2010

Student Digital Piracy In The Florida State University System:an Exploratory Study On Its Infrastructural Effects

Jeffrey Reiss
University of Central Florida

STUDENT DIGITAL PIRACY IN THE FLORIDA STATE UNIVERSITY SYSTEM: AN EXPLORATORY STUDY ON ITS INFRASTRUCTURAL EFFECTS

by

JEFFREY REISS
B.S. University of Central Florida, 2003
M.S. University of Central Florida, 2005

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Education
in the Department of Educational Research, Technology, and Leadership
in the College of Education
at the University of Central Florida
Orlando, Florida

Spring Term
2010

Major Professor: Rosa Cintrón

ABSTRACT

Digital piracy is a problem that may never disappear from society. Through readily available resources such as those found in a university, students will always have access to illegal goods. While piracy is a global phenomenon, an institution's resources combined with the typical college student's lack of funds makes it more lucrative. Students use a number of methods to justify their actions ranging from previewing media to bringing justice to a corrupt company. While trying to understand the mindset of pirates is one route to deal with piracy, corporations attempted to alleviate the situation using added software encoding. These messages are not always effective, and in some cases caused further damage to consumer morale. Furthermore, students such as Joel Tenenbaum, who continued to pirate music despite warnings from his parents and the recording industry, exemplify the type of person that is unfazed by legal threats, leading to a question of ethics. Students may not feel that downloading is stealing despite numerous warnings from the Digital Millennium Copyright Act and other major media organizations. The predominant solution used by universities involves monitoring the students' network connection to detect Peer-to-Peer (P2P) connections or other connections that involve the transferring of copyrighted goods. Unfortunately, the current tools contain flaws that a crafty student may easily circumvent, undermining any attempts a university's IT department may use to deter piracy.

This study explored the nature of piracy prevention tools used by IT departments in the Florida State University System in order to determine their relative effectiveness. The study also looked into the opinions of the Information Security Officer in terms of alternative piracy prevention techniques that do not involve legal action and monitoring. It was found that most institutions do not use a formal piece of software that monitors for infringing data. They also stated that while their current techniques can do its required task, it was not perfected to a point where it could run autonomously. Furthermore, institutions agreed that students lack proper ethics and concern over the matter of copyright, but were not fully convinced that other preventions methods would be effective. The study ultimately considered monitoring techniques a short-term solution and that more research should be put into finding long-term solutions. It also implied that IT departments should be better funded in order to keep up with the technological gap.

ACKNOWLEDGMENTS

First of all, I would like to thank my dissertation committee chair and advisor, Dr. Rosa Cintrón. Your passion for this program ensured that I reached my fullest potential in writing this dissertation. I greatly appreciate all of your dedication and guidance through the process. Thanks also go out to my committee members Dr. Tammy Boyd, Dr. Margaret Miller, and Dr. George Pawlas. Your suggestions and comments during the defense process helped immensely. I also value your collective interest in a topic that was a bit outside of the "norm" for this program.

I would also like to thank my friends and extended family for their consistent moral support and understanding of the level of commitment required for this process. Your thoughts and well wishes were always much appreciated.

To my sister, Dr. Elayne Reiss, commonly known as my "younger, female clone," I thank you for putting up with me over all these years of academia. The program would not have been nearly as interesting or fun without you. I am proud that we have now had the unique opportunity as brother and sister to graduate from the same program with the same degrees at the same time on three separate occasions. Finally, I would like to thank my parents for their support, encouragement, and patience.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: PROBLEM AND RESEARCH DESIGN

Introduction

Since the advent of the Internet, the act of copyright infringement has become an increasingly difficult issue to control. In the past, acts of copyright infringement were few and far between, but once devices such as the photocopier, the video cassette recorder (VCR), and most importantly, the Internet came into use, infringing became significantly easier to perform and harder to track (Liebowitz, 2006). The legal definition as stated by Nolo (2009) is:

> Any unauthorized use of a copyrighted work other than fair use. Uses can range from outright plagiarism to using a portion of a photograph in a CD-ROM. The copyright owner may file a lawsuit to stop the infringement and collect damages from the infringer, provided the owner has registered her copyright with the U.S. Copyright Office. (n.p.)

Given these restrictions, fair use has remained a major loophole in copyright law. Fair use consists of a list of uses that are still acceptable under copyright law despite violating copyright law at face value. For example, if a professor were to record a television program to show in a classroom environment, it would fall under fair use. If the professor then showed the program at an event outside of the educational environment, the showing would constitute a copyright infringement because it was no longer being used for an educational purpose (Chiang & Assane, 2007).

Though copyright infringement and piracy have always existed, the advent of the Internet has made the act easier to perform and harder to control. As a result, companies started taking measures to combat piracy using technologies such as CD-Keys on software to prove that a copy was authentic, and Digital Restrictions Management (DRM) to control what a user could do with the media. Chiang and Assane (2002) also discovered that the majority of people who pirated or infringed on copyrights were college students. Based on their work, they also theorized that a main factor was a combination of the financial limitations of college students and their technical ability to use Peer-to-Peer (P2P) software. With the combination of these two traits, students possessed both the technical savvy and the motivation to pirate media which could easily cause problems for a campus network.

