. Denial of injury frees the delinquent from the moral bind of law so that they are then more likely, willing, and able to commit the act of deviance. Additionally, it may be argued that no tangible harm is occurring since the producers of the product are not technically victims of theft. That is, because only a copy of the product is being pilfered, both parties are left with essentially the exact same possession. Software is nonexclusive and is not consumed by its use, and can be in many places at once without depriving another individual of the opportunity to utilize it. Nevertheless, it bears mentioning that the End User License Agreement (EULA) displayed during the installation of practically all pieces of software is a legal contract outlining restrictions by which the user agrees not to duplicate the program. This agreement continues to state that the purchaser has only obtained a license to *use* the program, and not the right of ownership or the freedom to do with it as s/he pleases (such as distributing it to friends or making it available on a server for public download). Additionally, the agreement prohibits users from electronically transferring the software from one computer to another over a network connection (e.g., the Internet), and from decompiling or reverse engineering the program for the purposes of developing illegal patches to "crack" the software protection scheme and render it ineffective.

It might also be proposed that these lucrative software businesses work into their yearly budget an amount solely allocated to overhead costs related to theft and "softlifting" (Thou, 1984) as a cost of operation. Thus, it might be assumed that funds to cover "shrinkage" are already in place and ready to be used. If the losses are expected, they do not take the company by surprise and presumably cannot be a detriment to their enterprise. This skewed rationalization precludes the idea that harm or injury will occur.

Further, many pirates who break copy protection measures convince themselves that those companies and corporations whose software protection scheme is not a veritable security vault actually *deserve* to have their vulnerabilities uncovered and exploited. The behavior then not only serves to demonstrate the inefficacy of their security measures to prevent "cracking", but also perceivably encourages companies to implement tighter protection features in the future. However, that justification is analogous to saying that because a person does not have an alarm system in his or her house, burglars are entitled to break in and have their way with the possessions and furnishings, and in fact are doing homeowners a favor by exposing a weakness in their line of defense.

Furthermore, as law enforcement agencies have only recently begun to crack down specifically on piracy and computer crime in general, there has never existed a real and viable threat of apprehension and prosecution for online miscreance. As recently as August 1999, the Department of Justice won its *first* pirating conviction under the No Electronic Theft Act (further explicated below), where the distribution of unauthorized files - even in the absence of monetary compensation or profit motive - was deemed illegal (RIAA, 2000). In this case, a 22-year old University of Oregon student pled guilty

to the distribution of pirated software, music, and movies using the school's high-speed network connection (Patrizio, 1999).

Perhaps due to the combination of a lack of technical savvy or interest, and the presence of a traditional mentality of focusing only on corporeal manifestations of lawbreaking through crime control and order maintenance, practices to dissuade potential offenders on the Internet have been severely lacking. This has compromised the ability of police to adequately respond to the increasingly prevalent phenomenom of computer crime. Assumedly, if law enforcement is perceived as unresponsive or apathetic to detecting and sanctioning offenders, students will be unable to internalize the ethical value of refraining from downloading or distributing illegal software, and might be more susceptible to using neutralization techniques to justify their behavior. To a notable extent, the most visible arm of government is behind in regulating and containing Internet crime, and is now attempting valiantly to catch up. However, this lack of enforcement facilitates a lack of awareness of consequences among potential and current pirates, allowing them to deny that any injury takes place.

Denial of Victim

Denial of the victim is another defense mechanism that can be invoked before the commission of a crime. The "softlifters" feel that no one is being physically hurt through the dissemination of unlicensed full-version software, and convince themselves that their actions are perfectly legitimate, even though they are engaging in theft. Sykes and Matza state:

> Insofar as the victim is physically absent, unknown, or a vague abstraction (as is often the case in delinquent acts

> committed against property), the awareness of the victim's existence is weakened. Internalized norms and anticipations of the reactions of others must somehow be activated, if they are to serve as guides for the behavior; and it is possible that a diminished awareness of the victim plays an important part in determining whether or not this process is set in motion. (1957:668)

In software piracy, the victim is not only a corporation rather than an individual, but is also a distant and remote entity seemingly oblivious of any harmful acts against them. In cyberspace, a truly "virtual" plane of existence, these companies have no bearing on the life of a "netizen" (Internet user), and are merely unsuspecting victims from whom to exploit and profit. Therefore, the "Robin Hood Syndrome" occurs when the wrongdoer differentiates between harm done to an individual and harm done to a company or business entity, freeing him or her to more readily discount any misgivings (Harrington, 1996; Solomon & O'Brien, 1990).

Further, although the offender admits partaking in a proscribed deed, s/he argues that retributive harm is deserved by the victimized party because of previous injustices that have been inflicted on others. Thus, similar to the syndrome described above, the offender becomes "a modern day Robin Hood dealing out deserved 'justice' to 'evildoers'" (Pfuhl & Henry, 1993:66). Pirates may feel they are exacting some sort of measure against profit-hungry corporations whose sole aim is to cheat consumers out of their hard-earned money by charging exorbitant prices for their products. Perhaps through piracy the scales are perceived to move closer toward equilibrium. Also, the

fiscal harm enacted on corporations through software piracy is not easily observed by the offender, and often fails to elicit any sentiment of compunction or sorrow. As a consequence, any reservation toward taking advantage of them can be dismissed to facilitate the crime.

Condemnation of the Condemners

The fourth technique of neutralization is condemnation of the condemners. This is where the authority figures in an individual's life, such as parents, teachers, government, and society as a whole, are viewed as corrupt and hypocritical, and therefore not worthy of respect nor submission to their prescribed value system. It challenges and questions the moral superiority of those who make the rules, thus precluding any controls the normative culture seeks to impose. Thus, the attention is shifted away from the person's aberrant behavior, and toward the presumed aberrant tendencies and weaknesses of those whom s/he is expected to esteem and revere, including those assigned the task of enforcing the prescriptive rules of the community. An attempt is made to reconceptualize the righteousness of those "pointing the finger" and dismiss their conventional morality as a farce, so that any censure received is irrelevant and even hypocritical (Young, 1988).

Also, the success of software corporations is sometimes viewed by pirates as due to luck, fortunate circumstances, or monopolistic practices. As such, the attribution of "blood, sweat, and tears" - albeit less dramatic in the business arena - to the growth and achievement of a company is not easily palatable, and is extremely difficult to envision and grasp. This might be due to the lack of "real-world" experiences among college

students and perhaps even a somewhat myopic view of, and an uncultivated deference for, hard work.

Finally, software pirates constantly complain that information should be free, and that the free-flowing exchange of information and programs is what stimulates progress and prevents other programmers from "reinventing the wheel". By not having to repeat the work that others have done, developers and coders can improve on previous software and thus promote growth and unrestrained development. In fact, much of the Internet itself was built on free software; for instance, the sendmail program which drives email correspondence was written and distributed freely, as was all of the initial World Wide Web and USENET software (Hudson, 1995). Increasingly, free operating systems such as Linux (http://www.linux.org) and free office productivity software packages such as StarOffice (http://www.sun.com/staroffice) are being written and distributed non grata for the purposes of promoting the uninhibited flow of ideas and information.

As another example, the Free Software Foundation (FSF) is dedicated to eliminating restrictions on the copying, redistribution, understanding, and modification of computer programs. This organization argues that users should have the freedom to:

> ...run the program for any purpose; study how the program works, and adapt it to [their] needs; redistribute copies so [they] can help [their] neighbor; improve the program, and release [their] improvements to the public, so that the whole community benefits. (What is Free Software, 1999)

However, an inherent fallacy exists in that argument. Software developers should be able to use their talent to earn a decent living, and their commodity should be valued

and worthy of compensation. The capitalistic, entrepreneurial society of the U.S. supports and encourages this in order to promote innovation, and so that programmers and others will continue to be inspired (at least financially) to create quality output.

Appeal to Higher Loyalties

The fifth and final technique of neutralization proffered by Sykes and Matza is the appeal to higher loyalties. If the pirate is a member of a warez group or gang, they may feel they are abnegating their own interests in favor of the welfare of the larger body. The goals and demands of that cohesive unit consequently take precedent over the constraints and directives of the normative culture. Moreover, the friendship and communal needs that are met through these groups foster an alliance to the objective of distributing unauthorized program files, even if this runs patently counter to what the law prescribes. Further, the loyalty engendered to fellow group members and the fellowship afforded by the online kinship, despite its virtual setting and unconventional method of social interaction (such as through typing words on a keyboard), is often enough to lessen the effectiveness of conforming imperatives. Peer pressure greatly influences pirating behavior as it is difficult to deny requests from online friends, and compliance to requests strengthens the individual's allegiance to the group's modus operandi.

The need to succeed in school and to please the family may serve as another justification to render a student morally unaccountable for his or her actions. Parents generally encourage their children to go to college, not only because of the benefit of gainful employment and better pay for those with a degree, but also because earning a college education is commendable and worthy of regard. Also, parents are exceptionally proud when a child has "made something of" himself or herself by attaining this

culturally valued goal, and conceivably some amount of pressure is put on the child to succeed in this way. Pirating useful software may make individuals more able to achieve their scholastic goals, such as doing well on projects and papers and achieving high grades. This, as a corollary, will ideally facilitate the acquisition of a solid, respectable job in the professional arena following graduation, or acceptance into a reputable graduate program. Software piracy then, in the minds of students, is well worth their time, effort, and the risk if it can aid in accomplishing these significant and life-changing aspirations. By using the unauthorized software as the means to attain culturally valued ends, any imputation of a deviant identity by others can be countervailed.

Metaphor of the Ledger

Many criminals rationalize qualms they experience about engaging in a particular proscribed behavior through the metaphor of the ledger. The negative effects of the act in question are mitigated by the aggregation of all the positive effects of past behavior, which are considered to be good. By comparing one's overall good works and constructive traits with the particular instance of the dysfunctional behavior, the current act of simply duplicating a program file can easily be excused and deemed as inconsequential in the "grand scheme of things".

Claim of Normalcy

In the virtual society birthed and shaped by the Internet, one can be exposed to the occurrence of much deviance by simply visiting the appropriate web pages and IRC chat rooms. One method in chat rooms to induce piracy is to issue a few textual commands to a remote user, which initiates an automated transfer of the desired piece of software onto the client computer. Another method is to merely request a particular product in the chat

channel to ascertain if anyone has it on their computer and is willing to send it to you, or provide an account on a server for you to login to and download the program file(s). The proliferation of software piracy an individual witnesses on the Internet demonstrates to him or her that this activity is widely accepted and common practice among a good proportion of netizens. Accordingly, this serves to reduce the perception that piracy is a crime, and subsequently tears down any walls of inhibition that have been erected to keep the individual from committing illegal acts. If so many Internet users are engaging in this conduct, it is surmised, how can it be illegal? This question, and the ensuant lack of a suitable answer, unbridles the individual from any ethical harnesses, freeing him or her to participate in communally accepted behavior.

Denial of Negative Intent

The negative consequences of an act can be denied when offenders are able to dismiss or brush it aside as a joke, accident, or otherwise unintended repercussion. With regard to unlawful software duplication, the contention held is that pirates merely want to see if the program does what it is intended to do before they pay exorbitant amounts of money to purchase it. The fact that there is no criminal motive to steal from the program manufacturers or deprive them of duly merited compensation serves to release them from moral culpability. Assumedly, by evaluating the product beforehand and determining if it meets their needs, software bootleggers can avoid being "ripped off" by manufacturers who put out a less than satisfactory or stable program, or one that does not otherwise live up to its billing. Additionally, the argument being heard with increasing frequency is as follows: if a company charges excessive sums of money for "buggy crashware" that

cannot do what it is supposed to do with reasonable reliability, who is stealing from whom?

Many pirates hold that software corporations are not deprived or cheated out of any capital due to warez because those individuals who use expropriated software were never likely to even consider buying the costly legitimate product in the first place. Further, it is proposed that since pirated software lacks the guaranteed functionality of the legitimate version, as well as user manuals, documentation, technical support, warranties, and upgrades, most average computer users would not bother with it, and that the small minority who do participate in its distribution and use should be left alone. Moreover, with warez the installation procedure is usually quite complex and involves searching for and locating the software on a file archive site, uncompressing files, reassembling them, manually choosing an installation directory, inoculating against viruses which might have been inadvertently included, applying patches, etc. Pirates believe that those who go through the trouble of wading through this somewhat complicated procedure should be left to their own devices. It is even held that warez facilitates a test and experimentation period that increases the notoriety, recognition, and level of popular usage. The reasoning is that pirates can "play around with" the application or game and see if it lives up to its billing, and then recommend it to family, friends, and acquaintances to purchase legally. Thus, by word of mouth, many more customers of the product are created than would have been possible had it not been initially (albeit illegally) downloaded and tried out. Finally, through piracy it is also conjectured that society will become more competitive as the technology from software is more evenly distributed among users, regardless of income level or access restrictions based on employment (Wong, Kong, & Ngai, 1990).

Another method of denying any negative intent often involves the stated guidelines accompanying the dissemination of unauthorized programs. That is, pirates who distribute the software renounce any responsibility of what others do with the unauthorized program and provide it with a caveat: "for 'educational' or 'evaluation' purposes only". This disclaimer allows the pirate to preempt any moral inhibitions and view his or her actions as perhaps tiptoeing the line between a legitimate and criminal act, but never truly crossing over into the realm of actual condemnable behavior.

Claim of Relative Acceptability

Offenders sometimes attempt to demonstrate the relatively insipid nature of their actions by comparing them to other, more deplorable deeds, thereby denying their purported unacceptability to the normative culture. Software pirates are easily able to engage in this technique of neutralization through the isolation and distance afforded to them by the Internet. Online misbehavior is not as readily considered a crime as are real-world violent and property offenses, and this fact precludes any reservations the potential pirate might be experiencing. Also, by subscribing to tenets of moral relativism, pirates can argue that there are no objective moral values, especially in a virtual online setting. In this view, since there are no clear-cut definitions of right and wrong in the real world, how can there possibly exist any semblance of those dichotomous entities in a faceless, nameless society? Pirates can thus engage in the unlicensed copying of programs by citing a lack of existing objective standards.

Neutralization is similar to the constructs derived from Cressey's (1953) analysis of embezzlement. In his seminal work, it was found that embezzlers use verbalizations to redefine the behavior as acceptable to their conscience, often by convincing themselves

that they are merely "borrowing the money". Thus, by stifling any inhibitions or reservations, the individuals are released to commit the crime. Despite the blatant illegitimacy of the act, these rationalizations occur not only after the crime is committed, but also during the behavior to render it permissible and the act unworthy of a "criminal" label. As Cressey (1970:111) states, "I am convinced that the words and phrases the potential embezzler uses in conversations with himself are actually the most important elements in the process that gets him into trouble".

While the similarities of this underpinning to Sykes and Matza's neutralization techniques are worthy of mention, Cressey's paradigm is not used to guide the current research for the following reasons. First, Cressey's study population was a group of middle-aged white-collar workers, already entrenched in the business scene for many years. This group differs significantly from the impressionable (albeit to varying degrees) college youths of the current study who are 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 support themselves. Presumably, embezzlers have had more extensive life experiences from which to draw upon and are generally more grounded in their ethical standards and morals, making them less susceptible to rationalizations than university students are. Sykes and Matza's theory was originally based on studies of juvenile delinquency, and it is perceived as more applicable to a study population of college students. Additionally, the linguistic legerdemain observed in Cressey's work, which was used to characterize the offense in unobjectionable terms, resulted primarily from personal financial problems. Furthermore, embezzlement stemmed from perceiving one's occupation as a means or a tool with which to "get back

in the black" through the use of accessible funds. While software piracy and embezzlement share characteristics of white-collar criminality and can both be considered more sophisticated or advanced in their creation and operation than traditional crimes, the differences that exist are substantial and preclude the applicability of the theory derived from Cressey's research to the present inquiry.

THE HISTORICAL EVOLUTION OF SOFTWARE PIRACY

In previous studies, software piracy was operationalized to include the sharing and duplication of floppy program disks and the misappropriation of application licenses for networks (Cheng, Sims, & Teegen, 1997; Im & Van Epps, 1992b; Rahim, Seyal, & Rahman, 1999; Reid, Thompson, & Logsdon, 1992; Simpson, Banerjee, & Simpson, 1994; Wong, Kong, & Ngai, 1990). In the past five years, however, additional forms of piracy have emerged as the media on which programs and games are primarily stored and sold has switched - from floppy disks, which are each capable of holding 1.44 megabytes (mb) of information, to CDROMs, which can each hold 650 mb of data. These higher density discs allow for easier installations of complex and powerful applications and games, as well as more advanced computing in general. When CDROMs first arrived on the market, they were extremely costly to copy, and one needed specialized duplication hardware not easily accessible through retail channels. However, as the IT industry boomed and the cost of personal computers dropped, CD-recording devices, or "burners" (as they are informally called), have become available for as little as $100, making it quite simple for end users to duplicate commercially created CDROMs, as well as generate their own compilation CDs consisting of various application and game files. Other types of software piracy include purchasing a single license for use of a program and installing it on multiple workstations, and the loading of new hard drives with unauthorized software applications by computer dealers as an incentive for customers to purchase their system (SPA Anti-Piracy Division's Copyright Protection Campaign, 1998).

Another key emergence has been the advent of high-speed connections to the Internet at affordable prices for universities, corporations, small businesses, and other

entities through the leasing of dedicated fiber optic or copper lines from a local or in-house telecommunications company. Furthermore, cable-modems and digital subscriber lines are currently being marketed to home computer users, offering a dedicated high-speed link to the Internet at a very reasonable price. While these technological advances have conduced to a revolutionary paperless form of communication and a burgeoning of productivity for society as a whole, they have made easier the unlawful transferring of illegal files. The exponential growth of the Internet, while becoming an essential fixture in the lives of so many individuals, has also served to increase the occurrence of piracy. According to a recent study by the Stanford Institute for the Quantitative Study of Society, 55% of individuals in the United States have Internet access either at home or at work, and that percentage continues to increase (Study, 2000). Many are being exposed to the seedier corners of the Information Superhighway, where pirates make warez available through easily navigated web sites offering "point-and-click one-stop-shopping to even the most novice of users" (Internet Software Piracy, 1998). A final impetus for the proliferation of piracy stems from the essential mechanics of the act – the transfer and distribution of software from a remote to host computer without personal communication, negotiation, or transaction, and with practically zero risk of detection.

Software products can be classified into two groups: public domain software (shareware, freeware, and demonstration software) and commercially produced software. Shareware products allow individuals to copy and distribute the evaluation software, but demand payment of a registration fee from those who sample the software and 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 is what most computer users are familiar with, where a license to use the program is purchased from corporations and retail stores prior to installation of the application or game. Both shareware, freeware, and commercially produced software are protected by copyright law aside from the stipulations specified above.