At the same time, the usefulness of copyright prevention features such as DRM and network software that allowed network operators to monitor for P2P usage has led groups such as the Common Solutions Group (2008), a group of Information Technology (IT) professionals in various universities, to question the effectiveness of monitoring alone. Furthermore, the Common Solutions Group has held the belief that methods such as DRM and monitoring represent only one step of the process to help correct a student's downloading habits. Until student computer ethics are simultaneously enforced as well, the problem will not be solved. Further support for such a proposal has emerged from the 2009 Joel Tenenbaum case. Tenenbaum was a student who was the focus of the Recording Industry of America's (RIAA) second trial-by-jury. He was accused of downloading 30 songs and was defended by Harvard Law Professor, Charles Nesson. Nesson originally aimed to argue the defense via fair use, but the judge ruled against that approach at the last minute. Tenenbaum, a habitual downloader who continued to download illegally even after discovering he was being sued, ultimately admitted his guilt and was fined $675,000 in damages. Authors have indicated that theoretically, the constant pressure of computer ethics may help contribute to preventing such incidents from reoccurring in the future (Anderson, 2009a; Sheffner, 2009a, 2009b).

Problem Statement

The majority of people who have engaged in modern-day acts of copyright infringement and digital piracy have been students in colleges and universities. Private industries, namely the Recording Industry Association of America (RIAA), have pressured institutions into becoming watchdogs (Chiang & Assane, 2002). Such acts reached a peak when Congress passed the 2008 reauthorization of the Higher Education Act of 1965. Among the many changes made to the Act was one that directly created mandates to postsecondary institutions about file sharing of copyrighted materials. The amended Act included rules such as providing "an annual disclosure that explicitly informs students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may be subject to the students to civil and criminal liabilities" (Higher Education Act of 2008, §487), along with a summary of the federal laws. Though the majority of universities have already adopted such rules and policies, not all institutions have possessed software that actively blocks transmissions that may contain copyrighted material. The amendment does not possess any form of action for failure to comply in 2010, but implementing some form of action has been inevitable and institutions may find themselves in a precarious position if funding is not provided to those without a form of copyright infringement policy and monitoring software (Worona, 2008).

The Higher Education Act has forced all institutions to have some form of this software in place on campus networks. The major issue with this addition has been that the software is expensive and takes a considerable number of man-hours to properly implement on a campus network. According to Green (2008), some universities may be required to spend at least $500,000 annually on Peer-to-Peer compliance--money that could be spent on a new degree program. Furthermore, the ease of implementation depends on both the size and structure of a campus's network. To complicate matters further, all of the available software has at least one flaw which could either permit a crafty student to circumvent the protection, or it may be filtered to the point where legitimate use of the resource is either impeded or prevented (Electronic Frontier Foundation, 2006; Worona, 2008).

At the time of this study, colleges and universities needed to comply with new legislation from the 2008 revision of the Higher Education Act of 1965 by taking a stronger stance on preventing students from procuring copyrighted material over the Internet. Because part of the revision has included purchasing and maintaining costly software, this study aimed to determine if a better, more cost effective alternative that infringed less on student rights was in existence for the institution.

Purpose of Study

With digital piracy by college students becoming an increasingly important topic, this study was focused on obtaining opinions about digital piracy from those who deal with it on a constant basis, the university IT professional. In this study, there was also an attempt to uncover more amicable alternatives to copyright infringement prevention that would benefit both the student and support the financial concerns of postsecondary institutions during the harsh economic climate of the 21st century. With the addition of the copyright infringement prevention clauses in the 2008 revision of the Higher Education Act, any institution funded by the Act was required to comply or face the possibility of losing precious federal funding. The research also aimed to heighten the awareness of the issue of student piracy on campus and the multiple facets the topic truly entails.

Significance of the Study

With pressure from the RIAA and federal policies introduced in 2008, post-secondary institutions must implement software to monitor network activity to keep students off P2P software, dorm servers, and any other online method of transferring media illegally (Joachim, 2004; Worona, 2008). Though some larger universities, such as the University of Florida, had already implemented software prior to the 2008 revision of the Higher Education Act, the remaining community colleges and smaller institutions were required to do the same. Furthermore, as the new rules currently stand, institutions will not, at the present time, suffer any penalties for failing to follow the procedures. After the appropriate committees interpret the rules, it is likely, however, that institutions will lose federal financial compensation for implementation failure, which makes the process burdensome for smaller, financially starved institutions (Worona, 2008). Though software will always play an important role, an expensive software solution becomes useless if students manage to find an alternate route around the software. As a result, an institution may ultimately waste money on an ineffective solution only to replace it with another solution with a limited life-span due to the constant evolution of technology.

The P2P blocking software, however, is only one part of the problem. With most institutions also blocking dorm servers and other potential outlets of piracy, students feel that their personal freedoms are hindered. Despite the plethora of legal uses for P2P, its adoption has been stifled due to the focus on illegal use. The dorm server ban is also problematic in a historical sense. The popular search engines Yahoo! and Google, two companies that made major contributions to the overall state of the Internet, began as dorm servers. By preventing students from utilizing these resources, institutions could easily and unknowingly prevent the next major Internet innovation because they were forced to satisfy a large private interest (Joachim, 2004). Thus, by exploring solutions that rely on more than software and legal threats, a university could potentially eliminate digital piracy without denying freedoms to students.

The majority of the literature related to piracy (Chiang & Assane, 2002, 2007, 2008; Gopal, Sanders, Bhattacharjee, Argwall, & Wagner, 2004; Gupta, Gould, & Pola, 2004; Higgins, 2005; Higgins, Fell, & Wilson, 2006; Hinduja, 2008; LaRose, Lai, Lange, Love, & Wu, 2005; Liang & Yan 2005; Logsdon, Thompson, & Reid, 1994; Rob & Waldfogel, 2006; Siegfried, 2004; Sims, Cheng, & Teegen, 1996) has focused only on the student. Some researchers have examined only student demographics, and others have been based on different theories of student behavior. None of the researchers, however, have explored the opposite end of the piracy spectrum in which universities must police their students. By combining the knowledge of student attitudes towards piracy, along with information from the IT perspective, a feasible solution to the copyright problem may finally emerge.

Research Questions

The following research questions guided this study:

1. What steps, policies, and measures have the 11 institutions that comprise Florida's State University System (SUS) taken to prevent copyright infringement as defined by Section 487 of the 2008 Higher Education Act?
2. What are the challenges of implementing the mandates stated in Section 487 of the 2008 Higher Education Act that require the introduction and implementation of tracking software?
3. What alternatives, if any, were considered or are currently being considered to discourage piracy by college students at a lower cost than monitoring software?

Definition of Terms

Computer Security Officer: An IT employee who is in charge of maintaining the security policies, and stability of a computer network (Goodyear, Salaway, Nelson, Petersen, & Portillo, 2009).

Darknet: A network that hides behind encryption, preventing software from detecting the information users transfer between one another (Electronic Frontier Foundation [EFF], 2008).

Digital Restrictions Management (DRM): Technology that inhibits actions that would otherwise violate a piece of media's copyright (Lincoff, 2008).

Electronic Frontier Foundation (EFF): An organization that is fighting for a more amicable solution for the pirating scenario that embraces the current digital technology, but still upholds copyright law.

Internet Service Provider (ISP): A company that provides Internet access to consumers. This may include private companies (phone and cable) and postsecondary institutions (VoIP Terms, 2009).

Internet Protocol (IP): A computer or server's address on the Internet. This is used to help identify users (VoIP Terms, 2009).

Motion Picture Association of America (MPAA): The organization that represents all of the major movie companies (Einav, 2008).

Peer-to-Peer (P2P) software: A program that allows one computer to directly connect to other computers in order to transfer files more efficiently (Adamsick, 2008).

Piracy: The act of procuring digital goods through illegal means. It also encompasses the illegal use or redistribution of copyright-protected works. It does not exhibit any similarities to plagiarism which is stealing one's ideas to claim as one's own while failing to credit the original source (Dames, 2007).

Ports: A virtual location that digital information is sent through. For example, e-mail is sent through port 25, standard web browsing is through port 80, and secure web browsing is through port 443 (EFF, 2006).

Recording Industry Association of America (RIAA): The organization that represents of all the major record labels in the United States. They are also the primary player in any litigation (EFF, 2008).

Rootkits: Pieces of software that operating systems and anti-virus software cannot detect and are typically used as a backdoor for viruses, trojan horses, and other malicious code (LaBelle, 2006).

Secure Socket Layer (SSL) encryption: The most common method of encrypting a connection through the Internet. It is used in all transactions that involve exchanging sensitive information to prevent a third-party from intercepting or reading the data (EFF, 2006).

Seeding: Part of the P2P functionality where the user hosts a completed version of a file to share between other users. The more seeders present, the faster a file transfers (P2P, 2009).

Conceptual Framework

Because non-student-based studies on the effects of digital piracy in universities are new, no known framework models currently exist. Automated morality as described by Friedman and Kahn (1992), however, will provide an appropriate starting point. Automated morality usually appears in fields such as artificial intelligence, but the software used to detect and stop the transfer of copyrighted material falls under these parameters. A program such as CopySense uses a set of defined parameters to check Internet traffic for known P2P violations and suspend the user's Internet account (Common Solutions Group, 2008). Friedman and Kahn made an analogy using a medical system known as APACHE (Acute Physiology, Age, Chronic Health Evaluation, Knaus et al., 1991) which decides on pulling life support from patients in an intensive care unit. In a closed-circuit situation, the system takes complete control, acting as both the patient's family and doctor, and allowing the medical professionals involved to distance themselves from making a life or death situation. In reality, the APACHE system should act as a consultant rather than the decider to allow medical personnel to make the final call. By relying primarily on the software, IT professionals would also rely on the software to make the ethical decision of whether or not to disconnect the user.