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

1. Unauthorized "full-version" software
2. Serial numbers for shareware software
3. "Keygens" (Software Key Generators) -- also for shareware/demo software
4. "Cracks" (programs to modify code in shareware, and unlock 'full version' capability)

These files are available on various web and archive sites, and accessing and executing them constitute software piracy.

Transmission Methods

For the purposes of this study, I will focus on the distribution of pirated software over a network or Internet connection. Software piracy online occurs through a variety of channels:

Bulletin Boards

Bulletin Boards were the first environment in which software programs were exchanged, and were the predecessor to the Internet as we know it today. A software program run on a host's computer would allow multiple users to dial into that computer

via the telephone network and connect to the remote system. Then, file transfers could take place, and requests for particular applications and games could be posted and filled by other users, allowing for the unauthorized sharing of software.

World Wide Web Sites

There is a growing presence of web servers that contain publicly downloadable full-version software files, although due to the more static and traceable nature of the World Wide Web, sites allowing access to these programs exist for the most part as pages of clickable links to other online computers where the files are stored. To clarify, many pirates offer software on remote computers through hypertext links on web pages advertising their wares. By clicking on the hyperlink, the web surfer can initiate a download of unlicensed software onto their computer in the privacy of their home or office, and obtain new and expensive programs without paying a cent. "Cracks", frequently housed on web servers and file archives, are small executable files used to break or bypass the requirement of a serial number, key code, or another piracy protection mechanism of certain applications, or to modify a computer's registry to recognize the software application as legitimate and licensed. Extensive lists of unauthorized license keys and registration or serial numbers for a multitude of applications can also be found on certain web sites.

Email

Email has afforded global netizens the ability to keep in touch and correspond with each other almost instantaneously and without cost (apart from one's subscription fees to an Internet Service Provider). However, advances in email messaging have allowed for pictures, audio, web page files, and even software files, cracks, and

unauthorized keygens to be sent through various networks as an attachment by encoding them as multi-purpose mail extensions (MIME).

IRC

IRC stands for Internet Relay Chat, and provides instantaneous communication and participation in a discussion environment, or "channel". Apart from textual messaging, users can send software, cracks, and keygens to each other through Direct Client to Client (DCC) transfers. The immediacy of IRC also facilitates dissemination of addresses and login and password combinations for sites where the hottest software is currently available for download. This is a great benefit to pirates because sites have a tendency to "go down", or deny remote access after a certain amount of time in order to avoid detection, overuse of bandwidth and computing resources, and "leeching" (constant downloading by those who do not contribute to the site). Additionally, IRC is a hotbed for the trading of software packages so that users can more easily obtain the particular program they seek after supplying another individual with another requested program. Incidentally, the first ever infiltration of a piracy ring on IRC took place in November 1999 as the Business Software Alliance (BSA) and the U.S. Marshals office filed lawsuits against 25 individuals from a channel called "warez4cable" who were distributing illegally copied programs with their high-speed Internet connections (Software Watchdog Attacks Cyberpiracy, 1999).

Newsgroups

USENET newsgroups are the bulletin boards of the Internet, where participants can email messages and have them posted in a particular topical group containing related information posted by other users. These messages are then broadcast to, and replicated

on, interconnected systems all over the Internet, allowing for others to download, view, and respond to the messages. As with regular email, file attachments of pirated program files, cracks, and registration codes can be included and posted, allowing for easy accessibility by other users who view messages in that particular newsgroup.

Personal Messaging Programs (ICQ, AOL IM, NetMeeting, PAL)

These programs are widely used to establish a community where netizens can determine when friends who share common interests are online at the same time. Client-to-client communications can then ensue through sending and receiving instant messages of text across the Internet, which then appear on each participant's desktop screen. Connections for file transfer can also be established between individuals, which can facilitate copyright infringement with the sharing of pirated programs, cracks, or unauthorized license keys.

FTP

File Transfer Protocol is a standard allowing computers on a network to share information, data, and program files easily and efficiently. Computer users can set up FTP daemons, which are applications allowing others to log into one's computer and access directories and files. These are usually restricted by a login and password combination, or a particular Internet Protocol address or mask, so that only certain users can obtain entry. FTP sites are nothing more than computers connected to the Internet configured to allow remote file exchanges, and can house enormous archives of software programs, limited only by the amount of hard drive space available to the owner of the system. Moreover, administrators of these file archives often seal off access privileges very soon after a large number of users try to download software from them. FTP is used

heavily by online warez groups to release and distribute programs from site to site, starting with the upper echelon of software pirates down through the tiers of participants in the piracy scene.

Copy Protection Schemes

Software vendors have used various means to thwart attempts at unauthorized duplication of their products, such as making laser-burn holes in floppy disks, writing data in between disk sectors, varying the format of the data recorded, instituting access locks which verify that the software is being used on the authorized machine during the proper license period, remote server verification where the software contacts another computer across the Internet and verifies the license, and by developing software that will not run without special hardware hooked up to the computer, such as a parallel port key (Im & Koen, 1990; Im & Van Epps, 1992b; Ellis, 1986; Smith, 1997; Swinyard, Rinne, & Kau, 1990; Malhotra, 1994b). In the late 1980s and early 1990s, to prevent piracy of computer games on floppy disks, the software manufacturers would require the user to type in a random word or code from the user manual before allowing the game to be played (Im & Van Epps, 1992b). This, of course, could be countered by making a photocopy of the manual when games were swapped between individuals, but it did cause an inconvenience to many, especially kids and teenagers who traded disks frequently and who did not have easy access to a copy machine.

Recently, computer game manufacturers have devised strategies to thwart duplication of official CDROMs. For instance, some games check to see if the actual, official CD occupies the CDROM drive so that individuals cannot copy the program files to their hard drive, or use a pirated version. This scheme, however, can be easily

countered by making an exact (bit for bit) disk image of the official CDROM, which will be recognized in the drive and accepted by the game upon load. Also, a skilled coder can develop a patch to apply to the game executable file so that it will no longer seek out the drive to verify that it houses the official CD. Another method, yet to be thwarted, involves a central server-based authentication system based on the CD key provided in the purchased game package. When a user attempts to play a networked game over the Internet, the program sends the CD key to a database on the company's server and crosschecks its validity to ensure that no other individuals have attempted to use that particular key. Upon verifying the legitimacy of the license, the user is granted permission to play the game online.

Copyright Law

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 & Koen, 1990; Im & Van Epps, 1992a; Peace, 1997). The law protects these rights for a lifetime plus 50 years for individuals and plus 75 years for corporations. The copyright owner can reproduce, distribute, and create derivative works of the software, and have 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 than running the program from the floppy disk or CD), and the second allowing for a copy to be made 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 & Koen, 1990; Im & Van Epps, 1992a).

Aside from intellectual property protection, under Title 17 of the United States Code, commonly referred to as the "shrink-wrap law," 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 (Peace, 1995; Im & Koen, 1990; 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 used on one computer system; that duplication, distribution, and modification is expressly forbidden; and that any warranty protection is thereby disclaimed (Im & Van Epps, 1992a; Im & Koen, 1990). Copyright infringement may include liability for damages incurred by the copyright owner and/or statutory damages resulting in fines up to $100,000 for every instance of piracy (Peace, 1995; Malhotra, 1994a). If the infringement was performed for pecuniary gain, the fines can increase to up to $250,000 and up to five years in prison (Peace, 1995). The aforementioned No Electronic Theft (NET) Act, signed into law in December 1997, allows for criminal punishments in addition to civil penalties to be doled out to perpetrators of illegal software duplication and dissemination, despite the absence of a profit motive (Software Piracy and U.S. Law, 1998; Warez, 1998). In December 1999, the Digital Theft Deterrence and Copyright Damages Improvement Act were approved, increasing the penalty for intellectual property theft such as software piracy from $100,000 to $150,000 per infringement (Press Release, 1999).

PRIOR RESEARCH

Previous Studies of Software Piracy

A few organizational theories have been posited to explain software piracy, and an even smaller number of criminological theories have been applied to this form of high-tech deviance. Some researchers have attempted to interpret piracy by distinguishing a profile of individuals who would most likely pirate software, focusing on such characteristics as age, socioeconomic class, level of education, level of computer experience, and gender (Peace, 1997; Rahim, Seyal, & Rahman, 1999; Sims, Cheng, & Teegen, 1996). Some studies have shown that software pirates generally are more male than female, younger than older, more comfortable and experienced with computers than novices, and more likely to own a personal computer than not (Wood & Glass, 1995; Solomon & O'Brien, 1990; Sims, Cheng, & Teegen, 1996; Rahim, Seyal, & Rahman, 1999). Others, however, have found that individual variables do not impact the proclivity to pirate (Harrington, 1989; Sacco & Zureik, 1990; Wong, Kong, & Ngai, 1990). Thus, mixed results have been found on the significance of these independent variables, rendering them useless from which to generalize. Parental income, geographical location of the institution, type of educational institution, faculty remarks, and copyright laws are all additional independent variables whose relevance has been measured. No inquiry has addressed how the independent variable of high-speed accessibility affects this particular crime.

Duplication of software programs for private use was not seen as unethical by the sample populations from other research work (Leventhal, Instone, & Chilson, 1992; Wong, 1995). As long as the copied software was not used for profit, 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 address the issue by focusing on individual beliefs from the perspective of an ethical decision (Gopal & Sanders, 1998; Im & 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.

Glass and Wood (1996) applied equity theory to determine the role that situational variables play in facilitating the illegal copying of software between two individuals. According to this perspective, "individuals determine the equity or fairness of their relationships or exchanges with others by assessing the ratio of what they receive from the exchange (outcomes) to what they bring into the exchange (inputs)" (Glass & Wood, 1996:1191). Equity theory suggests that the benefits one expects to receive from providing a legitimate piece of software to another to duplicate is related to what the other individual can provide. If the lender of the software feels that the exchange will produce equitable benefits to both parties involved, it is more than likely s/he will make the transaction. This however only addressed software piracy occurring in a tangible setting, through the borrowing of physical media such as floppy disks and CDROMs.

Christensen and Eining (1991) studied the effects of independent variables such as 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 developed a model utilizing the

theory of reasoned action, deterrence theory, and equity theory, and found that perceptions of authority figures' approval or disapproval affect piracy, while prices of programs do not significantly affect piracy (Christensen & Eining, 1991). In similar studies, however, software prices were shown to be positively related to pirating activity (Cheng, Sims, & Teegen, 1997; Harrington, 1989).

A study by Cohen and Cornwell (1989) found that many college students find software theft and other forms of IT unethical behaviors acceptable, and even condone them as normative behavior. Furthermore, they discovered that students believe professors and administrators also pirate software, which is related to the justification of condemnation of the condemners. 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 & Cornwell, 1989; Oz, 1990; Rahim, Seyal, & Rahman, 1999; Solomon & O'Brien, 1990; Reid, Thompson, & Logsdon, 1992; Wood & Glass, 1995).

Previous Studies of Neutralization Theory

Mixed results of empirical studies on neutralization theory have failed to clarify its scientific adequacy in explaining delinquency. Furthermore, many suffer from methodological problems such as operational definitions (Thurman, 1984). Two such problems are the tendency to confuse neutralization with a lack of commitment to prevailing societal norms, and the use of data better suited to study rationalizations that mitigate misgivings *ex post facto*, rather than moral excuses invoked prior to commission (Minor, 1981; Austin, 1977). Another issue relates to some studies failing to take into account the pertinent causal order between neutralization and delinquency (Thurman,

1984). There seems to be as much evidence to believe that delinquency affects neutralization as there is that neutralization affects delinquency, and the plethora of cross-sectional studies performed are unable to ascertain the direction of this relationship (Agnew, 1994). A brief review of empirical studies on neutralization theory is warranted.

In 1966, Richard Allen Ball developed and used a well-formulated index to measure neutralization, and found that delinquents in an age group of 15-18 were more apt to neutralize deviant behavior than were their nonoffending peers. Incidentally, this scale has been employed and adapted frequently by other scholars in appraising the merit and appropriateness of neutralization in various situations. However, this notion was challenged a few years later through research showing that a sample of sixth-grade schoolchildren legitimized deviant behavior as much as a sample of "tough" boys from an urban area of moderately high crime and delinquency and a sample of institutionalized male juveniles (Ball & Lilly, 1971). In another study, a cross-cultural analysis was performed through Rogers and Buffalo's (1974) work which seemed to indicate that Blacks and Whites both neutralize in a similar manner, although a slightly higher incidence was found among Blacks. An interesting observation posited was that general social situations and conditions of injustice provide Blacks with a genuine source of neutralization; for example, a condemner's racist behavior might supply a basis for the neutralization or rejection of some of the condemner's dictums (Rogers & Buffalo, 1974:325).

An attempt to explore the relationship between the type of crime and the type of excuses used among Florida prison inmates was performed by Minor (1980). The

findings were counterintuitive; it was expected that murderers and assaulters would favor denial of responsibility or denial of victim, while burglars would favor denial of injury, but no statistically significant differences between the type of excuse acceptance employed and the type of criminal were found (Minor, 1980). A year later, Minor (1981) sought to reconceptualize neutralization theory through an empirical analysis of data retrieved through a questionnaire given to a sample of criminal justice college students. Neutralization was speculated to more accurately fit into a framework congruous to subcultural explanations of criminality, since not everyone needs to morally justify his or her deviant behavior before its commission (Minor, 1981:311). Finally, it was suggested that neutralization is only one factor among many others that affect an individual's continuing or discontinuing commitment to the dominant social order (Minor, 1981).

Neutralization was found to be conceptually and empirically different from moral commitment in Thurman's (1984) analysis of a random sample of adults. Neutralization affected the level of involvement in deviance among those who had lower moral commitment, possibly suggesting a subcultural explanation supporting Minor's (1981) assertion. Those with marginal levels of moral commitment were more likely to use neutralization to accommodate any feelings of guilt and to deflect any internal and external demands for conformity. Those who had a high degree of internalized norms of compliance were rendered unsusceptible to techniques of neutralization depraving their adherence to upright standards of behavior (Thurman, 1984).

Hindelgang (1974) questioned the notion that both offenders and nonoffenders are equally adherent to conventional norms, and proffered that most delinquents who participate in deviant behavior endorse, or are at least apathetic to, the act committed.

Hindelgang's main contention is that techniques of neutralization are unnecessary because of the accommodating value system of some individuals, which permits involvement in certain antisocial conducts (Hindelgang, 1974). Contrary to Hindelgang's findings, Agnew (1994) found that only a small portion of respondents condone acts of violence and adhere to a delinquent value system in the first longitudinal study of this theory based on a national sample. Many respondents of Agnew's sample did justify impending deviance through neutralization, which lends support for the temporal order championed by Sykes and Matza that the latter serves to engender the former. It was also found that neutralization has the greatest effect on those who associate with delinquent peers and who have at least a moderate commitment to virtuous societal standards (Agnew, 1994).

Agnew and Peters (1986) found that adoption and use of the techniques occur only when individuals are in situations where the act can be rationalized away as situationally acceptable. It is not enough to be predisposed toward the commission of deviance through exculpatory mechanisms; it is also essential to perceive that the context in which one is immersed is suitable to that act. By differentiating between these two dimensions, a deeper comprehension of the applicability of the theory to various situations is effected, as well as a better understanding of when neutralization will lead to deviance (Agnew & Peters, 1986).

The contention posited in a 1994 study found that the use of neutralization techniques depends on the possibility of ignoring or numbing oneself to the notion of harm befalling another. The degree to which a deviant act induces personal (rather than property) damage and damage to a familiar (rather than unknown or impersonal) victim

were found to be positively related to the permissiveness of delinquents, while the extent of the damage was found to be unrelated (Landsheer et al., 1994). Ergo, it was demonstrated that personal reasoning in conjunction with societal influences affects permissiveness of deviant acts. Moreover, since commission of harm is affected by familiarity with the victim, it may be inferred that the symbiotic relationship between employer and employee might preclude property offenses against the business entity. However, this logic was countered in Hollinger's (1991) survey of employees of businesses, corporations, hospitals, and manufacturing firms in an effort to determine the degree of neutralizing that exists in conjunction with property and production deviance in the workplace. Neutralization was found to be significantly related to the unethical and illegal actions of employees, regardless of familiarity with the victim (the employer), as the highest levels of theft and counterproductivity were reported by those who invoked "denial of injury" and "denial of victim" (Hollinger, 1991).

A summary of the above arguments is asserted by Agnew, who states that delinquency is influenced by neutralizing techniques among those who:

> ...(1) believe they are in situations in which the neutralizations are applicable, (2) have some commitment to conventional beliefs (i.e., disapprove of delinquency, (3) encounter opportunities for delinquency (i.e., situations in which the likelihood of reinforcement for delinquency is high and the likelihood of punishment is low), and (4) have, in the words of Minor (1981:301), a "strong need or desire to commit the offense". (1994:562)

Neutralization techniques have also been shown in a few qualitative studies to be used as justifications for various deviant behaviors. Specifically, the justifications are used by pregnant women seeking an abortion, by international pedophile organizations with the publication of child pornography, and by female adult entertainers to disclaim personal responsibility for topless dancing. For instance, denial of responsibility is used by pregnant women to project blame onto factors such as the lack of birth control information, the difficulties of life, and the cost and sacrifice involved in raising unwanted children. Denial of victim is used to refute the legitimacy of the fetus by describing it in terms of non-human matter, such as a piece of tissue, birth material, or protoplasm (Brennan, 1974). Denial of injury takes place by child pornography publishers when they redefine pedophilia in positive terms by describing the moral, psychological, and even spiritual benefits that children obtain through early sexual experimentation, and by delineating the harms children experience when they are forced to repress sexual tendencies towards adults. Moreover, condemnation of the condemners occurs when these perverse organizations reconceptualize the blamers as individuals or entities who engage in similar exploitative acts for fun, profit, power, recognition, and to spread their own misguided and immoral agenda (Young, 1988). Harm is invalidated by topless dancers by suggesting that rapes, sexual assaults, and other offenses might occur with greater frequency if the patrons of adult establishments were forced to act out their fantasies outside of a protected setting (Thompson & Harred, 1992). Appeal to higher loyalties is employed by topless dancers who contend that their behavior is necessary to benefit others – perhaps to pay for schooling or to raise a child (Thompson & Harred, 1992). These rhetorical defense mechanisms serve to disavow any imputation of a

deviant identity onto the abortionees, pedophiles, and adult entertainers, and render any intrinsic scruples or extrinsic finger-pointing ineffective and easily dismissable.

Neutralization theory has been correlated with various aspects of socially unacceptable and stigmatized behavior since its initial application to juvenile delinquency forty years ago. Individuals use neutralizing techniques to achieve a release or a "moral vacation" from the constraints of the ethical code of society, freeing them to engage in disapproved and criminogenic activities. Neutralization has not been used to apply a theoretical perspective to the distribution of expropriated software among netizens, nor any other computer crimes. The theoretical framework's relevance to software piracy is extrapolated from the exhaustive review of previous research in the disciplines of Criminal Justice, Sociology, Business Administration, Computer Science, and Management Information Systems. The current research attempts to contribute to the existing body of information related to this high-tech crime, and specifically to work to fill the void in criminal justice studies related to online deviance by discussing the applicability of neutralization theory.

PRESENT STUDY

The present study seeks to determine whether the availability of high-speed access to the Internet conduces to, and increases the prevalence of, software piracy. My contention is that neutralization theory, as initially proposed by Sykes and Matza (1957), can be applied to pirating behavior as students temporarily deny the true nature and consequences of their actions to facilitate participation in pirating activity. This conjecture stems from extensive formal and informal research in academic journals, IT publications, the World Wide Web, the USENET newsgroups, Internet mailing lists, and lurking (observing but not participating) in Internet Relay Chat channels to obtain a practical viewpoint from those who participate. With the respondents' self-reported involvement in pirating behavior, as well as their tendency to situationally justify the act, I hope to attain a comprehension of how broadband connectivity, the techniques of neutralization, and participation in software piracy interact.

Hypothesis 1

The presence and availability of Ethernet, DSL, or cable-modem connectivity, and the high-speed Internet access afforded by those technologies, is strongly correlated to, and facilitates, software piracy among students who reside in university dormitories. This assumption is based on the fact that uploading and downloading of even sizeable files can be accomplished rather quickly over a broadband connection, while the transfer and distribution of similar files over a dialup link to the Internet is exponentially slower. Additionally, the existence of this rapid connection to the Internet in the privacy of one's bedroom (which is arguably the primary use of a dorm room), accessible at all hours of the day without interruption or delay, should further effectuate pirating activity.

Hypothesis 1 will be tested first with an independent samples T-test, second with a bivariate correlation matrix, and third with an OLS regression analysis, controlling for neutralization variables as well as for demographic characteristics. Therefore, the first hypothesis will be validated or rejected by determing if those with high-speed connections pirate more than those who do not have such capabilities. The independent variable is whether the individual used Ethernet, cable-modem, or DSL connectivity to access the Internet. Dummy coded, this variable will be used in an independent samples T-test against nine dependent items.

Seven of those eight dependent variables measured some singular aspect of piracy, and included "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?"; "The majority (50%) of software on my computer is legitimately licensed"; and "At least one piece of software on my computer is not legitimately licensed". In order to reduce the number of dependent variables for subsequent analyses, I factor analyzed the seven items and found that only five loaded high on one factor following varimax rotation (See Table 1). These remaining five items, jointly considered a solid and appropriate measure of "Overall Online Pirating Behavior", were also reliable ($\alpha = .76$). With a mean of zero and a standard deviation of one, this newly created continuous item was used as the ninth dependent variable in the T-test and as a singular dominant outcome measure for all ensuing hypotheses and statistical examinations.

Table 1. Dependent Variables To Measure Overall Online Pirating Behavior

Variables	Rotated Factor Loadings	Factor Loadings for Final Dependent Variable Components[1]
"How frequently do you upload/download pirated software to/from others (on average)"	.67	.67
Number of mediums used to pirate software	.78	.78
Degree of Hardcore Pirate	.77	.78
"How often in the last month have you pirated software?"	.72	.74
"How often in the last year have you pirated software?"	.79	.81
"The majority (50%) of software on my computer is legitimately licensed"	-.17	
"At least one program/game on my computer is not legitimately licensed."	.31	

[1] Overall $\alpha = .76$

Hypothesis 2

University students who engage in software piracy do so in part by utilizing one or more of the techniques of neutralization to resolve or suppress any dissonance stemming from the incompatibility between a predominantly ethical value system and the potential unethical behavior. By analyzing a situation, and focusing on particular features which make the current instance an excusable exception to the usual moral response, the potential offender can be loosed from social and conceptual bindings to the normative ethos. Construction of exemptive verbalizations can then occur, which influence the perception of piracy and consequently increase the likelihood of pirating.

Thus, in the second hypothesis I sought to determine if neutralization theory is a fitting framework in which to view software piracy, and whether the usage of *a priori* rationalizations based on situational variables is positively correlated with participation in the crime. Data analysis will occur through a bivariate correlation matrix and from an OLS regression examination, controlling for high-speed access and previous experience with piracy through unlawful CD duplication. The predictor variable utilized was one factor score representing all nine tenets of neutralization (expounded upon below). The dependent item employed was Overall Online Pirating Behavior, the continuous variable produced by the factor analysis discussed in the first hypothesis.

Hypothesis 3

It is predicted that the most salient techniques of neutralization will be Denial of Victim, Claim of Normalcy, and Appeal to Higher Loyalties. These assumptions are made based on: the geographical distance and impersonal relationship between the offender and victim allowing damage done to the victim to be easily discounted; the

observed preponderance of illegal computing behavior online, permitting many to find solidarity in numbers and more readily engage in a commonly practiced activity; and the contention that students are a population particularly prone to participation in questionable activities in order to further their goals. To summarize, the third and final hypothesis will allow me to determine which techniques of neutralization are most frequently used to facilitate piracy. My specific conjecture will be validated using data generated from the tests of Hypothesis 2, and a determination of which neutralization precepts are most applicable will then be made.

Hypothesis 4

My belief is that those who have pirated software using traditional methods (i.e., the duplication of floppy disks and CDs) are more likely to engage in the same act of copyright infringement using the Internet as a facilitating medium. This assumption is based on the fact that individuals will already be predisposed to the crime, and will be familiar with the rewards that come from obtaining a desired application or game for free. Also, the circle of peers who participate in piracy through physical media are likely to have displaced their proclivities online to provide for easier distribution of programs through file transfers, rather than having to duplicate a CD onto a blank disc and give it to someone, either in person or through postal mail service. Another beneficial by-product is that the scope of warez trading can be greatly widened as global connectivity furnishes a large user base and an even larger assortment of program titles to exchange. I suspect that those who are familiar with (and use) CD burners are more likely to pirate software online, as many individuals with high-speed access download massive amounts of warez and then archive each and every program to CD. This is done either to amass a large

collection to provide to others in the future, or in case the individual wants or needs to use an application or game at another time or on another computer. Finally, my prediction is that those individuals who have somehow obtained a pirated copy of software on CD *and* have created a bootlegged CD of software on their own are exponentially more likely to engage in Internet piracy.

The dependent variable utilized in this particular relationship was Overall Online Pirating Behavior. Two independent factors were employed: "I have bought/received/borrowed a copy of at least one software package on CDR" and "I have burned/recorded at least one software package onto CDR". This fourth hypothesis will be supported or refuted based on a two-way analysis of variance test to ascertain each predictor's influence on pirating, as well as if there exists any multiplicative interaction effect between them. Also, an OLS regression analysis will be conducted and will include the techniques of neutralization, the usage of high-speed Internet connectivity, and demographic variables as controls to remove their determining power on Overall Online Pirating Behavior.

Population

The subject population includes university students who live on campus in dorm rooms and predominantly use Ethernet, cable-modem, or DSL connectivity to access the Internet, those in an off-campus apartment or house equipped with high-speed access, and those who primarily use a dialup modem to access the Internet - regardless of living situation or locale. University students residing on site are a study population susceptible to involvement in unethical computing behavior, as many who live in dormitories are provided with high-speed Ethernet access 24 hours a day, 7 days a week. Ethernet is a

local area network (LAN) technology that allows for the transmission of information data between computers at speeds of 10 and 100 million bits per second (mbps). Presently, the most widely used form of Ethernet technology is the 10 mbps twisted-pair variety, which is currently utilized by Michigan State University. External connectivity (the link from the wide area network across campus to the external Internet) is currently provided at 155 mbps, and that capacity is expected to increase in coming months.

More and more individuals are acquiring other forms of speedy Internet services, such as DSL, which stands for "digital subscriber line". This technology facilitates high-speed online connectivity by pushing more data across the copper wiring that houses and business offices already have in place for their telecommunication needs. Asymmetric DSL (ADSL) is the most popular form of DSL technology, and is known for its different download (usually ranging from 1.5-9 mbps) and upload (ranging from 64 kilobits per second to 1.5 mbps) speeds. Individuals obtain this service from their local telephone company, and can expect to pay $30-40 a month for the access.

Another service, the most prevalent form of high-speed home Internet access, involves the use of cable-modems. These devices use the existing cable TV network connection installed in houses to provide a high-speed, dedicated online presence to subscribers. They differ from Ethernet and DSL lines because they are broadcast-based, as all connections share the same bandwidth resources. Thus, during periods when many individuals are online at the same time in an area serviced by a particular cable-modem provider, transfer speeds are markedly reduced as bandwidth is distributed among many by a local router. Speeds can range up to 10 mbps under pristine conditions, but the average download speed on a cable-modem is around 768 kbps, with upload speeds

capped at 128 kbps. In contrast, DSL lines are connected directly to the central telephone office, so no intentional sharing of bandwidth takes place. Cable-modem connections are provided by the local cable company in one's area, and currently cost approximately $40 a month.

Having a fast link to the Internet in the privacy of one's house, apartment, or dorm room, coupled with the necessity to use software for research, papers, correspondence, and projects for coursework or other purposes, lends itself to a significant increase in computer and Internet usage. This increase consequently results in the amplified likelihood of encountering the occurrence of illegal activity on the Internet (such as software piracy), and the chance that an individual will become socialized or somewhat conditioned to condone and ultimately participate in it. Further, researchers have pointed out that colleges and universities are breeding grounds for software 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 lower education or the "working world"). This is evidenced by research findings on the subject of cheating and plagiarism (Agnew & Peters, 1986; Buckley, Wiese, & Harvey, 1998; Crown & Spiller, 1998), as well as on software piracy (Cheng, Sims, & Teegen, 1997; Sims, Cheng, & Teegen, 1996; Im & Van Epps, 1991; Im & Van Epps, 1992b; Eining & Christensen, 1991; Temple, 2000; Wong, Kong, & Ngai, 1990, 1990).

Instrument

An anonymous and voluntary questionnaire, included in Appendix A, has been designed to gather the data required to analyze the relationships in this study. In order to

preclude generalizability issues stemming from the need to infer characteristics and trends from questions eliciting responses about excuses and justifications in general, the instrument was developed to specifically measure software pirating attitudes and beliefs. Additionally, I hope these ad hoc questions will not be subject to varying responses on account of the structure of the questions themselves, but will retrieve a wide range of responses based on differing thought processes and sentiments among students. Questions were asked in as neutral a manner as possible to facilitate open, candid communication from the participants, as well as to avoid the predisposition of responses and any subsequent bias. Software piracy is a controversial topic, and self-reporting instruments usually suffer from underreporting of the deviant activity. Therefore, the survey begins with an introduction defining its purpose; that is, to measure how the Internet has become an integral part of students' lives (addressed via prosocial questions), and to determine students' attitudes and perceptions towards ethical and unethical behavior (addressed primarily via situational neutralization items). The introduction then makes the respondents aware that participation is completely voluntary, and that they are free to not answer any question. Furthermore, anonymity is promised, as the data received in scantron format is not linkable to any person, and no identifying information (such as one's name or student identification number) is to be written on the questionnaire or scantron form. I hope that the inclusion of these guidelines in the introduction, as well as the verbal instructions given at the onset of the survey administration, will encourage a greater number of truthful and objective responses, and aid in garnering an internally consistent cross-section for measuring the prevalence of software piracy.

The questionnaire begins with prosocial questions seeking to discern general sentiments towards the Internet and Internet usage. Items were answerable by choosing a response among a Likert scale of Strongly Disagree, Disagree, Undecided, Agree, and Strongly Agree. This section included questions such as, "I am concerned about security, privacy, and confidentiality on the Internet" and "Individuals should be able to assume different identities, personas, and roles while using the Internet if they so choose". Next, a myriad of items are presented to determine if the respondent uses high-speed, dedicated Internet access, the respondent's purposes for using the Internet, and the amount of time spent engaging in various Internet-related tasks or activities.

Then follows a section intended to ascertain the respondent's level of immersion in pirating activities through esoteric questions generally only answerable by those who frequently participate in the crime. Additionally, a more accurate picture of the transmission methods used to distribute full-version commercial software is assayed through multiple inquiries concerning the various tools and forums which allow for the uploading and downloading of unauthorized programs. A short section to determine frequency and possible past cessation of piracy is also provided.

The core of the survey follows, consisting of a set of 50 questions seeking to measure the applicability of neutralization theory to software piracy, and to acquire an understanding of the underlying motivations and rationales of pirates. Each item presented a possible situational justification or environmental circumstances which the respondent might employ to render piracy an acceptable, or otherwise legitimate, behavior. A respondent could select an answer from the aforementioned Likert scale to indicate the degree to which the given situation would neutralize any reservations or

constraints and allow them to participate in the uploading or downloading of commercial full-version software. Thus, after operationalizing the original techniques into questions specifically designed to correspond to software piracy, the use of neutralization can hopefully be appraised as a determining factor in the degree of participation. It is posited that this set of possible neutralizations is exhaustive, and encompasses the entire range of exculpatory devices that might be employed to facilitate piracy.

The next section seeks to engender possible policy solutions to the crime by inquiring about the time of day the respondent engages in file transfers and whether s/he has pirated in the past with only a dialup connection to the Internet and without dedicated high-speed access. To further explore the motives and cognitive processes of pirates, other questions are posed, including whether any feeling of guilt or apprehension stems from participation in piracy and whether the individual is aware of, and concerned about, the possibility of litigation and criminal charges. The instrument culminates with questions seeking demographic information, such as age, sex, race, socioeconomic status, year of study, and choice of major. These are additional variables that may prove helpful in crystallizing a profile of those individuals who are most likely to pirate. Subsequently, the findings can later be compared to previous studies that developed a profile of those most likely to pirate through conventional means, such as through the copying of physical media from a friend or family member, or by installing software licensed for use by one individual on multiple computer systems. Other piracy variables elicited from the questionnaire and not expressely covered in this paper will be analyzed in a forthcoming work.

As a whole, the inventory is structured in nature, and does not allow for a great deal of freedom or deviation in responses. My hope is that a thorough understanding of the factors that play a role in participation in software piracy can be attained through this comprehensive instrument. Further, I believe an awareness of the behavioral dynamics and personal characteristics of those who engage in piracy will lend itself to the conception of policy initiatives to preclude or combat justifications used to commit the crime.

Principal Issues of the Study

Four primary issues are analyzed:

1. What is the demographic makeup, level of Internet expertise and usage, and proportion of those individuals who engage in software piracy?

The demographic makeup of those who participate in piracy can be analyzed and used to determine whether a certain age, sex, race, socioeconomic status, year of study, choice of major, or level of expertise with computers and the Internet makes a difference in the collective profile of individuals that take part in this crime. This can be used to support or refute previous studies in this area that intended to educe a profile of the typical software pirate, particularly since these previous studies have not examined the student body as a whole but have taken convenience samples of students in introductory Business, Management Information Systems, and Computer Science classes (Buckley, Wiese, & Harvey, 1998; Rahim, Seyal, & Rahman, 1999; Kievit, 1991; Im & Van Epps, 1991; Sims, Cheng, & Teegen, 1996).

The level of expertise with the Internet will be measured with a list of 11 constructs, ranging in degree of difficulty from changing the "startup" or "home" page on

one's web browser, to listening to a radio broadcast online, to configuring the incoming and outgoing servers in one's email program and creating a web page. Having done 0-2 of the 11 items will constitute minimal Internet experience, while having done 9-11 out of the 11 items will indicate advanced or heavy Internet experience. Variety of Internet use - the range of activities the respondent performs on the Internet – was measured with a list of 13 items including research for school work, online auctions, and web page design. Again, the larger the count of items the respondent has participated in, the greater the scope of his/her usage of the Internet. The items in these questions are available for perusal in Appendix A.

2. To what extent do university students engage in software piracy because of their high-speed access to the Internet?

The relationship, if one exists, between broadband connectivity and pirating activities can be demonstrated through the analysis of the computing behaviors of those so equipped. One of the primary independent variables throughout the study is whether the individual uses Ethernet, DSL, or cable-modem online access. Further comparative information is sought through inquiries about past and present Internet activities. By asking questions about individuals' prior Internet use at home (through analog modem) as well as current Internet use at school (through the LAN), I should be able to garner a reliable measure of the level of change between pre-Ethernet and post-Ethernet environments. If the ramifications of this difference due to type of online access are substantial, it can be inferred that the availability and presence of a speedy link is one factor that conduces to this particular computer crime. This construct will be measured with questions including the following: (a) I use Ethernet, cable-modem, or DSL

connectivity in my dorm room, apartment, or house; (b) for which file transferring purposes do you use the Internet?; (c) how many hours/day do you spend on the Internet transferring files?; (d) have you ever uploaded/downloaded pirated software files to/from someone?; (e) before your Ethernet access, did you download pirated software?; and (e) does Ethernet access in your dorm room make it easier to download pirated software from the Internet than a standard telephone/modem connection would?

3. How deep are students' immersion in the software piracy scene?

The level of involvement in pirating activity can be ascertained through statements inquiring about knowledge of particular concepts prevalent in the piracy scene, as well as through probing questions intended to determine empirically the amount of time spent online participating in the distribution or transfer of unauthorized program files. The time availed by students for pirating activities can then be compared to the time period of general Internet usage for innocuous practices such as email, school research, shopping, and games, to determine the degree to which online access is utilized to partake in activities for which it was not designed nor intended. With regard to the amount of time students actively spend online, light Internet usage is coded as 0-2 hours; moderate usage as 3-4 hours; and heavy usage as 6 or more hours. The frequency of the behavior is coded as 1-5 times per month for a small degree of piracy, 16-30 times per month for a moderate amount, and 31 or more hours per month for heavy illegal activity.

The time of day when piracy most frequently occurs will also be obtained through two questions, which will aid in the forumulation of possible policy solutions governing bandwidth allocation. Finally, a construct of Degree of Hardcore Pirate was developed to measure how deeply immersed was the respondent in the pirating scene. This variable

was constructed using an additive scale comprised of eight items including: "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". Since these questions were all dichotomous, an additive model resulted in a range from 0 (for no knowledge of, and no participation in, the pirating scene) to 8 (representing complete awareness of, and participation in, the pirating scene). As previously stated, this item is one of the facets of the Overall Online Pirating Behavior variable.