Stahl (2004) explored the concept of autonomous moral agents from the perspective of the Moral Turing Test. Based on the traditional Turing Test that determines if a computer program could imitate human thought patterns, the Moral Turing Test determines if a computer program could imitate the behavior of a moral being. The use of the term "imitate" is used because determining if a computer could truly think like a person has been impossible to prove. Ethics as well as morality can take so many different routes that no one will ever decide upon what truly is ethical and moral from a theoretical perspective. Furthermore, while a computer could imitate a moral being, the computer also processes morality from a black and white perspective according to its programming. Humans, unlike computers, rationalize their ethical decisions. This is both beneficial and dangerous according to the situation. This situation can be related to Friedman and Kahn's (1992) analogy of the medication machines and monitoring software. Both imitate moral thought and are limited by their programming. If a student were to pirate a song for educational reasons that would safely fall under fair use. Monitoring software would, however, flag and block the student because its programming was unable to determine the difference between fair use and outright piracy. If the same situation were replayed with more human interaction, the student could notify the IT department prior to the act and obtain permission. From this perspective, human-based ethics and morality supersede the monitoring software as a moral agent.

Wallach, Allen, and Smit (2008) have viewed moral agents from a programming perspective. Though this perspective may not directly tie with this study, it could affect the future of monitoring software. Organizations such as the Common Solutions Group (2008) believed that monitoring software will continue to evolve and that programming a more effective and ethical piece of monitoring software will become more useful in the future. Programming ethics, however, contains its own set of debates as to the values and beliefs that should comprise an artificial intelligence system or if the parameters should take a traditional stoic stance. Regardless, a paramount concern involves trust. If the IT professional cannot trust the software, problems will occur and the overall effectiveness of the software and IT staff will degrade as a result of constantly monitoring the software to ensure it performs its tasks to the desired specifications. By trusting the software, IT staff can focus on other, potentially more important tasks while the software operates to the staff's expectations.

Delimitations of the Study

Considering the scope of the 2008 revision of the Higher Education Act, a national study was warranted. Due to time limits on the study, however, the population was restricted to the 11 Florida State University System (SUS) institutions. Because the majority of studies had been concerned with the student aspect of the situation, there was a greater need to explore the administrative component of the problem.

1. The data were limited to only post-secondary institutions in the state of Florida.
2. Only key personnel in university network operations were surveyed via a questionnaire distributed through the Internet.

Organization of the Study

This dissertation has been organized into five chapters. Chapter 1 contains a brief introduction to the study and the concept of digital piracy. Chapter 2 explores the literature based on piracy; P2P usage on campus, the major technologies behind P2P and what is used to prevent it; major lawsuits involving P2P; and student ethics on piracy and computer usage. Chapter 3 details the methodology used to conduct the study. Chapter 4 reveals the results of the study. Finally, in Chapter 5, discussion, conclusions and recommendations related to the issue of copyright infringement and privacy in post-secondary institutions are presented.

CHAPTER 2: LITERATURE REVIEW

Introduction

The literature review has been organized to discuss the many facets of the student piracy problem. First, a general history of copyright law and piracy is provided followed by a review of many of the methodologies used to identify student piracy. Next, the technological and policy rules to combat piracy and their effectiveness are explored. Finally, the potential solution of ethics are discussed with an overview of ethical theory and challenges to ethics in the digital environment.

The History of Copyrights and Copyright Infringement

Copyrights and copyright infringement are far from new concepts. Originating in medieval times in a different form as a response to the invention of the printing press, copyrights first appeared in Renaissance Italy to grant "monopolies in the form of exclusive licenses to print or sell books for a particular term" (Sun & Baez, 2009, p. 13). In other words, copyrights granted a company the rights to publish a particular book for a set period time along with any other subsequent rights. Unlike the modern copyright that has focused on the author, the original copyright aimed to protect the publisher because most high-demand publications were public domain. In the United States, the framers of the Constitution granted Congress the ability to provide exclusive rights to people's works or discoveries. At the copyright law's inception in the United States, a person was granted 14 years to exclusively publish a new work and 21 years for any pre-existing work. By providing these rights, the goal was to promote creativity and discovery in the nation and allow those who devised the work to appropriately benefit (Sun & Baez).