4. What is the rationale behind engaging in software piracy?

Approximately 75 items were developed during multiple brainstorming sessions to represent the nine concepts of neutralization proposed by Sykes and Matza (1957), Klockars (1974), and Henry (1990). Each question in this section is intended to gauge the tendency of college students to neutralize pirating behavior based on specific situations or conditions. Each subset of questions targets one of the nine previously specified neutralizations, and the set as a whole is deemed to be an exhaustive measure of neutralizations which might countervail dominant and conventional norms as checks on behavior. During construction, the wording and phrasing of the questions, and the perspicuousness, originality, and relevance to each specific technique were taken into

consideration. Equivocal, pointed, and inapplicable questions were weeded out, and fifty final measures of the propensity to neutralize were added to the instrument.

As previously mentioned, responses to these particular items are based on a Likert-scale of Strongly Disagree, Disagree, Undecided, Agree, and Strongly Agree. The first two, indicating reservation about rationalizing criminal behavior, were coded as 1 and 2 respectively. The middle choice of Undecided was coded as 3, and represents an equivocal response to the situation presented. One might argue that a response of "Undecided" is more indicative of the possibility an individual may dabble in proscriptive behavior, rather than refrain completely from any action which challenges his or her moral conceptions. However, as it falls between the contradicting choices of Disagree and Agree, I contend that it is a middle value on the continuum, and should be coded as such. The last two responses were coded as 4 and 5, as they indicate a lack of allegiance to a normative value system and a susceptibility to absolving justifications. The respondent is asked to select an answer based on whether s/he would feel guilty about engaging in software piracy, taking into account the specified stipulation. The alpha levels for each subset of neutralization theory questions are provided in Appendix B. In the instrument, the heading of "Would you be more likely to pirate software:" prefaced all of the situational questions. Also, the heading was repeated throughout in order to increase internal validity, as well as to remind the respondent of the underlying keynote of the questionnaire.

The intention of these neutralization items is to garner insight into the particular motives, rationalizations, and justifications that are used to mediate moral commitment. An idea of how students approve behaviors antithetical to social norms based on

situational or environmental characteristics will also ideally be attained. How do students define pirating behavior as acceptable under certain circumstances? Which circumstances have the greatest influencing power in shaping behavior? The answers to these questions will seemingly be provided through the substantive interpretation of the ethical environment among college students.

In sum, by asking qualitative and quantitative questions about individual Internet usage, the survey instrument attempts to accumulate a thorough understanding of what factors play a role in participation in software piracy. The development of a behavioral model for piracy, taking into account societal, cultural, economic, and environmental influences, will ideally lend itself to the conception of educational, administrative, and legal campaigns and strategies to effectuate change in computing behavior and consequently reduce the damage caused by unauthorized software copying.

METHODOLOGY

In order to construct a sampling frame, a catalogue of the various colleges and academic units at the university was first procured, along with a breakdown of every major housed under them. In each college, one or two majors were randomly chosen. A roster of the classes surveyed is specified in Appendix C. After narrowing down the list to specific majors, searches were run through the university's online database of current courses being offered in an attempt to select particular classes potentially conducive to surveying. Initially, four courses were selected: two lower-level undergraduate courses generally occupied by freshmen and sophomores, and two upper-level undergraduate courses, generally available only to juniors and seniors because of prerequisite limitations. Thus, a conscious effort was put forth to obtain a sample representative of the entire student population, inclusive of freshmen, sophomores, juniors, and seniors.

Additionally, some classes selected were core classes which the university requires all students to take, such as Psychology, while others were endemic to each specific discipline (such as forestry and kinesiology) and would likely not be taken by students not majoring in the particular field. When this listing was finalized, the instructor or professor of each class was contacted to see if s/he would be receptive to granting thirty minutes of the period to facilitate administration of the questionnaire. Seventy classes were initially selected; however, only thirty professors responded positively. Some were unable to accommodate the request, primarily due to the fact that summer courses are inherently tightly packed, as an entire semester's worth of material must be covered in just over a month. In these classes, no time could be detracted from instruction and teaching to allow students to participate in a survey. Conversely, other

professors were able to oblige the research request, and seemingly understood the potential contribution the study might have. When the actual data collection took place, a short verbal introduction of myself and the project was given to the students in each class prior to distribution of the questionnaires and accompanying scantrons. Again, while specified on the survey itself, it was also verbally emphasized that the anonymity of individuals and the confidentiality of data would be maintained. This was done in order to reduce bias usually concomitant with the self-reporting of deviant behavior, and to encourage a greater number of forthright responses.

Surveys were then conducted in twenty-five classes between May and June 2000. A sample size of 507 was derived prior to data cleaning, resulting from an average of 20 students in each class. Upon listwise removal of cases with missing variables, the final sample size totaled 433 cases. Univariate analysis involving the exploration of variables, crosstabs, and descriptives was then performed. Bivariate analysis consisted of determining the correlations between the independent and dependent variables through the use of independent sample t-tests and one-way analysis of variance. Multivariate analyses took the form of OLS regression to determine relationships while controlling for certain demographic and historic pirating variables. These tests are further described below.

Pretest

A draft questionnaire was developed from the pool of items and was distributed to five students and professors at Michigan State University for comments and suggestions. Minor modifications were made based on the responses received to prevent inconsistencies from invalidating the research before its commencement. Furthermore,

feedback was solicited concerning the clarity of each survey item, as well as the tendency of the questions to elicit untruthful responses that might misrepresent the degree of piracy that occurs or the amount of neutralizing that takes place. Suggestions were accordingly incorporated to increase the reliability and validity of the instrument.

STATISTICAL ANALYSES

Descriptive Statistics

Descriptive statistics allow researchers to summarize data in an easily interpretable format, and to identify basic and important measures of distribution. Thus, they will be provided here to paint a broad picture of the respondents' demographics, their use of the Internet and computers, their medium of connectivity, and their knowledge and awareness of software pirating activities online. Furthermore, a comprehensive examination of the sample's perceptions of, and conceptions about, ethical (and, by extension, unethical) behavior on the Internet will be depicted based on these univariate tests. The percentages and numbers provided below are inclusive of a sample population of 507, prior to the removal of missing cases.

Traditionally, demographic information is given first. Continuing with that convention, it was found that the majority of respondents were white (71.8%), female (53.1%), 21 years of age or older (70.6%), and either majoring in Business (23.5%) or a discipline of the Social Sciences (34.3%) (see Table 2). Annual income of the parents of respondents was expressed to be $50,000 or more by 69.4% of respondents. Despite the reasonably comfortable economic status of most families, though, three-fourths (74%) of the students who participated in the study worked at least 10 hours a week. Of those respondents who were employed, use of a computer at their jobs was evenly distributed among "minimal", "moderate", and "heavy" in intensity.

Table 2. Demographics of Software Pirates

Demographic Statistics	Total Sample Percentage	Piracy Measures 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?"

Most individuals indicated that the Internet was not "indispensable" to them - a surprising finding to me, as I assumed that the wealth of informational resources online would render it absolutely essential for any college student. Another interesting observation gleaned from the data was that only 31.4% of respondents reporting using the Internet to meet their social needs. With the continually burgeoning popularity of instant messaging programs such as America Online Instant Messenger and ICQ (with 59 and 71 million users respectively, according to their official web pages in July, 2000), it was thought that the percentage would have been higher. With respect to ideas about the new public and social issues that have been birthed by the growth of the Internet, a number of important conclusions can be made. Interestingly, most students (68.6%) are not concerned with security, privacy, and confidentiality issues online. This was found despite the media frenzy that seems to habitually ensue upon every hacking attempt on a major web site, every discovery of new technology that collects information about visitor demographics or web surfing practices, and every instance of disclosed credit card or personal information from e-commerce web site databases. Almost half (43.4%), however, were cognizant of, and concerned about, copyright infringement online, and did not believe that information, graphics, and files posted to the Internet are free rein for anyone to use (60.4%).

In general, the student sample has been using the Internet more as each year goes by, has been an Internet surfer for over three years, and has worked with computers for seven or more years. One of the survey questions presented a list of common Internet activities, ranging from research for school work to stock trading to the collection of personal-, hobby- or interest-related information, and asked each respondent to count up

how many s/he has done. Most (41%) have used the Internet for 6-8, or approximately half, of the items. To indicate proficiency of Internet use, another list was proffered, delineating a list of items of varying difficulty levels. Some of these included changing the 'startup or 'home' page in one's web browser and setting up the incoming and outgoing server preferences in one's email client. The findings for this question were not normally distributed like the prior example, but were weighted towards the lesser ranges, as 57.4% had done four or less actions and only 20.7% had done seven or more actions. It is suspected that if a larger number of computer science and engineering students were included in this sample (only 8.9%, or 45 of the 507 individuals in this study), many more would have done most, if not all, of the items on the list. Almost three-fourths (74.1%) of those queried spend between zero and ten hours on the Internet each week. Time spent in various online activities was further dissected, and it was revealed that most students spend less than one hour a day chatting or instant messaging, less than one hour browsing the World Wide Web or the USENET discussion groups, and less than one hour transferring files (of any type).

As the specific topic of this paper is software piracy, it was imperative to obtain statistics related to that particular behavior. When inquired about their perception of the frequency of piracy on the Internet, most (30.4%) gave the middle response of "Occasionally prevalent", with the rest of the answers evenly distributed around the mean. As expected, more individuals (58.2%) do not know how to obtain pirated software over the Internet, compared to those who do. The size of that percentage is cause for concern, especially when coupled with the fact that one-third (33%) have unlawfully transferred at least one copyrighted application or game online. While 84.4%

spend less than one hour per day transferring files, 41% reported that they transfer pirated software one to five times per week. In the last month and last year, the vast majority (89.2% and 82.6% respectively) have transferred software between zero and five times. Remarkably, in a question that speaks volumes about perceptions of ethical computing behavior, 48.4% revealed that they would not feel guilty about pirating software. One-fourth of the respondents (25.4%) chose "Undecided", and it is presumed that these individuals might be most likely to use the techniques of neutralization to influence their behavior in one direction or the other, based on certain situational characteristics.

Reinforcing the lack of an inculcation of computing ethics is the finding that 63.3% of those who distribute pirate software do not regard it as improper or intrinsically wrong. This determination is somewhat disquieting, particularly when considering the legion of news reports on the increasingly panoptic controversy surrounding the online distribution of intellectual property in the form of digital music files. Other findings along the same lines, and indicative of the power of sanctions to dissuade or deter pirating behavior, were that the majority (52.7%) of students who pirate software do not believe they will ever be disciplined for their copyright infringing activities. Moreover, the threat of legal repercussions and fines are, according to the responses, irrelevant at best and laughable at worst, with 72.4% unconcerned about the law's mandates. Moreover, the research ascertained that one in five (19.8%) of those who have pirated software had more illegitimate than legitimate software on their computer, and that half (49.9%) had at least one application or game on their computer that was not properly licensed.

It is also suggested that the more mediums an individual uses for pirating activities, the greater his or her knowledge of, and immersion in, the criminality.

Mediums for transferring software included a web browser, to/from the USENET newsgroups, using an instant messaging program, using a chat program, logging into an FTP server to upload/download to/from others, and setting up an FTP server to allow others to do the same. Nearly half (44.3%) had done at least one of the above, while 20.1% had used 3-4 mediums to illegally obtain or distribute software. Not surprisingly, the most popular medium to unlawfully obtain copyrighted applications or games on the Internet was through a web browser. Interestingly, the distribution of Degree of Hardcore Pirate demonstrated that 56.2% scored 1 or higher. That is, the majority of respondents have participated in at least one activity considered an indicator of immersion in the software piracy scene.

Past studies have focused exclusively on copyright infringement through the exchange of software piracy on physical removable media, such as floppy disks. With the increase in availability and decrease in cost of CD Recorders or "burners", I sought to discover whether the sample population had participated in piracy through this process. An sizable 55.6% of respondents had bought, received, or borrowed a copy of at least one software package on a recordable CD, with 31% indicating that they themselves had made such a CD copy using a burner. While this illustrates the growing ubiquity of CD Recorders in personal computers, it also provides evidence that college students are contributing to the widespread theft of intellectual property through traditional duplication of software discs (or disks). This corroborates the research of previous scholars, who had analyzed piracy through disk copying in a university setting.

The impetus for this thesis was the supposition that high-speed online access might be facilitating intellectual property theft in general, and specifically software

piracy, on campuses around the nation. No research until the present had attempted to discover how broadband connections affect the frequency and prevalence of piracy. While extensive analyses between specific variables will be conducted later, it is important to point out that the univariate statistics garnered from the current study lend support for this hypothesized causal relationship. More than one-third (37.2%) of students queried were equipped with Ethernet, DSL, or cable-modem access to the Internet; this figure most likely would have been higher if the questionnaire had been administered during the fall or spring semester, when the number of students who occupy campus resident halls is greatly increased in number.

In addition, approximately one-fourth (21%) of those who pirate software also did so prior to obtaining a broadband connection, and a almost one-third (30.3%) stated that without the fast, dedicated link to the Internet, they would still transfer copyrighted works over a dialup modem. In fact, one-fifth (22.3%) revealed that their pirating habits would remain as frequent regardless of their connection speed. It is evident that while it would take longer with a slower pipeline - perhaps hours or days to obtain an application or game of respectable size – this group of students would gladly wait in order to achieve the same end result – the acquiring of a desired piece of software at no cost.

One-fourth (23.7%) of students surveyed have transferred pirated software prior to starting college. Moreover, 34.9% have uploaded or downloaded illegal programs since obtaining connectivity in their current living situation. An overwhelming two-thirds (67.2%) of respondents expressed the sentiment that high-speed Internet access makes it easier to pirate software than a standard dialup connection would. This demonstrates that having a faster connection to send and receive data invariably contributes, at least in the

mind of students, to the commission of piracy. These findings legitimate an overall cognizance by students of software piracy on the Internet.

Bivariate Statistics

Bivariate statistics are used to measure the presence and strength of a relationship between two variables. The first analysis conducted involved independent sample T-tests to determine if the pirating activity of those who had high-speed Internet access differed from those who did not. The sample means are higher for every piracy variable for those who have high-speed Internet access, indicating that respondents so equipped pirate software with greater incidence and frequency than those who are not. Further, the findings derived from this analysis show support for the contention regarding the relationship between the means of the independent and dependent variables in the population. Assuming unequal variances, the t-statistic for "At least one program/game on my computer is not legitimately licensed", "How frequently do you pirate per week", "Degree of Hardcore Pirate", "I have transferred at least one piece of pirated software to/from someone", "Number of mediums used to pirate software", and Overall Online Pirating Behavior all were significant at the .05 level. These items are further specified in Table 3, and support the first hypothesis. Significant negative relationships exist for six piracy variables, as the calculated t value fell outside the prescribed critical value of -1.96 and five of six alphas fell below .01, with the sixth alpha level less than .05.

Table 3. Independent Samples T-Test: Dialup (D/U) vs. High-Speed (H/S) Internet Access and Piracy Variables

Dependent Variables	Means (D/U)	Means (H/S)	Mean Difference	t
How often in the last month have you pirated software?	1.14	1.20	-.06	-.95
How often in the last year have you pirated software?	1.25	1.43	-.18	-1.94
The majority (50%) of software on my computer is legitimately licensed.	.70	.77	-.07	-1.76
At least one program/game on my computer is not legitimately licensed.	.41	.51	-.10	-2.03*
How frequently do you pirate per week?	1.37	1.59	-.22	-3.39**
Degree of hardcore pirate	1.15	1.76	-.61	-3.26**
I have transferred at least one piece of pirated software to/from someone	.28	.46	-.18	-3.79**
Number of mediums used to pirate software	.78	1.39	.61	-4.01**
Overall Online Pirating Behavior	-.14	.24	.10	-3.48**

* Correlation is significant at the 0.05 level (2-tailed).

** Correlation is significant at the 0.01 level (2-tailed).

A correlation matrix was next created with the predictor and dependent variables to discover which items were related, and how strong of a relationship existed between those items. As evidenced by Table 4, "I have burned/recorded at least one software package onto CDR" - a measure of traditional pirating activities - is significantly correlated to overall Internet piracy (r=.38). The coefficient of determination for that predictor is $(.38)^2$, or .14. As a Proportionate Reduction of Error statistic, it can be concluded that 14% of the variation in overall Internet piracy can be explained by, or attributed to, previous experience with the creation of pirated CDROMs.

Table 4. Bivariate Correlation Matrix for High Speed Access, Neutralization, and Piracy Variables

	A.	B.	C.	D.	E.	F.	G.	H.
A.	1.00	.11*	.17**	.18**	.08	.10*	.18**	.09
B.		1.00	.44**	.38**	.06	.30**	.22**	.10*
C.			1.00	.40	.03	.21	.38	.08
D.				1.00	.07	.31**	.49**	.13**
E.					1.00	.18**	-.10*	-.01*
F.						1.00	.25**	.11*
G.							1.00	.20**
H.								1.00

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Opportunity Variable

(A). I use high-speed Internet access

Past Piracy through Physical Media (duplicated CDROMs) Variables

(B). I have bought/received/borrowed a copy of at least one software package on CDR

(C). I have burned/recorded at least one software package onto CDR.

Internet Piracy Variables

(D). I have transferred at least one piece of pirated software to/from someone.

(E). The majority (50%+) of software on my computer is legitimately licensed.

(F). At least one program/game on my computer is not legitimately licensed.

(G). Overall Online Pirating Behavior

Neutralization Variable

(H). Overall Neutralizing Behavior is significant at the 0.01 level (2-tailed).

Overall neutralizing was positively related to "I have transferred at least one piece of pirated software to/from someone" ,"At least one program/game on my computer is not legitimately licensed", "I have bought/received/borrowed a copy of at least one software package on CDR", "The majority of software on my computer is legitimately licensed, "and "Overall Online Pirating Behavior", demonstrating that the incidence and onset of piracy among those who employ the nine techniques of neutralization is greater than those who are not prone to justifying their behavior. These findings lend support for the second hypothesis.

Interestingly, neutralizing was not related to "I have burned/recorded at least one software package onto CDR", a variable that measures deeper involvement in the pirating scene. Perhaps as individuals become further entrenched in software piracy and reach the stage where they are duplicating and distributing pirated CDs that they have created, they no longer feel the need to rationalize their actions. It is possible that neutralization is only necessary at the onset of participation in this specific crime, and once the behavior increases in frequency and scope, it becomes more readily acceptable. Future research will seek to determine the causal time order of neutralization on piracy.

Use of broadband Internet access was also included in the model and compared to the variables that measured piracy. As depicted in the matrix, high-speed connectivity was significantly related at the .01 level to illegally transferring at least one piece of pirated software and with the measure of "Overall Online Pirating Behavior". This provides some evidence that Ethernet, cable-modem, or DSL Internet users are more likely have participated in piracy, perhaps because of the easy accessibility and rapidity of a dedicated file transferring pipeline.

Unarguably, these correlations remain relatively weak, perhaps because of the amount of variation that must be explained. In fact, the trend throughout the bivariate correlation results is that in general, the independent and dependent variables are significantly related to each other; however, not much differentiation can be made. Overall, the third hypothesis - which predicted three distinct tenets of neutralization to be most applicable to pirating behavior - was unable to be tested in this analysis.

One-way analysis of variance (ANOVA) was also conducted to see how categorical variables might be inserted into the picture as influencers of pirating behavior. Proficiency in Internet-related activities, such as participating in an online auction or creating a web page, is expected to be positively related to pirating behavior. Succinctly put, it is supposed that the more capable and skilled an individual is in the performance of online actions, the more likely the possibility that s/he pirates software.

ANOVA tests to see if the population means are equal by determining the significance of the difference of the sample means. Those who engaged in six or less items of the variable measuring Internet use proficiency rated negatively on pirating behavior (see Table 5). As anticipated, those who had performed seven or more items were most likely to rate highly on overall pirating behavior. The significance for F is .000, and falls markedly below the standard .05 alpha level. Therefore, at least one category of the independent variable in the population significantly influences pirating behavior.

Table 5. ANOVA of Proficiency of Internet Use and Overall Online Pirating

Proficiency of Internet Use	Mean	F
0-2 items	-.35	26.578**
3-4 items	-.12	
5-6 items	-.06	
7-8 items	.28	
9-10 items	1.32	

** Correlation is significant at the 0.01 level (2-tailed).

The Bonferroni Post Hoc test determines which of the five predictor categories differ significantly from the others in their power to influence the dependent variable in the population. The alpha level for comparisons of the category of 9-10 items with the other categories was .000, indicating that a higher degree of Internet proficiency, as measured by this scalar variable, is likely to differentiate those in that category from the others. Eta squared (η^2) measures how much total variation can be attributed to the variation that occurs between groups, and was obtained by dividing the Between Groups Sum of Squares (89.955) by the Within Groups Sum of Squares (346.045). η^2 was found to be .2559. That is, 25.6% of variation in the population for overall online piracy can be explained by proficiency in Internet use. As an assessment of strength, it is indicative of a moderate relationship between the predictor variable and pirating activities.

A survey item to measure variety of Internet use was utilized in order to ascertain the relationship between broader employment of online resources and overall pirating behavior. The sample means allow me to conclude that those with a higher degree of variety in their online activities pirate more, as measured by the dependent variable. Furthermore, the significance of F (.000) indicates that at least one category mean is

different from the others in the population (see Table 6). The Post Hoc comparison test found that the alpha values for the category of 12-13 items was significantly different from 0-2 items (α=.01), 3-5 items (α=.00), and 6-8 items (α=.00), signalling that those who used the Internet in a wider context were significantly different in their pirating than those whose online use was more specific. However, 12-13 items was not differentiated from 9-11 items (α=.094). Thus, it seems a demarcation can be made between 0-8 items and 9-13 items, and 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 are substantively different in their pirating behavior than those who only utilize the Internet for a few specialized functions. A relatively small 12.8% of variation in the dependent variable is explained by this predictor.

Table 6. ANOVA of Variety of Internet Use and Overall Online Pirating

Variety of Internet Use	Mean	F
0-2 items	.10	13.666**
3-4 items	-.28	
5-6 items	-.08	
7-8 items	.42	
9-10 items	1.02	

** Correlation is significant at the 0.01 level (2-tailed).

Other one-way ANOVA tests revealed that freshmen differed from the other years of studies in pirating behavior; this statistic, however, cannot be considered internally consistent as only four freshmen were surveyed. A question intended to determine general adherence to a normative value system – "Generally speaking, I would feel guilty for pirating software" – did not significantly differentiate users in their level of software

expropriation, with the only significant difference existing between the responses of Strongly Disagree and Undecided. Those who strongly opposed the statement "I am concerned about copyright infringement on the Internet" were significantly different from the other Likert-scale categories in the mean level of overall pirating behavior in the population. However, only 4.43% of the variation in pirating was due to this predictor variable. Finally, the number of years an individual has been using the Internet did not matter in distinguishing higher levels of pirating activity among respondents.

Multivariate Statistics

To determine if the means of online pirating for those who participated in software piracy with physical removable media were significantly different in the population than those who did not, two-way analysis of variance was employed (see Table 7). The overall model - a measure of the influencing power of all factors and interactions involved on the dependent variable - was significant. Also significant was whether the individual had facilitated intellectual property theft through the use of his or her own CD burner. However, no differentiation was evident among those who had simply used an unauthorized CD copy, nor was there an exponential interactive effect among the independent variables apart from their additive power. Based on the analysis, involvement in piracy through physical media accounts for 15.3% of variation in the unlawful duplication of software over a network connection. To summarize, merely having exchanged or obtained pirated software on CD is not significantly related to online piracy, but having burned or recorded pirated software onto CD is a significant predictor of uploading or downloading warez on the Internet. This lends partial support for the fourth hypothesis.

Table 7. Two-Way ANOVA of CDROM Piracy and Overall Online Pirating

Variable	F	Sig.
Corrected Model		.000
V30 – "I have bought/received/borrowed a copy of at least one software package on CDR"	.036	.849
V31 – "I have burned/recorded at least one software package onto CDR"	43.033	.000
V30 * V31	2.457	.118

R Squared = .153 (Adjusted R Squared = .147)

To empirically evaluate the viability of the four hypotheses, Ordinary Least Squares regression was performed. This multivariate analysis was used to examine all of the variables together; that is, to determine the influence of the predictors on pirating, controlling for demographic and historic pirating variables. Three models were created to evaluate the relationship of the variables, and the findings are summarized below.

The first model aimed to determine the relationship of demographic variables to Overall Online Pirating Behavior. Sex, race, age, college major, year of studies, employment status, parent's annual income, father's educational level, and mother's educational level were included to control for the sample characteristics. Those who were male, nonwhite, and not majoring in Social Science or Business had increased levels of Internet piracy. Only 7% of variation was explained by demographic differences among respondents.

Table 8. Model I: OLS Regression Analysis on Overall Online Pirating (n=433)

Model Predictor	Std. Error	Beta	t
Constant			
Demographic Variables			
Male?	.10	.19	4.01**
White?	.11	-.11	-2.19*
21 or older?	.12	-.02	-.35
Social Science Major?	.11	-.13	-2.54*
Business Major?	.13	-.13	-2.35*
Senior?	.12	.01	.13
Employed?	.11	-.03	-.54
Family makes $50,000 or more?	.11	-.01	-.24
Father has his College Degree?	.11	-.09	-1.63
Mother has her College Degree?	.11	.07	1.32

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).
R Squared = .07

The second model incorporated three independent variables to determine the impact of opportunity and past piracy: "I use Ethernet, cable-modem, or DSL connectivity in my dorm room, apartment, or house"; "I have bought/received/borrow a copy of at least one software package(s) burned onto a CD-R (custom-made CD)" and "I have burned/recorded at least one software package onto CD-R (custom-made CD)". Once again, the dependent variable utilized is Overall Online Pirating Behavior.

As expected, there is a significant positive relationship between high-speed Internet access and overall pirating (see Table 9). This supports the first hypothesis that speedy and dedicated online access facilitates software piracy. An interesting finding stemmed from the control variables included to assess the influence of past pirating behavior involving tangible removable media (such as the duplication of CDROMs). It was discovered that those who have used a copy of a program on an unauthorized and

duplicated CD are no more likely than their counterparts to pirate. However, those who own a CD burner, and have created and recorded CDs themselves, are significantly differentiated in their pirating activity than those who have not. Owning and using a recording drive to duplicate software increases pirating behavior, once again affirming one aspect of the fourth hypothesis. To reiterate, while obtaining broadband connectivity increases overall pirating, having experience with the creation of illegal CD duplications of software differentiates pirates to a larger degree. The explained variation of Model II, based on these three predictor variables, is 21%, a notable increase from Model I.

Table 9. Model II: OLS Regression Analysis on Overall Online Pirating (n=433)

Model Predictor	Std. Error	Beta	t
Constant			
Demographic Variables			
Male?	.10	.12	2.71**
White?	.10	-.08	-1.79*
21 or older?	.11	.02	.37
Social Science Major?	.10	-.13	-2.60**
Business Major?	.12	-.09	-1.89
Senior?	.12	-.01	-.22
Employed?	.10	-.04	-.94
Family makes $50,000 or more?	.10	-.05	-1.02
Father has his College Degree?	.10	-.09	-1.69
Mother has her College Degree?	.10	.05	1.01
Opportunity and Physical Media Variables			
I use high-speed Internet access in my home	.09	.10	2.12*
I have bought/received/borrowed a copy of at least one software package on CDR	.10	.08	1.60
I have burned/recorded at least one software package on CDR	.11	.31	6.19**

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).
R Squared = .21

The third model added the variable of Overall Neutralization Behavior to determine whether *a priori* justifications lend themselves to an increased amount of Overall Online Pirating Behavior (see Table 10). As mentioned earlier, the usage of neutralization techniques in freeing each student from any imposed constraints of ethical computing was measured with a series of questions, each of which presented a particular situational aspect or characteristic which may or may not influence the student to pirate. Arrival at this one measure of the theoretical perspective warrants description. The nine techniques each were represented by varying numbers of questions: Denial of Responsibility was measured with 11 items (two were subsequently deleted because they did not satisfactorily differentiate between those who were more and less likely to pirate); Denial of Injury, 6 items; Denial of Victim, 4 items; Condemnation of the Condemners, 5 items; Appeal to Higher Loyalties, 6 items; Metaphor of the Ledger, 5 items; Claim of Normalcy, 4 items; Denial of Negative Intent, 7 items; and finally, Claim of Relative Acceptability, 3 items.

A reliability analysis was first conducted to determine which variables are more dependable in differentiating individuals and in measuring the respective construct. The derived alpha values all fell above .8, and are specified in Appendix B. Furthermore, for practically every item in the section designed to measure the applicability of neutralization theory, the alpha values would have decreased if the question was removed from the analysis. Then, because of the large number of items, a factor analysis was conducted to make sure that each set of observable measures was specifically identifying a particular, heretofore unobservable concept (that is, a technique of neutralization).

For Denial of Responsibility, the factor analysis revealed two primary constructs with Eigenvalues over 1. Two questions were subsequently discarded because they loaded high on each factor, and the analysis was rerun. The Eigenvalue for the second construct remained greater than 1. However, upon closer examination, it was detected that the first construct explained 50% of the variance among the items, while the second explained only 14%. Also, all factor loadings for the Denial of Responsibility variables were greater than .6. A subsequent scree plot validated the contention that there existed only one dominant factor. Finally, as noted in the table below, the alpha value for the items in totality was .90, which indicates that if an individual answered one way for a particular question, it is very likely that s/he answered the same way for the other items in the set. For these reasons, a one-factor solution was forced. The sets of questions measuring the eight other tenets were also found to be very consistent measures of each construct, and loaded highly on their respective factor scores. Consequently, these nine variables, normally distributed with a mean of zero and a standard deviation of 1, were considered to be solid appraisers of Sykes and Matza's techniques of neutralization. Please see Appendix B for the factor score breakdown and reliability analyses on these items.

When they were included in the regression model however, a few techniques were found to be positively related to Overall Online Pirating Behavior, one was found to be inversely related, and the others were not found to be related at all. This indicated to me that the tenets could not be adequately and reliably differentiated from each other in the manner that I had sought, and necessitated aggregation into one factor score measuring Overall Neutralization for inclusion in the analysis. My theoretical justification for

piracy, then, had to be measured at a macro level, rather than specifically identifying which techniques were most conducive to the crime. Therefore, responses from the fifty situational questions in the survey were factor analyzed. Seven components were initially derived with Eigenvalues over 1, but a one-factor solution was forced as 45.2% of the overall variance was explained by the first component. This produced a singular variable to measure one's proclivity to neutralize and was used in the regression analysis to ascertain the theory's applicability to Internet piracy.

Table 10. Model III: OLS Regression Analysis on Overall Online Pirating (n=433)

Model Predictor	Std. Error	Beta	t
Constant			
Demographic Variables			
Male?	.09	.12	2.56*
White?	.10	-.08	-1.72
21 or older?	.11	.02	.43
Social Science Major?	.10	-.13	-2.79**
Business Major?	.12	-.09	-1.80
Senior?	.11	-.01	-.22
Employed?	.10	-.03	-.77
Family makes $50,000 or more?	.10	-.04	-.95
Father has his College Degree?	.10	-.08	-1.67
Mother has her College Degree?	.10	.04	.86
Opportunity and Physical Media Variables			
I use high-speed Internet access in my home	.09	.09	1.95*
I have bought/received/borrowed a copy of at least one software package on CDR	.10	.07	1.34
I have burned/recorded at least one software package on CDR	.11	.31	6.21**
Theory Variable			
Overall Neutralization Behavior	.04	.16	3.55**

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).
R Squared = .23

Male respondents and non-Social Science majors were still more likely to pirate. Also, the significance of high-speed access and piracy through the creation of physical media both hold after inclusion of these additional variables. Of the variation in the dependent variable, 23% can be attributed to the group of predictors. Thus, very little predictive power was gained through the addition of the neutralization construct, a likely indication that while Sykes and Matza's theory is a suitable framework in which to view intellectual property theft, opportunity and past piracy differentiate among online pirates to a much greater degree. In sum, potential employment of the techniques of neutralization, broadband access to the Internet, and previous pirating behavior with recordable CDs are the most important determinants of Internet piracy (with the latter continuing to be the strongest predictor with beta = .31).

Unfortunately, due to the limitations in my conceptualization of the questions to measure each respective neutralization precept, I was unable to specify exactly which of the nine individual techniques were most important predictors of piracy. As such, I could not test if Denial of Victim, Claim of Normalcy, and Appeal to Higher Loyalties were most frequently employed to discount any misgivings or cast aside any need to adhere to social and legal constraints, thus freeing the individual to commit the crime. This leaves Hypothesis 3 unproved. Furthermore, because of a general inability to identify all of the aspects that most lend themselves to this little-studied high-tech crime, much variation in the dependent variable remains to be explained. I hope that I am able to determine in future research another factor that will better differentiate software pirates.

The impetus for this research was the conjecture that high-speed access facilitates software piracy to some degree. However, not much overall variation in pirating could be

attributed to broadband connectivity. The theoretical components of neutralization theory were then added to the empirical assessment and accounted for much more variance in the dependent measure. Finally, demographic characteristics were included, and only slightly more variation was elucidated. The second hypothesis, which stated that Sykes and Matza's neutralization theory was an applicable perspective with which to view software piracy, is hence corroborated.

It bears mentioning at this time that in each of these models, F was significant, signalling that the variables utilized were a good fit for the analysis. Also, the tolerance and variance inflation factor statistics for each model did not indicate a problem of shared explained variance among the independent variables. This occurred when each of the nine neutralization tenets was included both separately and together into the OLS regression, as well as when the one variable of Overall Neutralization was included.

LIMITATIONS

A few limitations exist in attributing software piracy to Sykes and Matza's neutralization theory. First, the theory does not indicate why some students engage in software piracy and why some do not. It focuses on the reasoning behind the behaviors rather than the initial decision to contemplate the behavior itself. What makes software piracy attractive in the first place? The theory is based on rationalizing processes originating before the act occurs, but why some are more likely than others to have that penchant towards deviance is not determinable. The theory also assumes that individuals are committed to the mores of society well before the option for transgression even presents itself. If no bond to convention exists in the first place, there would be no need to use techniques of neutralization to evade obligations to societal laws (Lanier & Henry, 1998). Thus, since there are varying degrees of commitment to the dominant culture, perhaps those distinctly committed to antisocial standards do not employ neutralization to weaken or sever any potential constraints. Additionally, it is difficult to determine the causal order involved with a cross-sectional study – that is, if neutralizing techniques and verbalizations are employed before, during, or after piracy takes place. Finally, the theory does not establish how the techniques, motives, and rationalizations for committing piracy are learned by new offenders, or how piracy first became a problem. Only one longitudinal study could be located that provides an empirical analysis on neutralization theory has been performed (Minor 1981).

Neutralization theory, as posited by Sykes and Matza (1957), holds that offenders only justify the misbehaviors that they themselves commit (McCarthy & Stewart, 1998). It needs to be determined if, and to what degree, software pirates use (or would use) these

rationalizations to disengage themselves from conventional morality for other acts of deviance. If it is discovered that excuses are accepted allowing engagement in piracy, but not in other high-tech crimes (such as hacking or child pornography), additional credibility would be lent to the specific applicability of the theory to the illegal duplication of software files.

How long are neutralizing techniques necessary in the course of a pirate's criminal career? Perhaps they are used quite frequently at the commencement of infringing behavior, but decrease in incidence as the pirate becomes more and more entrenched in the delinquent activity. Thus, in time s/he would no longer need to resolve any dissonance stemming from the conflict between moral values and immoral behavior, and would continue the misdeed in accordance with a new deviant value system. Furthermore, at what point in a delinquent's career are these methods of rationalization most employed? More generally, what degree of influence do the techniques have in facilitating software piracy through the traditional borrowing and copying of programs on physical media, as compared to the illegal transfer of warez over the Internet?

Another question has to do with the degree of success the techniques of neutralization have in preventing the onset of feelings of guilt. Perhaps as time goes on, these rationalizations have become more acceptable in both the minds of the deviants and to society as a whole, while the line between upright behavior and criminal behavior is increasingly blurred. The validity of this supposition requires a longitudinal study to analyze the influence of the theory at the commencement, continuance, and resolution stages of piracy participation.