Any work is protected by a copyright upon its completion, but only works under a registered copyright may seek damages upon infringement. In order to obtain a registered copyright under the United States copyright laws, the work must meet certain requirements. The work must be "'original works of authorship' that are fixed in a tangible form of expression. The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device" (U.S. Copyright Office, 2008, pp. 2-3). This means that the work must exist in some physical form as opposed to a concept like choreography or ideals. The length of a copyright's exclusivity began at 14 years. Any work created on or after 1978, however, has been protected for the life of all authors involved in the work plus 70 years. All "for hire" or anonymous work copyrights, however, lasts for "95 years from publication or 120 years from creation, whichever is shorter" (U.S. Copyright Office, p. 5). Regardless, any copyrighted material has been determined to remain exclusive to the author during the entire lives of the majority of the nation (U.S. Copyright Office). Thus, copyrights in the United States evolved tremendously from a simple right to exclusively publish for a set period of time to the right to exclusively publish one's material for the remainder of one's life.

In the university setting, however, ownership of the copyright may become questionable depending upon the circumstances. Any copyrightable material created as an employee of the university becomes property of the university, not the student or faculty member. If a non-academic employee is hired, the employee will only retain ownership if the contract warrants it. Students working under their own means in the university environment, however, retain ownership (Sun & Baez, 2009).

Foreign Copyrights and the United States

Though works in the United States always benefited from copyright protection, protecting foreign works left much to be desired. Up until 1891, foreign works received no copyright protection whatsoever in the United States (Nimmer, 1992). Hence, the United States was once a hotbed of piracy of a different type. Instead of digital works, it was foreign works and the government refused to step in because of economic reasons. The United States could not afford the fees related to protecting foreign works, and American authors had not yet been recognized on a global level. In 1891, the United States finally began to acknowledge foreign copyrights in response to the Berne Convention of 1886. The Berne Convention created the first international copyright treaty which the United States declined to ratify for the aforementioned reasons. The International Copyright Act of 1891, the Chace Act, provided minimal to non-existent copyright protection. If a foreign work complied with traditional United States notice, registration, deposit, and a manufacturing clause, a copyright would be granted. Although the first three components were expected, the manufacturing clause required foreign works to utilize American materials (Nimmer). Until the manufacturing clause was removed in the 1976 copyright reform, the Chace act proved to make foreign copyright protection more illusory than useful.

In 1955, the United States helped charter the Universal Copyright Convention which gave an alternate route for United States works to obtain international protection through concurrent releases in the States and in a Berne Convention nation such as Canada. Berne Convention members who were not part of the Universal Copyright Convention, however, did not need to protect copyrights of American works. Following a lost case in Thailand where the concurrent release method was not recognized and the general air of the United States acting hypocritical of itself, the United States finally ratified the Berne Convention into copyright law (Nimmer, 1992). Considering it took close to 200 years for the United States to properly work with foreign copyrights, one must wonder how long it will take for proper handling of digital copyrights.

The Fair Use Clause

Fair use has been commonly viewed as the one loophole in copyright law that allows people to use the original material in its original form without any legal repercussions. As defined by the Copyright Act, fair use is granted after considering the following four factors:

> (1) The purpose and character of the copying, including whether the use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the work being copied; (3) the amount and substantiality of the portion that is copied in relation to the copyrighted work as a whole; and (4) the effect of the copying upon the potential market value of the copyrighted work. ("Software Piracy," 1998)

Thus, factors such as whether or not the material is published, being used in an educational setting, and the proportion of the material being used verbatim will also determine if fair use applies (Edgar, 2003). Digital works also allow personal backups as an additional method, but allowing a friend to borrow a CD under the guise of making a "backup" copy falls under infringement and piracy.

Klein, Lerner, and Murphy (2002) questioned the value of fair use in a networked environment. In the Napster trial, the company attempted to use fair use as a defense for the illegal file sharing occurring on its network. Going under the terminology of sampling, users may sample a song before purchasing a full album.

Such a methodology, however, is problematic when a user may download an entire album with relative ease. Napster also likened its software as a form of “space shifting” which involves taking songs and moving them to another location for personal use; similar to how VHS recorders allow a person to record a program and view it at a later time or at another location. Klein et al. further believed that while such a method is accepted in the courts for devices such as mp3 players as a form of fair use, they rejected the claim made by Napster. In the Napster scenario, mp3 copies would be considered to be less valuable than the original and would also make the original less desirable in a long-term scenario. Library versions of books may cost more than consumer versions because the copyright holder expects people to make copies, but in the case of Napster, file s can come from any source. A library version of a CD could never be created and in turn leads to higher prices to compensate. Finally, the authors also believed that while mp3 devices fall under the umbrella of fair use, mp3 devices may encourage illegal copying. At the same time, denying a user the ability to make a copy of a purchased CD for personal use infringes upon fair use, leading to copy-protection and DRM to restrict the user to only do what the record labels consider fair use.

Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) was passed in 1998 and at the time of the present study was the latest copyright law designed to provide some clarification on digital copyrights. The DMCA added extra restrictions to digital media, but standard copyright procedures remained the same. Any means of circumventing a control on digital media such as DRM was prohibited with some exceptions. Circumvention was authorized for actions such as U.S. government employees or law-enforcement if it was pertinent for an investigation, and for software developers who needed to ensure interoperability. Furthermore, companies were allowed to issue DMCA take-down notices which are legal subpoenas if it was discovered that copyrighted material illegally exists on a service or website. Thus, if copyrighted works appeared on a site such as YouTube, the owners of the copyright can and would force YouTube to remove the content (Hayes & Fenwick & West, 2001; Kierkegaard, 2006).