It was initially suggested that a panel study might be used in addition to the cross-sectional perspective of this research in order to more thoroughly test the applicability of the theory. However, I contend that for the purposes of the current work, it is not necessary. It would be difficult to survey the same set of people two or more times, considering this research is based on self-reported criminal activity - an inherently sensitive subject - and must remain anonymous due to this fact. The same set of students would also be problematic to keep track of, as many decide to leave a particular dorm room for another, or choose to move off campus into an apartment or house. The experimental mortality would most likely cripple the reliability of the findings. A panel study, though, would provide evaluation data if any particular policy solutions were implemented, on account of my findings or otherwise. Nevertheless, since neutralizations are specified by Sykes and Matza to occur *before* the act is committed, I feel that studies after policy implementation would necessitate an entirely new theoretical perspective. Additionally, there are a multitude of logistical difficulties concerning time, money, and other resources requisite to measure tendency to neutralize at one occasion or time period, and then to follow up with the same individuals months or even years later to determine their level of involvement in piracy at that time.

A few methodological issues arised during the research. For one, although anonymity and confidentiality were promised, we could not ensure the veracity of the feedback received, an inherent negative characteristic of self-report studies. Nonrespondent bias may have occurred in that those who did respond might have been less likely to expropriate software than those who did not respond (Seale, Polakowski, & Schneider, 1998).

The ad hoc questionnaire developed solely for this paper suffered from some methodological weaknesses. It is likely that these occurred simply due to inexperience with developing a survey instrument, and the mistakes have taught me valuable lessons which from which I will be able to benefit during future quantitative research procedures. For instance, the answer choices in a few questions did not include an "N/A" option for those who had not participated in software piracy. These items consequently had to be removed. The responses might have been more conducive to analysis if the scales always provided "0" as the first option, and then increased incrementally in the next answer choice (e.g., 1-?). This author twice made the mistake of grouping 0 with 1, 2, 3, 4, and 5 in questions intended to measure incidence and intensity of piracy, not realizing the drastic difference between those who had not pirated at all, and those who had pirated at least one time.

The survey itself had an inordinate amount of questions (131), as it was believed that each and every question was important to the study. Admittedly, if some of the prosocial questions had been removed, the number of items would have decreased by 15-20%. Nevertheless, without prosocial questions, the intrinsic purpose of the instrument to measure students' pirating activities would have been transparent to practically all respondents. A few professors and students in the classes surveyed did suggest reducing the amount of questions to preclude the possibility of individuals skipping or randomly answering items. Unfortunately, some inquiries (such as the respondent's discipline and age) were only presentable by extending the answer choices over a series of questions and providing "None of the above" as an option for each one, due to the limitations of the scantron forms utilized. For example, to determine the discipline under which a student's

major falls among twenty three choices, six questions had to be utilized to cover every single option (see Survey Instrument in Appendix A for further clarification).

A relatively serious problem stemmed from the use of scantron forms to collect response data. After performing listwise deletion of missing cases, a shocking 14.6% (73 responses) of the sample were removed. On some scantrons, individuals seemed to be missing questions randomly; that is, it was not a particular small set of respondents who were failing to answer all of the questions. The trend seemed to be distributed without any semblance of logic. Upon pondering the possible reasons for this unexpected occurrence, it was conjectured that some students did not properly bubble in the response for each question, perhaps marking beyond or outside of the circles, or not fully erasing a previous answer choice, or left stray marks on their scantron form. Their intended responses, then, likely were not recognized by a fastidious scantron scoring machine, leaving blank (e.g., missing) responses. It might have been prudent to go through each scantron manually and ensure that each answer choices entered in error were properly erased, and that all responses were properly bubbled inside the appropriate circle, and that no stray marks were left which might potentially confuse the scoring machine. In retrospect, it is somewhat amusing to think that a study about a consequence stemming from the advancement of technology would be tripped up due to the nuances associated with another technological development – the computerized scoring system.

A few final limitations stem from the study population chosen. For instance, it is possible that the moral value systems of university students are already established, decreasing the potential influence of the techniques of neutralization on behavior. Additionally, a logistic problem occurred as the race, age, and year of studies were all

highly skewed. A very small proportion of the sample was nonwhite, of freshman or sophomore standing, or less than 21 years of age. While the distorted distribution of race in my sample mirrors the overall student population at this university, age and year of studies might have been more varied had the research occurred during the fall or spring semester of a school year. It is conjectured that upperclassmen take summer classes to a greater degree than younger students, presumably to assist in graduating on time. Freshmen and sophomores generally seem to be unconcerned with degree and credit hour requirements at the early stages of their academic career, and are not likely to take summer classes unless they are eager to "get ahead". This unintended consequence made it impossible to compare the pirating behavior between age groups and cohorts. Moreover, the vast majority of the student population was wealthy (as inferred by the fact that their parents' income of $50,000 or more), and so it was difficult to determine if pirating behavior is differentiated by socioeconomic status. Academic major or discipline of study was another variable not as evenly distributed among respondents as I would have hoped, precluding the possibility of accurately comparing the infringing activity of one group to another. Fortunately, these logistic problems can be corrected quite easily in a future wave of study.

POLICY IMPLICATIONS

Through this extensive study and analysis, three of the four previously specified hypotheses were substantiated. The dominant finding was that piracy is a problem among college students, supporting descriptive research conducted on this topic. Moreover, it was found that high-speed Internet access, particularly Ethernet access in dorm room or residential hall settings, lends itself to this particular intellectual property theft. What can be done about this problem? We must now turn our attention to possible solutions that can be implemented to curb the incidence and frequency of the computer crime. When the boundaries of lawful behavior are clearly defined, it will presumably be more challenging for potential offenders to neutralize their deviant actions through the techniques previously mentioned. 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 creations and property among students is an intrinsically essential function of higher learning, particularly when it involves a networked environment where duplication and dissemination of works without the author or owner's permission can proliferate easily and with great celerity.

While Acceptable Use Policies (AUP) in university handbooks and codebooks are used frequently to accomplish this end, they are not enough, as many students do not take the time to read such lengthy administrative discourses. The Michigan State University AUP (1998) states:

5. Michigan State 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 scrupulously with, the license and copyright provisions of the software that they use.

5.1. 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 form of criminal activity, as proposed by the Vice Provost of Computing and Technology. Furthermore, the AUP goes on to specify that "Users are responsible for informing themselves of, and complying scrupulously with, the license and copyright provisions of the software that they use" (Michigan State University AUP, 1998). While this disclaimer 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, which is seemingly essential to refraining from piracy. Such codes must clearly delineate the unethical 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 provides a Recommended Internet Usage Policy that can be adapted as

necessary by universities to suit their interests (Recommended, 1999). Aside 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. The SIIA and the BSA provides interested organizations and individuals with a self-audit kit at either zero or minimal cost (SPAudit Software Management Tools, 1999; Software Piracy, 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 crime.

Monitoring is currently being performed to ensure the efficiency and peak functionality of the campus LAN by analyzing 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 determination of exactly what is being transferred (through a technique called "packet sniffing") is increasingly necessary to address the issue of illegal copyright infringement occurring over university communication lines. However, there are some issues that preclude the possibility of using this technique. At the routing level, where the local area network (i.e., 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, thus reducing the amount of throughput requiring monitoring. This, unfortunately, might unintentionally restrict legitimate users in their computing and networking abilities. Further, determining the content of the data transversing over the network pipelines is much more difficult.

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 transfer of data, increasing 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 servers and workstations online and maintaining network connectivity throughout campus. Finally, most transfers of program files occur in binary format, rather than ASCII 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, and many would argue that this is a fundamental breach of students' civil and privacy rights.

Perhaps a proviso in text can be called up on the computer screens of students the first time they register to use the dedicated Ethernet access in their residential halls, delineating the honorable behavior required while using the school's resources and access to the Internet, and reminding users of the negative implications that will result from illegal behavior. A small automatically executable file can even be written and installed on every user's computer displaying a similar warning message upon logon concerning proper computer usage. Periodic mass emails sent to the student body may help to remind individuals that unethical actions online will not be tolerated. Another idea would

be to require the signature of all potential users of the university network and bandwidth, perhaps incorporated into the university application for enrollment form, to officially indicate an agreement to abide by virtuous computing standards. These strategies should reduce, to some degree, the erosion of accountability for unethical computing practices. The SIIA provides a sample policy statement for organizations to use, and recommends that all users (faculty, staff, students) read and sign such a document to indicate agreement to abide by the rules (Sample Corporate Policy Statement, 1999).

Another possible solution results from the existence of a caching server, which exists in each dorm room and resides on a network between a student's computer and web and ftp browsing software and the Internet web and file servers from which documents and information are being retrieved. It 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 request is made by a client computer. Rather than going out onto the Internet 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 origin server. When a student turns on his computer, 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. It is suggested that 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 the user 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 high-speed 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 dorm room residents. Perhaps the popup reminder's absence has fostered piracy among students to a greater degree than would have occurred had it been utilized.

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 MSU Acceptable Use Policy, the Business Software Alliance, or the Software and Information Industry 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.

One suggestion initially contemplated was to install secondary phone lines in each of the dorm rooms and increase the number of ports that the campus dial-in server can hold in order to allow for more users to be connected through an analog, low-speed (maximum threshold of 56 kbps) line. This would shrink ideal and maximum bandwidth usage from 10 mbps to 56 kbps (although current FCC regulations limit download speeds to 53kbps), and thereby discourage users from software piracy by requiring them to spend

hours and hours online to download files, since the speed of transfer is exponentially lower. Admittedly, this idea is quite drastic and might not even be considered if the piracy rate among students was extraordinarily high.

Upon further inquiry, the prospective solution was downed for a host of financial and logistic reasons. The cost of each outlet on the average in a hall is about $500 to install. Additionally, there is an annual cost of about $10 per outlet to maintain the network and the electronics. The current system functions at 10 mbps but has the capability to be extended to 100 mbps and 600 mbps and possibly higher as technological needs and the added value of service warrant it. To add a second phone line, one must essentially rewire the hall phone system and add a replacement line and a second line. Notably, the cost to do this is not any cheaper than the cost to do the cabling necessary for Ethernet. However, upon activation of the second phone line, the service costs for each of these additional phone lines is $17.50 per month to the national provider, Ameritech. That is a cost of $200 per year per dorm room, and the necessity to install additional phone lines at the dial-in end will cost approximately the same. The present Ethernet installation is considered to be good for a minimum of 10 years. The electronics will be changed after about 5 years at the cost of approximately $100 per outlet. Ethernet cost over 10 years will be roughly $700 per line while the telephone costs will be closer to $2500 per line plus the cost of additional dial-in lines. In sum, the idea of secondary phone lines for dial-in Ethernet access, albeit idealistic and well intentioned, was found to be unworkable.

The illegal expropriation of software was found to be a significant problem for the sample as a whole, not exclusive only to those with high-speed Internet access. Some

discussion of policy implications to deal with copyright infringement by the entire student body is merited. One such potentially beneficial solution might involve relational interaction between universities and the IT industry, particular 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 then discuss the germane copyright laws and infringements that accompany unethical computer usage and conceivably aid in deterring denial of responsibility, denial of negative intent, and claim of relative acceptability. Furthermore, the speakers could champion their cause by describing the damage that is done to the IT industry, developers and programmers (both by removing financial incentive and through the stifling of innovation and creativity), and ultimately the consumer population, plausibly countering denial of injury. 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.

As previously explained, neutralization is used to curtail the emergence of dissonance developing from committing the proscribed act. However, to preclude the onset of these techniques, 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 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 moral and immoral 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 engender a deeper awareness of the seriousness of the issue at hand and facilitate cognitive restructuring. 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.

Solomon and O'Brien (1990) found that nearly half of the students they surveyed had never heard a faculty member or administrator speak out against software piracy, and that 25% had heard university personnel condone the unauthorized duplication of a program. While the generalizability of these findings is as yet unproven, it can be inferred that faculty members do influence, consciously or unconsciously, the ethical practices of their students to some degree. Perhaps it is necessary to require instructors and professors in all courses where the use of a computer is expected to include in their syllabus a warning against the use of illegal software, as many have found it necessary to provide a similar admonition against plagiarism. At the very least, professors of certain majors in which the use of computing resources is extremely high (engineering, computer science, graphics design, journalism) should emphasize the importance of complying with the school's directives in this area. It is hoped that these admonitions will forestall any neutralizing techniques.

With regard to class assignments and student projects, perhaps faculty members should ask students to attach evidence of the purchase of original software if the students use software which are not supplied by the university. Faculty should caution students that they may turn down a student's assignment or project if they are developed using pirated software. A possibility might be to require students to attach evidence of the official purchase of software when turning in class papers or projects if that software is not freely accessible in student computer labs or at the library. This, unfortunately, would usher in a host of inconveniences and problems, as many individuals likely have misplaced or discarded proof of purchases and receipts. Additionally, as more software is available for download through online retail stores and distributors after the provision of one's credit card number, there may be no tangible indication of purchase aside from a receipt in the form of a web page, which many will forget to save to their hard drive or print out a hard copy. Most notably, however, will be the added burden on both faculty and students to coordinate the process and ensure that everyone has a legitimate copy of the necessary application(s).

What punitive measures can be instituted to discipline transgressors and dissuade others from following in those footsteps? As mentioned earlier, perhaps those who transgress codes of ethics in a university setting should be denied access to future use of the Internet for a specified period of time. Although this would be hard to monitor and enforce, the presence of such a sanction might deter potential offenders. Restricting bandwidth at certain times of the day also seems feasible. At first glance it might make sense to cap transfer speeds at night, either in the aggregate (for all students as a whole) or for each network port or dorm room connection. While this time of day is when most

users are on their computers for purposes other than work (e.g. downloading software or music), it will not aid the problem of excessive bandwidth consumption and subsequent traffic bottlenecks during the day, when most individuals are working or needing the network resources for lawful occupational or educational purposes. Further, while it might reduce the frequency of software pirated overnight, it likely will not decrease the incidence of illegal file transfers. Additionally, by implementing restrictions on the amount of data an individual can transfer, legitimate users are unnecessarily penalized and precluded from using the network connection for appropriate purposes. These range from obtaining a new freeware operating system build or a software service pack or patch to fix operational problems, to backing up their data on a remote site in the event of a local hard drive failure, to sending an engineering professor a host of large computer-assisted drafting (CAD) files for inclusion in a research project.

As mentioned earlier, software manufacturers are increasingly implementing server-side verification designs to reduce the piracy 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 appropriated only to the user who purchased the product. If an individual attempts to utilize a key previously designated to another user, the program will shut down and not function until a valid license is purchased. That key will then become "blacklisted", and subsequent pirates 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 always be online and able to contact a remote database to verify a serial number or keycode before granting access to utilize the program. This can be countered, of course, by unplugging one's Internet connection before executing a program – something very few individuals will deem reasonable and worthy of the extra effort. 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.

To further explore countermeasures that might be implemented, and to obtain a comprehensive understanding of unethical computing behavior that occurs on campus, an interview with Dr. Robert Wittick (personal correspondence, March 27, 2000) was conducted. Dr. Wittick is the Director of Central Services at Michigan State University and handles all disciplinary actions resulting from breaches of the Acceptable Use Policy by students. Some of the unethical behaviors that have been brought to his attention include chain letters, pyramid schemes, the posting of copyright material (particularly unauthorized full-length music files), port scanning to exploit vulnerabilities in other computer systems and subsequently commandeer through the use of trojan horse programs, mail bombs, spamming, and other related attacks. Most such unauthorized computing activity occurs in dorm rooms rather than in computer labs, conceivably because when a student logs onto a lab system, s/he must provide a user ID to obtain access. This has the effect of reminding the individual that his or her actions are recursively traceable. In a residence hall, the student's ID is automatically authenticated when the operating system loads up, and an Internet Protocol address is allocated,

enabling readily accessible and instant Internet access. Because of this seamless, transparent background-processed verification of a user's ID, students may forget that the port being used has been assigned specifically to them and that therefore all online actions made using that port are traceable.

When a complaint has been received, the network manager is contacted to check the logs of date, time, and IP address to verify that the questionable activity was performed by the suspected individual (or, by someone using that account). The student is then contacted by US Postal mail as well as by email and asked to come in for a meeting. If it is determined that the student is blatantly at fault, any number of measures can be taken based on the seriousness of the act, such as disabling the individual computer account, bringing the student up before a Judicial Board for disciplinary action, or contacting the police. Disabling a student's computer account is by no means a benign sanction; many critical academic functions such as email, registration for classes, the distribution of coursework, the use of expensive software licensed by the university, and the conducting of much research all require access to a computer, a privilege available only to those with a valid username and password.

With regard strictly to software piracy, Wittick asserts that in the six years of tenure in his current position, there has not been a single case of software piracy brought to his attention. In addition, no bandwidth monitoring is performed at this particular university with the intention of ascertaining the identity of those transferring large volumes of files. No packet sniffing is performed to determine the content of files being transferred, as the university is particularly adamant about abiding by the Academic Freedom for Students doctrines in place, and respecting unconditionally the student's

privacy and personal rights. Finally, no personal information about a student will be released if, for instance, a software manufacturer which remotely verifies license keys contacts the university after detecting that a student attempted to use an illegal serial number to register an application. Even the police, unless serving a subpoena or another legal document, cannot demand information about the identity of a student. These dictums exist to promote the advancement, dissemination, and application of knowledge through the freedom of expression and communication, and consequently are in place to maintain and further a scholarly environment conducive to learning (Student Rights, 1999). While some of these policies might not be plausible at smaller universities and colleges, noteworthy potentialities can be extrapolated, modified, and put to use based on these practices, such as informally interrogating those students consuming inordinate amounts of bandwidth and putting a strain on the network as a whole.

In order to determine the efficacy of codes, ethical training, warning signs, disclaimers, and entreatments to students from faculty and software manufacturers in reducing the frequency of software piracy through increased awareness and sensitivity, longitudinal studies must be performed following such policy implementation. As always, replication with samples from other universities of varying student and regional demographics are required to further validate the appropriateness of applying neutralization theory to software piracy, and to increase external validity.

CONCLUSION

Prior to the current work, the majority of research in the software piracy arena has been rather descriptive, and has been used only in identifying the existence and purview of the problem. The present study is markedly different and has sought to determine behavioral, sociological, economic, and environmental factors that facilitate the prevalence of piracy. The instrument served to extrapolate the applicability of neutralization theory as well as to infer policy solutions that might curb the problem. Further, the incidence and frequency of pirating behavior online was found to be positively correlated with high-speed Internet access. Support was found for Sykes and Matza's neutralization theory as a mechanism that students employ to achieve a break with any normative constraints, freeing them to commit the act after redefining the behavior in a positive, acceptable light. Contrary to the third hypothesis, the influence of neutralization's separate components could not be accurately fleshed out; therefore, no particular tenet was found to be a stronger predictor than another. Finally, support was discovered for the fourth conjecture that experience with illegal duplication of software through the use of CD burners lends itself to an increased participation in copyright infringement over the Internet

Advancements in information technology, allowing for improvements in the speed of communications, the accessibility of information and data files, and the increase in overall computing power to run processes previously unfeasible, have opened the door to a multitude of new behaviors. The file-sharing capabilities of the Internet, concomitant with high-speed access provided to students in residential hall settings, have greatly increased the prevalence of the unauthorized distribution and downloading of copyrighted

programs from various web and archive sites. Unfortunately, the distinction between right and wrong among these behaviors is sometimes unclear and susceptible to varying interpretations. The deficiency of such a demarcation line, the failure of universities to step up and address this issue through the specific and conspicuous delineation of appropriate and inappropriate computing behavior, and the failure to cultivate cognitive restructuring among those particularly prone to engage in online deviance has in some respects fostered and perpetuated the problem of software piracy.

Matrix Information and Directory Services (http://www.mids.org) estimates that the total number of worldwide Internet users will grow to 707 million by 2001. As we move into a global economy, information will be the main source of power among people. Most of these individuals will use the Internet for legitimate purposes, but a good proportion will exploit its vulnerabilities and weaknesses, and violate the rights of others through software piracy and other forms of criminal activity. The role computers and the Internet play in our lives will continue to increase in scope and intensity, and the development of policy to combat deviance resulting from technological progress, such as software piracy, warrants immediate attention and additional inquiry by academics. The convergence of communications, computing, and crime has already reaped sizeable deleterious consequences for business and industry, and a subsequent decrease (or even a plateau) of this malfeasance does not seem imminent. Therefore, software manufacturers and developers will continue to be exploited and cheated out of revenue rightfully theirs while online bandits plunder substantial but undeserved benefits. As a result, companies will be forced to pass on the costs associated with the crime to legitimate consumers in the form of higher prices for their products. Employee layoffs, cutbacks, and the

production of less stable and shoddier programs will also inevitably occur as businesses attempt to stay afloat in an enormously competitive market. The only winners in this situation will be the lawbreaking Internet rogues, while the victimization of law-abiding corporations and citizens will continue with reckless abandon. However, an effort towards addressing this critical issue can be made with the implementation and sustaining of prescribed policy measures, as well as with further inquiry into novel forms of deviance spawned by technological advances such as the Internet.

APPENDICES

APPENDIX A

APPENDIX A

Internet Use Questionnaire

Thank you for taking the time to fill out the following questionnaire. Its purpose is to obtain an understanding of college students' perceptions of, and attitudes toward, their use of the Internet. Your input is valuable to us and will aid in:

1. assessing the extent to which the Internet has become an integral part of students' lives.
2. examining your ideas of acceptable and unacceptable conduct on the Internet.

Please select an answer for each of the following questions based on your personal circumstances/knowledge. Also, don't spend too long on any one statement; just input your initial reaction on the scantron form provided.

This survey is completely voluntary and anonymous. You are free to not answer any question. Do not write your name or any other identifying information on the questionnaire or scantron.

I would sincerely appreciate your honest answers in order to obtain a reliable measure. You indicate your voluntary agreement to participate by beginning this questionnaire.

Thank you in advance for your response. Should you have any questions or concerns, please feel free to call (517) 355-2197 or email Sameer Hinduja at hindujas@msu.edu.

FOR EACH OF THE FOLLOWING QUESTIONS, PLEASE RESPOND AS FOLLOWS: A = STRONGLY AGREE, B = AGREE, C = UNDECIDED, D = DISAGREE, E = STRONGLY DISAGREE

1. The Internet is indispensable to me.

2. I use the Internet to meet my social needs.

3. I am concerned about security, privacy, and confidentiality on the Internet (e.g., people reading my email, finding out what websites I visit, collecting information about me through my web surfing practices, criminals intercepting my credit card number when I make online purchases, etc.)

4. I am concerned about copyright infringement on the Internet

5. Censorship on the Internet is necessary in some cases.

6. The anonymous nature of the Internet is something I value.

7. Information, graphics, and files posted to the Internet can and should be used for personal purposes by whoever is able to access them.

8. Individuals should be able to assume different identities, personas, and roles while using the Internet if they so choose.

For the following questions, please answer A for TRUE and B for FALSE

9. I have Ethernet, cable modem, or DSL connectivity to the Internet in my dorm room, apartment, or house, allowing me to use the Internet at relatively high speeds without tying up a telephone line.

10. I use Ethernet, cable modem, or DSL connectivity in my dorm room, apartment, or house.

11. I connect to the Internet using a telephone line and regular computer modem.

12. As each year goes by, I spend more and more time on the Internet.

13. I find it easier to communicate with others in a "virtual" online setting than in real life.

14. In the following list, please count up the number of items that you use the Internet for, and answer accordingly.

- 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

A. 0-2 items
B. 3-5 items
C. 6-8 items
D. 9-11 items
E. 12-13 items

15. In the following list, please count up the number of items that you have done, and answer accordingly.

- 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

A. 0-2 items
B. 3-4 items
C. 5-6 items
D. 7-8 items
E. 9-10 items

For each of the following questions, please select from the answer choices provided.

16. On average, how many hours per week do you spend on the Internet, not including email?

A. Less than 5 hours
B. 5-10 hours
C. 11-15 hours
D. 16-20 hours
E. 21 or more hours

17. On average, how many hours per week do you spend on the Internet, including email?

A. Less than 5 hours
B. 5-10 hours
C. 11-15 hours
D. 16-20 hours
E. 20 or more hours

18. How long have you been using computers?
    A. Less than 1 year
    B. 1-2 years
    C. 3-4 years
    D. 5-6 years
    E. 7 or more years

19. How long have you been using the Internet?
    A. Less than one year
    B. 1-2 years
    C. 3-4 years
    D. 5-6 years
    E. 7 or more years

20. For which file transferring purposes do you use the Internet? (In the following list, please count up the items that you have done, and answer accordingly.)

- Uploading or downloading documents, text, and web pages
- Uploading or downloading graphics, pictures, .wav files, midi files, .au files, screensavers
- Uploading or downloading music mp3s
- Uploading or downloading shareware or freeware applications/games
- Uploading or downloading commercial full-version programs (applications/games)

A. One of the above
B. Two of the above
C. Three of the above
D. Four of the above
E. All of the above

21. How many hours/day do you spend on the Internet chatting or messaging with other Internet users (Internet Relay Chat (IRC), Personal Online Messaging Programs (ICQ, Microsoft NetMeeting, AOL Instant Messenger, etc.)?
    A. Less than one hour
    B. 1-2 hours
    C. 3-4 hours
    D. 5-6 hours
    E. 7 or more hours

22. How many hours/day do you spend on the World Wide Web or USENET?
    A. Less than one hour
    B. 1-2 hours
    C. 3-4 hours
    D. 5-6 hours
    E. 7 or more hours

23. How many hours/day do you spend on the Internet transferring files?
    A. Less than one hour
    B. 1-2 hours
    C. 3-4 hours
    D. 5-6 hours
    E. 7 or more hours

24. The frequency of transferring commercial full-version applications/games (not shareware or demo software) that exists on the Internet is (from YOUR experience):
    A. Extremely prevalent
    B. Prevalent
    C. Occasionally prevalent
    D. Very rare
    E. Unheard of

25. How frequently do you upload/download commercial full-version software programs to/from others (on average)?
    A. N/A
    B. 1-5 times a week
    C. 6-15 times a week
    D. 16-30 times a week
    E. 31 or more times a week

For the following questions, please answer A for TRUE and B for FALSE.

26. I know what warez is.

27. I know what an .nfo file is.

28. I know what 0-day means.

29. I know how to obtain commercial full-version applications/games.

30. I have bought/received/borrowed a copy of at least one software package(s) burned onto a CD-R (custom-made CD).

31. I have burned/recorded at least one software package(s) onto CD-R (custom-made CD).

32. I have uploaded/downloaded at least one commercial full-version software program to/from someone.

33. I have accessed commercial full-version software through my web browser.

34. I have uploaded/downloaded commercial full-version software to/from the USENET newsgroups.

35. I have uploaded/downloaded commercial full-version software through IRC or an Instant Messaging Program.

36. I have transferred or received commercial full-version software through an Instant Messaging program (ICQ, AOL IM, NetMeeting, PAL).

37. I have logged into an FTP server in order to upload/download commercial full-version software.

38. I have set up an FTP server on my computer system in order to allow others to log in and upload/download commercial full-version software to/from me.

For the following questions, please choose one of the responses provided.

39. When was the first time you transferred commercial full-version software on the Internet?

A. less than 6 months ago
B. 6 months ago
C. 1 year ago
D. 2-4 years ago
E. 5 or more years ago

40. When was the last time you transferred commercial full-version software on the Internet?

A. Last year
B. Last month
C. Last week
D. Yesterday
E. Today

41. How often in the last month have you transferred commercial full-version software on the Internet?

A. 0-5 times
B. 6-15 times
C. 16-25 times
D. 26-35 times
E. 36 or more times

42. How often in the last year have you transferred commercial full-version software on the Internet?

A. 0-5 times
B. 6-15 times
C. 16-25 times
D. 26-35 times
E. 36 or more times

FOR EACH OF THE FOLLOWING QUESTIONS, PLEASE RESPOND AS FOLLOWS: A = STRONGLY AGREE, B = AGREE, C = UNDECIDED, D = DISAGREE, E = STRONGLY DISAGREE

43. Generally speaking, I would feel guilty for downloading/uploading commercial full-version software?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

44. if I could not afford the purchase price of the product?

45. if I have too many other expenses as a college student?

46. because school and life in general is hard enough as it is?

47. since numerous sites offering commercial full-version software for free download are readily available?

48. if I heard or read news reports stating that software companies drastically overcharge and rip off the consumer for their products?

49. since there are no clear-cut rules, laws, regulations, or even instruction on proper computing usage, and therefore it might not even be illegal?

50. if all my friends and classmates were doing it?

51. because businesses do it, and similar questionable activities, a good proportion of the time?

52. because no one else seems to have the time or the desire to help me out, so I am forced to help myself out any way I can?

53. because life is unfair, and everyone is corrupt and in a rat race to get ahead, regardless of who gets hurt.

54. because people do what they need to do to get to the top, and if I don't take advantage of a situation, someone else will, to my detriment?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

55. if it were known that the software company "could afford it" and would never miss the tiny amount of proceeds lost from just one copy?

56. if it were held that "theft" isn't really taking place because all parties involved still have the same software and no one is being denied use of it, as only a copy of the program is being borrowed for use?

57. if it were known that software companies work into their annual budget an amount allocated solely to cover the costs of "shrinkage", or loss of capital because of theft, and therefore are already accounting for and expecting some loss through Internet distribution?

58. if it were held that by conquering security protection schemes of programs, I am actually exposing flaws and encouraging companies to fix them, and are thereby doing them a favor?

59. if it were known that law enforcement agencies, universities, and authorities in general couldn't care less about the activity, lack adequate abilities to detect or combat the activity, and have bigger things to worry about?

60. if it were known that through sales to corporations and individuals, software companies more than make up for losses incurred through downloading and uploading on the Internet by individuals?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

61. if it were held that software companies, to some extent, deserve to have their commercial full-version software distributed freely considering the fact that they rip off consumers?

62. if it were held that no one is really getting hurt from Internet distribution?

63. if it were held that software companies are an unsuspecting, remote, and oblivious entity, and are clueless of a little distribution of their commercial full-version products over the Internet?

64. since it is difficult to believe that anyone really cares if a piece of software is copied over the Internet?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

65. because software companies, and a good proportion of corporations and wealthy people for that matter, succeed and get rich through unethical practices anyway, and Internet distribution serves to counteract that?

66. if it were held that any practices or conventions that restrict the free flow of information and programs stifle progress and technological development, and should be done away with in the best interests of society?

67. because a good proportion of laws are unfair and unjust in and of themselves?

68. because hardly anyone has been caught or punished or has been subject to even the slightest repercussions for Internet distribution?

69. since I've been victimized before and unfairly taken advantage of in the past by others, it's therefore alright to try to compensate or make up for that through Internet distribution?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

70. if I needed the software and wouldn't be able to obtain or use it any other way?

71. if a family member, friend, or significant other needed it?

72. if a family member, friend, or significant other pressured me to get it?

73. if it will be used to complete a project for school or work, or to achieve other school-related and career-related goals?

74. if it will be used to benefit an individual or a business somehow?

75. if I had little other choice?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

76. if it were held that Internet distribution is harmless and relatively innocent and minor compared to all of the harm that occurs in the world?

77. since it is okay if I do something questionable every now and then - it is better than a frequently dishonest person engaging in misdeeds over and over again?

78. because it isn't so bad to do something for myself occasionally, especially if I really need it, considering all the good things I do for others?

79. because I deserve something for free sometimes?

80. because in "the grand scheme of things", it really does not matter?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

81. if it were prevalent all over the Internet, and if a lot of people were doing it?

82. if it were held that no one else seems to care whether or not they get caught?

83. if it were held that other people are benefiting from it, and so why shouldn't I?

84. if having access to free software makes me feel at least a little more "cool", or to some degree increases my perception of self-worth?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

85. because there aren't really any steadfast rules or objective values about behavior in a virtual setting such as the Internet?

86. if it were held that I am not really doing anything wrong?

87. because I need to try it out before I go out and spend money to purchase it, since I can't afford to waste money on an inferior product?

88. because without the ability to evaluate the product, I will not be able to determine if it meets my needs?

89. because I wouldn't or couldn't purchase the product anyway, and therefore the software company is not really being denied of any potential profits?

90. because by using the product, I might be able to recommend it for purchase to family, friends, and acquaintances?

91. because I plan to use it for educational purposes, or to learn from it?

I WOULD BE MORE LIKELY TO DOWNLOAD/UPLOAD COMMERCIAL FULL-VERSION SOFTWARE:

92. because the anonymous nature of the Internet affords privacy and somewhat of a shield from detection; and so, why not take advantage?

93. because no one really cares about what I do online - it is just too removed from the "real world"?

94. because it is better, or at least more acceptable, to be engaging in this activity on a computer than going out and tangibly harming people?

For the following questions, please answer A for TRUE and B for FALSE and C for NOT APPLICABLE.

95. The majority of my file transferring takes place at night (11pm to 7am).

96. I leave my computer on for extended periods of time (e.g., overnight) to transfer files.

97. I am a member of an online group that trades/distributes commercial full-version software

98. I have a personal account on one or more FTP sites

99. I can find almost any piece of commercial software I might need on the Internet, either through friends or searching/browsing through file archives

100. The majority (50%+) of software on my computer is legitimately licensed.

101. At least one program/game on my computer is not legitimately licensed.

102. Before my high-speed access, I used to upload/download commercial full-version software.

103. Without my high-speed access, and with only a telephone/modem connection, I would still upload/download commercial full-version software at times.

104. Without my high-speed access, and with only a telephone/modem connection, I would still download commercial full-version software at the same rate I am currently doing so.

105. I have transferred commercial full-version software on the Internet since I started college while living in my dorm room or on campus apartment.

106. I have transferred commercial full-version software on the Internet prior to starting college and prior to living in my dorm room or on campus apartment.

107. High-speed access in my dorm room, apartment, or house makes it easier (or would make it easier if I had high-speed access) to upload/download commercial full-version software from the Internet than a standard telephone/modem connection would.

108. I upload/download files using my Network Neighborhood (over the university's local area network) to and from individuals on campus MORE than I transfer files to and from individuals who are off campus (over the external Internet, outside of the local area network).

109. I have recently stopped transferring commercial full-version software.

110. I feel that the distribution of commercial full-version software is wrong.

111. I don't think I will ever be disciplined or get into trouble for transferring commercial full-version software files.

112. 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.

113. I have at least one time felt so guilty that I went and purchased the software that I had downloaded.

For each of the following questions, please select from the answer choices provided.

114. Race:
   A. Caucasian/White
   B. African American
   C. Asian/Pacific Islander
   D. Hispanic
   E. Other

115. Sex:
   A. Female
   B. Male

116. Age:
   A. 16 or younger
   B. 17
   C. 18
   D. 19
   E. None of the above

117. Age:
   A. 20
   B. 21
   C. 22
   D. 23 or older
   E. None of the above

118. Year of Studies:
   A. Freshman
   B. Sophomore
   C. Junior
   D. Senior
   E. Graduate Student

119. My major is housed in the college of:
   A. Agricultural and Natural Resources
   B. Arts & Letters
   C. Eli Broad College of Business
   D. Communication Arts and Sciences
   E. None of the above

120. My major is housed in the college of:
   A. The Detroit College of Law
   B. Education
   C. Engineering
   D. Honors College
   E. None of the above

121. My major is housed in the college of:
   A. Human Ecology
   B. Human Medicine
   C. International Studies & Programs
   D. James Madison College
   E. None of the above

122. My major is housed in the college of:
   A. Nat Super Cyclotron Lab
   B. Natural Science
   C. Nursing
   D. Osteopathic Medicine
   E. None of the above

123. My major is housed in the college of:
   A. Social Science
   B. Urban Affairs Programs
   C. Veterinary Medicine
   D. None of the above

124. My major is housed in the College of Engineering, and is:
   A. Engineering (Agricultural, Chemical, Civil, Environmental, Electrical, Mechanical, Engineering Arts, etc)
   B. Computer Science
   C. Computer Engineering
   D. Materials Science
   E. My major is not housed in the College of Engineering

125. My major is not housed in the College of Engineering, but I have obtained my experience with computers from:
   A. Previous employment
   B. Training programs
   C. School courses
   D. A family member, relative, or close friend who works with computers
   E. My major is housed in the College of Engineering

126. What is the highest degree of education your father has completed?
   A. High School or equivalent
   B. Vocational/Technical School (2 year)
   C. Some College
   D. College Graduate (4 year)
   E. Graduate/Professional Degree

127. What is the highest degree of education your mother has completed?
   A. High School or equivalent
   B. Vocational/Technical School (2 year)
   C. Some College
   D. College Graduate (4 year)
   E. Graduate/Professional Degree

128. What is your parents' annual household income?
   A. $0 to $19,999
   B. $20,000 to $29,999
   C. $30,000 to $39,999
   D. $40,000 to $49,999
   E. $50,000 or more

129. Your employment (job) status:
   A. I do not have a job
   B. I work approximately 10 hours a week
   C. I work approximately 20 hours a week
   D. I work approximately 30 hours a week
   E. I work approximately 40 hours a week

130. At my job, my use of a computer is:
   A. Minimal
   B. Moderate
   C. Heavy
   D. I do not use a computer at my job
   E. I do not have a job

131. I live in an:
   A. On-Campus Residence Hall (dorm room)
   B. On-Campus Apartment
   C. Off-Campus Apartment or House
   D. Other