Software Piracy

With the advent of the computer, the initial concept of the copyright no longer fits. Despite the fact that current copyright laws protect tangible works, digital works have fallen into a gray area that has been harder to define. Forester and Morrison (1994) noted that because software is more compact, easier to replicate, and easier to transmit, copyright laws cannot offer the same level of protection that more tangible works enjoy. Signs of how copyrights altered the landscape have come from increasing numbers of patents, copyright registrations, and infringement lawsuits. Forester and Morrison also noted the trend for companies to utilize copyrights to help increase their profits rather than to defend their work. In some cases, the dispute could be a legitimate infringement, but in others the reasoning may seem trivial. In the mid-1980s, Lotus, the maker of the software Lotus 1-2-3, pressed charges against two smaller software companies over imitating the look and feel of Lotus 1-2-3. Lotus, in turn, was then sued by the Software Arts Products Corporation for utilizing the same keystrokes and commands as the program VisiCalc.

According to Forester and Morrison (1994), software Piracy first occurred in 1964 when Texaco was offered $5 million in stolen software. Other cases occurred over the years but were restricted to private corporate programs such as air-traffic control programs and CAD software. Although these instances of software piracy were simply a different form of stealing trade secrets, mass software piracy only surfaced with the advent of the desktop computer and Microsoft. Bill Gates created the software programming language, BASIC, as a part of a package with the desktop computer kit, the Altair. Despite the poor construction of the computer, the software proved more useful, and some people made copies of the program to prevent others from needing to purchase the entire package (Forester & Morrison).

This view combined with the more powerful viewpoint of a software package being too expensive helped fuel consumers' justification to pirate or sell counterfeit copies. With the help of the early form of the Internet, counterfeit software became easier to distribute. In 1992, a major crackdown occurred on an Internet bulletin board known as Davy Jones Locker that sold pirated versions of expensive programs such as AutoCAD, and a number of Lotus and IBM products. Considering the pirated software from this site crossed national boundaries into nations such as Iraq (Forester & Morrison, 1994), the notion of a hostile nation obtaining software that could lead to the creation of a weapon to be used against the United States or its allies could prove dangerous. Another crackdown in 1992 yielded approximately $9 million of pirated software across 10 sites. These sites not only included pirated versions of programs like MS-DOS but also possessed counterfeit versions of manuals, holograms, and even the packaging (Forester & Morrison).

In the courtroom, software piracy becomes harder to define. As Edgar (2003) noted, the term plagiarism may appear to be an appropriate term for piracy, but while a person is making a copy of another's work the copier is not claiming authorship of the file. At the same time, piracy can expand the range of one or two files or programs to the mass warehouses as described in the 1992 counterfeit software crackdown. This brings up the question as to the limits of policy (Forester & Morrison, 1994). The dilemma has been to find common ground for a policy to be applied to those who feel software should be free under any condition, and those who feel piracy is reprehensible in any situation. If a person pirates only one software program or song, it may be so minor that such an infraction, while still illegal, may be ignored. Though one infraction may be tolerable, there is the slippery slope issue as to just how many infractions can be permitted before the acts become intolerable.

When the Internet becomes a factor in a piracy case, determining who is responsible also becomes a gray area. Blame could be placed on the person who put the files up for download, the service that hosted the files, or even users who logged on and downloaded (Edgar, 2003). For music, the Recording Industry Association of America (RIAA) started with individual services such as Napster which left users immune, then moved to the individual users who both uploaded and downloaded files, and has since changed their tactics to holding Internet Service Providers as the responsible party in performing the RIAA's work (EFF, 2008).

Physical Media versus Digital Media

The differences between physical media and digital media, whether on a disc or obtained through an online service, have been considerably different from traditional media such as a book. As Edgar (2003) discussed, when copyrighted material such as a book is purchased by someone, that person becomes the sole owner of that copy. The individual is welcome to do whatever he/she wishes with that copy of the book--read it, sell it, let a friend borrow it--the book acts no differently than any other piece of property. The only restriction copyright law places is that substantial sections of or the entire work are never reproduced and redistributed with exception of fair use situations such as pure classroom uses (Edgar). Digital media has operated differently, because companies have sold licenses of a good rather than a physical reproduction. A license issued by a company only intends use of a good for one person and one computer in the case of software and digital downloads. Fair use principals would only apply for educational reasons or personal backups. A software license also creates complications in any of the aforementioned uses with traditional media. Clearly, a person could still use the media, but letting a friend borrow the media becomes a gray area because the friend could make an unauthorized copy. Software reselling or giving away old software also contains fuzzy rules because while the physical discs could be sold, the software was not licensed to the second person. If the software was already registered, the new user loses much of the software's functionality as a result. In a sense, software is akin to digital music downloads with DRM. There are a number of restrictions of what can or cannot be performed with the program; it is limited to a single user unless specified otherwise; and there will always be someone who feels the DRM presence is unjust for any application.

Software licenses may sound harsh and unfair, but Brancomb (1993) wrote that a trade secret license was the only way for software developers to protect their work before software was accepted into copyright law. When the copyright office eventually granted copyrights to programmers, the program's source code was considered the tangible portion of the software and further allowed software makers to remove any trade secrets from the code. In some cases, no identifying material was provided. When copyright infringement cases first surfaced afterward, determining what parts of the software fell under copyright protection soon came into question. The most notable was the Lotus 1-2-3 case against Borland's Quattro Pro. Although the two programs were different in terms of code, Quattro Pro also implemented an interface that captured a similar look and feel to Lotus 1-2-3, even using the same keystrokes (Brancomb). Despite the laws only applying to the software code, the judge concluded that Quattro Pro deliberately copied the interface to Lotus 1-2-3 in an environment where a number of different alternative routes were available citing Microsoft Excel as a program that offers similar services but presents itself in a manner that completely differs from Lotus 1-2-3. Other court cases agreed with the ruling coming to the conclusion that an idea such as a spreadsheet program or a word processor is public domain, but the manner that the program expresses said idea is protected by copyright law. Further enforced by Apple's case against Microsoft and Hewlett-Packard over both companies' creation of windows-like software, items must be considered "virtually identical" to contain any merit. The revised copyright scheme may appear to work, but it is still an adaptation of laws that never took an item such as software into consideration (Brancomb). With the added digital factor, it may finally be time to explore a new method if the corporations and record labels are willing.

Copyright Infringement and File Sharing

Liebowitz (2006) explored the history of copyright concerns with technology that related to legal issues regarding the increasing ease of infringement. A series of revolutionary devices were all enveloped in some form of copyright controversy: (a) The photocopier made illegal replication of copyrighted text easier, (b) the video cassette recorder made copying television broadcasts easier, and (c) CD/DVD recorders made copying disk-based media easier. What makes file sharing stand out from the rest is the scope of the potential distribution. Previously, the copies could only be transferred between a small group of known people at one time. With file sharing, the same copy may be distributed among thousands of strangers, unbeknownst to the owner of the original (Liebowitz, 2006).

In order to properly understand the problem of file sharing, however, one must first understand the technology behind it. The majority of illegal file sharing has been conducted over peer-to-peer (P2P) networks. Adamsick (2008) described P2P technology as a unique form of file sharing that allows people to transfer a file in a decentralized environment. Before P2P, a person would simply log onto a server somewhere on the Internet and download a file. If copyrighted material existed on such a server, it would simply be a matter of time until the discovery and potential shutdown of the server. Considering that servers deliver information to a massive number of users, lawsuits were typically directed to the owner of the server rather than the thousands of people who connected and downloaded the files. By comparison, P2P technology breaks a file into small pieces, and users transfer pieces of the file among themselves until all the pieces are received. Provided enough people own copies of the file in question, files can be transferred at a significantly faster speed than through traditional methods. The Electronic Frontier Foundation (2006) stated that NASA has utilized the technology to reduce bandwidth costs for one of their programs. Unfortunately, while the technology has great potential in practical applications, it also provides the same potential for illegal file sharing.

P2P file sharing existed before Napster as a lesser-known program known as Hotline, a Mac-only program that hosted only a handful of users (Norton, 2009). The birth of modern P2P file sharing originated in 1999 when Shawn Fanning, a student of Northeastern University in Boston, developed Napster to share music with the rest of his residence hall. The program quickly gained popularity when people realized the abundance of digital versions of songs, but it was eventually stopped for Digital Millennium Copyright Act (DMCA) violations by the recording industry after a lengthy legal battle on the grounds of indirect copyright infringement. Even though

Napster did not infringe from a program perspective, it actually assisted in the act of copyright infringement by allowing the sharing of files that may or may not be commercial works (Langenderfer & Cook, 2001). Though the battle destroyed Napster, it encouraged piracy and the use of P2P and mp3 files. After Naptster lost its case in the courts, the company decided to pursue a legitimate route by retooling its network to serve as an online subscription service. In its wake, a plethora of alternative programs such as KaZaA replaced Napster, boosting the file sharing community (Gopal et al., 2004; Liebowitz, 2006; Norton; Oberholzer-Gee & Strumph, 2009).

After the RIAA's announcement in 2003 of charging individual users with copyright infringement, a sharp decline in usage occurred. Although the decline represented a public reaction to the RIAA's lawsuits, it is also possible that P2P traffic simply went into hiding. Karagiannis, Broido, Brownlee, Claffy, and Faloutsos (2004) believed that P2P technology left its infancy stage and began to provide users with options to let them hide from prying eyes. P2P originally worked on a specific Internet port in order to properly traffic data, but P2P has become configurable using any port. This means that a sneaky user could use port 80, the Internet port used to handle standard HTTP web traffic, to transfer P2P data. If monitoring software was not in tune with this tactic, crafty users could easily hide their activity. For systems that check all ports for offending traffic, P2P users also have had the option of encrypting their connection through SSL. Under SSL encryption, packet data are effectively invisible to monitoring software. Even if software detects packets across encrypted connections, any attempts to inspect it would result in a break in the connection. Thus, to an IT professional, the encrypted data connection could literally be anything, and the P2P connection would never be detected (Karagiannis et al.).