APPENDIX B

Table A. Denial Of Responsibility $\alpha = .9035$

Variables	Factor Loading
V44 if I could not afford the purchase price of the product?	.687
V45 if I have too many other expenses as a college student?	.703
V46 because school and life in general is hard enough as it is?	.765
V47 since numerous sites offering commercial full-version software for free download are readily available?	.636
V48 if I heard or read news reports stating that software companies drastically overcharge and rip off the consumer for their products?	.705
V49 since there are no clear-cut rules, laws, regulations, or even instruction on proper computing usage, and therefore it might not even be illegal?	.689
V50 if all my friends and classmates were doing it?	.713
V51 because businesses do it, and similar questionable activities, a good proportion of the time?	.781
V52 because no one else seems to have the time or the desire to help me out, so I am forced to help myself out any way I can?	.725
V53 because life is unfair, and everyone is corrupt and in a rat race to get ahead, regardless of who gets hurt.	.708
V54 because people do what they need to do to get to the top, and if I don't take advantage of a situation, someone else will, to my detriment?	.733

Table B. Denial Of Injury $\alpha = .9147$

Variables	Factor Loading
V55 if it were known that the software company "could afford it" and would never miss the tiny amount of proceeds lost from just one copy?	.827
V56 if it were held that "theft" isn't really taking place because all parties involved still have the same software and no one is being denied use of it, as only a copy of the program is being borrowed for use?	.839
V57 if it were known that software companies work into their annual budget an amount allocated solely to cover the costs of "shrinkage"?	.852
V58 if it were held that by conquering security protection schemes of programs, I am actually exposing flaws and encouraging companies to fix them, and are thereby doing them a favor?	.798
V59 if it were known that law enforcement agencies, universities, and authorities in general couldn't care less about the activity, lack adequate abilities to detect or combat the activity, and have bigger things to worry about?	.842
V60 if it were known that through sales to corporations and individuals, software companies more than make up for losses incurred through downloading and uploading on the Internet by individuals?	.868

Table C. Denial Of Victim $\alpha = .8519$

Variables	Factor Loading
V61 if it were held that software companies, to some extent, deserve to have their commercial full-version software distributed freely considering the fact that they rip off consumers?	.821
V62 if it were held that no one is really getting hurt from Internet distribution?	.831
V63 if it were held that software companies are an unsuspecting, remote, and oblivious entity, and are clueless of a little distribution of their commercial full-version products over the Internet?	.833
V64 since it is difficult to believe that anyone really cares if a piece of software is copied over the Internet?	.844

Table D. Condemnation of the Condemners $\alpha = .8663$

Variables	Factor Loading
V65 because software companies, and a good proportion of corporations and wealthy people for that matter, succeed and get rich through unethical practices anyway, and Internet distribution serves to counteract that?	.822
V66 if it were held that any practices or conventions that restrict the free flow of information and programs stifle progress and technological development, and should be done away with in the best interests of society?	.783
V67 because a good proportion of laws are unfair and unjust in and of themselves?	.872
V68 because hardly anyone has been caught or punished or has been subject to even the slightest repercussions for Internet distribution?	.764
V69 since I've been victimized before and unfairly taken advantage of in the past by others, it's therefore alright to try to compensate or make up for that through Internet distribution?	.794

Table E. Appeal to Higher Loyalties $\alpha = .8924$

Variables	Factor Loading
V70 if I needed the software and wouldn't be able to obtain or use it any other way?	.851
V71 if a family member, friend, or significant other needed it?	.880
V72 if a family member, friend, or significant other pressured me to get it?	.642
V73 if it will be used to complete a project for school or work, or to achieve other school-related and career-related goals?	.864
V74 if it will be used to benefit an individual or a business somehow?	.823
V75 if I had little other choice?	.787

Table F. Metaphor of the Ledger $\alpha = .8851$

Variables	Factor Loading
V76 if it were held that Internet distribution is harmless and relatively innocent and minor compared to all of the harm that occurs in the world?	.770
V77 since it is okay if I do something questionable every now and then - it is better than a frequently dishonest person engaging in misdeeds over and over again?	.864
V78 because it isn't so bad to do something for myself occasionally, especially if I really need it, considering all the good things I do for others?	.871
V79 because I deserve something for free sometimes?	.868
V80 because in "the grand scheme of things", it really does not matter?	.769

Table G. Claim of Normalcy $\alpha = .8265$

Variables	Factor Loading
V81 if it were prevalent all over the Internet, and if a lot of people were doing it?	.847
V82 if it were held that no one else seems to care whether or not they get caught?	.876
V83 if it were held that other people are benefiting from it, and so why shouldn't I?	.855
V84 if having access to free software makes me feel at least a little more "cool", or to some degree increases my perception of self-worth?	.663

Table H. Denial of Negative Intent $\alpha = .8954$

Variables	Factor Loading
V85 because there aren't really any steadfast rules or objective values about behavior in a virtual setting such as the Internet?	.691
V86 if it were held that I am not really doing anything wrong?	.720
V87 because I need to try it out before I go out and spend money to purchase it, since I can't afford to waste money on an inferior product?	.831
V88 because without the ability to evaluate the product, I will not be able to determine if it meets my needs?	.838
V89 because I wouldn't or couldn't purchase the product anyway, and therefore the software company is not really being denied of any potential profits?	.790
V90 because by using the product, I might be able to recommend it for purchase to family, friends, and acquaintances?	.822
V91 because I plan to use it for educational purposes, or to learn from it?	.788

Table I. Claim of Relative Acceptability $\alpha = .8210$

Variables	Factor Loading
V92 because the anonymous nature of the Internet affords privacy and somewhat of a shield from detection; and so, why not take advantage?	.869
V93 because no one really cares about what I do online - it is just too removed from the "real world"?	.879
V94 because it is better, or at least more acceptable, to be engaging in this activity on a computer than going out and tangibly harming people?	.827

APPENDIX C

APPENDIX C: CLASSES SURVEYED

Course Number	Course Name
MSC 300	Managerial Marketing
MSC 300	Managerial Marketing
ENG 310	Literature in English to 1660
MSC 310	International and Comparative Dimensions of Business
MSC 310	International and Comparative Dimensions of Business
ADV 205	Principles of Advertising
ECE 345	Electronic Instrumentation and Systems
ECE 345	Electronic Instrumentation and Systems
ANT 316	General Human Anatomy
MTH 103	College Algebra
CJ 421	Minorities, Crime, and Social Policy
CJ 110	Introduction to Criminal Justice
CJ 220	Criminology
CJ 335	Police Process
PLS 200	Introduction to Political Science
PLS 324	American Legislative Process
ANP 202	Biocultural Evolution
ANP 452	North American Prehistory
PSY 295	Data Analysis in Psychological Research
SOC 131	Social Problems
SOC 322	Sociology of Work
PHL 130	Logic and Reasoning
ACC 411	Auditing
COM 240	Introduction to Organizational Communication
BCH 401	Basic Biochemistry
PSY 304	Psychological Measurement
EC 330	Money, Banking, and Financial Markets
MSC 401	Procurement & Supply Management
PSY 200	Cognitive Psychology

REFERENCES

REFERENCES

Agnew, R. (1994). The techniques of neutralization and violence. Criminology, 32 (4), 555-580.

Agnew, R. & Peters, A. A. R. (1986, March). The techniques of neutralization: An analysis of predisposing and situational factors. Criminal Justice and Behavior, 13 (1), 81-97.

Austin, R. L. (1977). Commitment, neutralization, and delinquence. Pp. 121-137 in T. N. Ferdinand (ed.), Juvenile Delinquency: Little Brother Grows Up. California: Sage.

Ball, R. A. (1966). An empirical exploration of neutralization theory. Criminologica, 4 (2), 22-32.

Ball, R. A. & Lilly, J. R. (1971). Juvenile delinquency in a rurban [sic] county. Criminology, 9 (1), 69-85.

Brennan, W. C. (1974, December). Abortion and the techniques of neutralization. Journal of Health and Social Behavior, 14 (4), 358-365.

Buckley, M. R., Wiese, D. S., & Harvey, M. G. (1998, May-June). An investigation into the dimensions of unethical behavior. Journal of Education for Business, 73 (5), 284-290.

Cheng, H. K., Sims, R. R., & Teegen, H. (1997, Spring). To purchase or pirate software: An empirical study. Journal of Management Information Systems, 13 (4), 49-60.

Christensen, A. L. & Eining, M. M. (1991, Spring). Factors influencing software piracy: Implications for accountants. Journal of Information Systems, 67-80.

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

Clausing, J. (2000). Software executives say consumers will pay for piracy. New York Times Online. [Online] Available http://partners.nytimes.com/library/tech/00/06/cyber/articles/08piracy.html

Cohen, E. & Cornwell, L. (1989). College students believe piracy is acceptable. CIS Educator Forum, 1 (3), 2-5.

Computer crime, can it affect you? (2000). Royal Canadian Mounted Police. [Online] Available http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html, November 10, 1999.

Colorado Governor Issues Executive Order On Computer Software Piracy. Business Software Alliance. [Online] Available http://www.bsa.org/bin/show.cgi?URL=pressbox/policy/952979724.html, March 25, 2000.

Cressey, D. R. (1953). Other people's money: A study of the social psychology of embezzlement. Montclair, NJ: Patterson Smith.

Cressey, D. R. (1970). The respectable criminal. In James Short (ed.), Modern Criminals. New York: Transaction-Aldine.

Crown, D. F. & Spiller, M. S. (1998). Learning from the literature on collegiate cheating: A review of empirical research. Journal of Business Ethics, 17 (6), 683-700.

Eining, M. M. & Christensen, A. L. (1991). A psycho-social model of software piracy: The development and test of a model. In Ethical Issues in Information Systems (editors: R. Dejoie, G. Fowler, & D. Paradice), Boyd & Fraser Publishing Co., Boston, MA, pp 134-140.

Ellis, D. R. (1986, April). Computer law – A primer on the law of software protection. The Florida Bar Journal.

Glass, R. S. & Wood, W. A. (1996). Situational determinants of software piracy: an equity theory perspective. Journal of Business Ethics, 15, 1189-1198.

Global Software Piracy Report. (1997). International Planning and Research Corporation for the Business Software Alliance and Software Publishers Association. [Online] Available http://www.bsa.org/statistics/97ipr.pdf, October 9, 1999.

Global Software Piracy Report. (1998). International Planning and Research Corporation for the Business Software Alliance and Software Publishers Association. [Online] Available http://www.siia.net/piracy/pubs/99g.asp, August 01, 2000.

Gopal, R. D. & Sanders, G. L. (1998, December). International software piracy: Analysis of key issues and impacts. Information Systems Research, 9 (4), 380-397.

Harrington, S. J. (1989, Summer). Why people copy software and create computer viruses: Individual characteristics or situational factors? Information Resources Management Journal, 28-37.

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

Henry, S. (1990). Degrees of Deviance, Student Accounts of Their Deviant Behavior. Salem, WI: Sheffield Publishing Company.

Hindelgang, M. J. (1974). Moral evaluation of illegal behaviors. Social Problems, 21, 370-385.

Hollinger, R. C. (1991). Neutralizing in the workplace: An empirical analysis of property theft and production deviance. Deviant Behavior, 12, 169-202.

Hudson, G. (1995, October). Copyright in the digital medium: A comparison of two proposals. Massachusetts Institute of Technology. [Online] Available http://www-swiss.ai.mit.edu/6805/student-papers/fall95-papers/hudson-copyright.html, December 12, 1999.

Im, J. H & Koen, C. (1990). Software piracy and responsibilities of educational institutions. Information & Management, 18, (4), 189-194.

Im, J. H. & Van Epps, P. D. (1991, Summer). Software piracy and software security in business schools: An ethical perspective. Data Base, 22 (3), 15-21.

Im, J. H., & Van Epps, P. D. (1992a). Legal and ethical issues of software piracy. International Association for Computer Information Systems. New Orleans, LA.

Im, J. H. & Van Epps, P. D. (1992b). Software piracy and software security measures in business schools. Information & Management, 23, (4), 193-203.

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.

Internet Software Piracy. (1998). Business Software Alliance. [Online] Available http://www.nopiracy.com/internet_piracy_c.html, December 12, 1999.

Kievit, K. (1991, Fall). Information systems majors/non-majors and computer ethics. Journal of Computer Information Systems, 32 (1), 43-49.

Landsheer, J. A., Hart, H., & Kox, W. (1994, Winter). Delinquent values and victim damage: Exploring the limits of neutralization theory. British Journal of Criminology, 34 (1), 44-53.

Klocklars, C. B. (1974). The Professional Fence. New York: Free Press.

Lanier, M. & Henry, S. (1998). Essential Criminology. Boulder, CO: Westview Press.

Leventhal, L. M., Instone, K. E., & Chilson, D. W. (1992). Another view of computer science ethics: patterns of responses among computer scientists. Journal of System Software, 17, 49-60.

Malhotra, Y. (1994a, June). Controlling copyright infringements of intellectual property: The case of computer software – part one. Journal of Systems Management, 45, 32-35.

Malhotra, Y. (1994b, July). Controlling copyright infringements of intellectual property: The case of computer software – part two. Journal of Systems Management, 45, 32-35.

McCarthy, J. G. & Stewart, A. L. (1998, December). Neutralisation [sic] as a process of graduated desensitization: Moral values of offenders. International Journal of Offender Therapy and Comparative Criminology, 42 (4), 278-290.

Michigan State University AUP. (1998). Network Communications Committee of C.C.S.A.C. Vice Provost for Computing and Technology. [Online] Available http://www.msu.edu/dig/aup/msuaup.html, November 29, 1999.

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

Minor, W. W. (1980, May). The neutralization of criminal offense. Criminology, 18 (1), 103-120.

Minor, W. W. (1981, July). Techniques of neutralization: A reconceptualization and empirical examination. Journal of Research in Crime and Delinquency, 18 (1), 295-318.

Oz, E. (1990, August). The attitude of managers-to-be toward software piracy. OR/MS Today, 17 (4), 24-26.

Patrizio, A. (1999, August 23). DOJ cracks down on MP3 pirate. Wired News. Wired Digital, Inc. [Online] Available http://www.wired.com/news/politics/0,1283,21391,00.html, November 20, 1999.

Peace, A. G. (1995). A predictive model of software piracy behavior: An empirical validation. Unpublished doctoral dissertation, University of Pittsburgh.

Peace, A. G. (1997, Fall). Software piracy and computer-using professionals: a survey. Journal of Computer Information Systems, 38 (1), 94-99.

Pfuhl, E. H. & Henry, S. (1993). The Deviance Process. 3rd ed. Hawthorne, NY: Walter de Gruyter, Inc.

Pogue, David. (1998, October 30). Some "warez" Over the Rainbow. MacWorld. 14,10.

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

Rahim, M. M., Seyal, A. H., & Rahman, N. A. (1999). Software piracy among computing students: a Bruneian scenario. Computers and Education, 32, 301-321.

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

Reid, R. A., Thompson, J. K., & Logsdon, J. M. (1992, Fall). Knowledge and attitudes of management students toward software piracy. Journal of Computer Information Systems, 33, 46-51.

RIAA - The Net Act. (2000). Recording Industry Association of America. [Online] Available http://www.riaa.com/Protect-Online-2.cfm

Rogers, J. W. & Buffalo, M. D. (1974). Neutralization techniques: Toward a simplified measurement scale. Pacific Sociological Review, 17 (3), 313-331.

Sacco, V. F. & Zureik, E. (1990). Correlates of computer misuse: data from a self-reporting sample. Behaviour and Information Technology, 9, 353-369.

Sample Corporate Policy Statement. (1999). Software & Information Industry Association. [Online] Available http://www.siia.net/piracy/programs/sftuse2.htm, December 12, 1999.

Seale, D. A., Polakowski, M., & Schneider, S. (1998, Jan-Feb). It's not really theft! Personal and workplace ethics that enable software piracy. Behaviour and Information Technology, 17 (1), 27-40.

Simpson, P. M., Banerjee, D., & Simpson, C. L. Jr. (1994). Softlifting: A model of motivating factors. Journal of Business Ethics, 13, 431-438.

Sims, R. R., Cheng, H.K., & Teegen, H. (1996). Toward a profile of student software piraters. Journal of Business Ethics, 15, 839-849.

Smith, R. (1997, January). Internet Piracy. Australian Institute of Criminology. Trends and Issues in Criminal Justice, 65, 1-6.

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

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

SPA Anti-Piracy Division's Copyright Protection Campaign. (1998). Software and Information Industry Association. [Online] Available http://www.siia.net/piracy/programs/backgrounder.htm, December 12, 1999.

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

Software Watchdog Attacks Cyberpiracy. (1999). Business Software Alliance. [Online] Available http://www.bsa.org/pressbox/enforcement/index.html?/pressbox/enforcement/942331921.html, December 11, 1999.

Solomon, S. & O'Brien, J. A. (1990, Spring). The effect of demographic factors on attitudes toward software piracy. Journal of Computer Information Systems, 40-46.

Student Rights and Responsibilities at Michigan State University. (1999). Michigan State University. [Online] Available http://www.vps.msu.edu/SpLife/afr1.htm, March 27, 2000.

Study of the Social Consequences of the Internet. (2000). Stanford Institute for the Quantitative Study of Society. Stanford University. [Online] Available http://www.stanford.edu/group/siqss/Press_Release/Preliminary_Report.pdf

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

Sykes, G. M. & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22, 664-670.

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

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

Thompson, W. E. & Harred, J. L. (1992, July-September). Topless dancers – managing stigma in a deviant occupation. Deviant Behavior, 13 (3), 291-311.

Thou Shalt Not Dupe. (1984). Association of Data Processing Service Organizations. Arlington, VA.

Thurman, Q. C. (1984). Deviance and the neutralization of moral commitment: An empirical analysis. Deviant Behavior, 5, 291-304.

Tittle, C. R. (1980). Sanctions and social deviance: The question of deterrence. New York: Praeger Publishers.

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

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

Wong, E. Y. H. How should we teach computer ethics? (1995, December). A short study done in Hong Kong. Computers and Education, 25 (4), 179-191.

Wong, G., Kong, A., & Ngai, S. (1990, November). A study of unauthorized software copying among post-secondary students in Hong Kong. The Australian Computer Journal, 22 (4), 114-122.

Wood, W. & Glass, R. (1995, Winter). Sex as a determinant of software piracy. Journal of Computer Information Systems, 36 (2), 37-40.

Young, M. (1988). The indignant page: Techniques of neutralization in the publications of pedophile organizations. Child Abuse and Neglect, 12, 583-591.