Karagiannis et al. (2004) attempted to determine if the theory of P2P traffic going "underground" was indeed occurring. The authors' monitoring techniques, however, contained a number of limitations. The main restriction involved not being able to inspect the entire packet. This created some ambiguity in what was being sent and obfuscated any P2P data transferred through the HTTP protocol. As mentioned earlier, any encrypted connections went undetected in the study. Finally, the study simply monitored all P2P traffic and could not differentiate between legal and illegal P2P data. Because of this limitation, legal P2P transfers that were not related to the RIAA's P2P crackdown were counted. To compensate for some of the limitations, traffic was split into multiple groups and coded as either P2P traffic, possible P2P traffic, or non-P2P traffic. The final results did agree with Karagiannis et al.'s initial hypotheses. The Fasttrack program, which the RIAA based most of its litigation on, showed declines as trends state, yet programs such as Gnutella and eDonkey maintained steady traffic and BitTorrent traffic showed major increases. These results also showed that users would easily jump from one program to another to avoid lawsuits. It was apparent that P2P was not likely to disappear in its entirety and was actually in a second recovery period. As Karagiannis et al. stated:

> The first comeback was the switch from the easy-to-locate Napster, to distributed Gnutella-like protocols [another P2P protocol]. Thus, locating a single responsible entity became impossible. The industry then relied on detecting P2P traffic. Now the users take a step further by making P2P traffic hard to identify. (p. 7)

From some perspectives, pursuing the individual through monitoring will become futile because as soon as software figures out how to detect the current method for hiding, P2P software will find a new way to disguise their traffic. P2P software even has the ability to alter its traffic patterns to make its usage less obvious. The findings by Karagiannis et al. easily match up with findings from the Electronic Frontier Foundation (2006) and the Common Solutions Group (2008).

Gopal et al. (2004) looked into digital music piracy by comparing it to software piracy. They explored various economic impacts digital music piracy has had on the industry compared to the main model the industry has used. First, the authors explored the mp3 file format and recordable CD devices--tools that continued to assist music pirating. Mp3 files that are compressed on audio tracks, so a song that takes up an eighth of a 650 megabyte CD may only take up two or three megabytes as an mp3. This helps increase the overall portability of music files and allows people to easily transfer an mp3 over means such as email. Combining the compressed audio file with a writeable CD and a single disc may "contain over 160 compressed digital music files that play for over 14 hours on a personal computer" (p. 90). This means that a single CD of mp3 files could contain between 14 and 18 standard albums, even more when factoring in digital media devices such as the iPod. When Internet service with increasing bandwidth speeds are also factored in, the problem becomes harder to control. An mp3 file is small enough that a person could transmit one or two files over a standard e-mail service. With file sharing services, the ease of transferring files becomes even greater.

With the prevalence of pirating and P2P, one questions the types of users on the piracy stage. Molteni and Ordanini (2003) conducted a study to identify different types of file sharers and determine potential solutions to reduce the probability that they would continue to pirate. Based on a sample of 204 individuals who answered a questionnaire on the Bocconi University website where 95% of the sample were students, the authors were able to create five different groups via cluster analysis. One group consisted of occasional downloaders who download some, but predominantly purchase, CDs. This group is essentially the control group because online strategies would least affect this group. The second group, the mass listeners, had a high dependency on P2P sites and rarely purchased CDs. Their file sharing practices are generally to obtain music for their own entertainment. The authors suggested that strategies that could provide a heightened experience or possibly a streaming service could benefit them. Third, the explorers/pioneers group used downloaded content to influence further CD purchases. This group could be beneficial to new artists if free songs are provided to their consumption. Fourth, the curious group used the act of downloading as a form of entertainment. Determining a solution for these people is almost impossible. Finally, the fifth group was the duplicators who downloaded music for the sole purpose of making copies. Like the curious group, finding a simple solution is difficult, but legal action may be the only path in this situation (Molteni & Ordanini). This study provided a solid foundation for the process of identifying solutions to such a massive problem involving diverse groups of downloaders.

Profiling Student Software Pirates

In order to truly understand the strength of the connection between students and piracy, a number of studies were conducted over the years. Cohen and Cornwell (1989) conducted one of the earliest studies that replicated prior studies of Schuster (1987) and Christoph, Forcht, and Bilbrey (1987/1988). According to Cohen and Cornwell, both of the prior studies held no real merit alone but if combined there could be significant results. Christoph et al. examined the ethical beliefs of Information Systems students at James Madison University but could not draw any conclusions from the results because there were no expert opinions with which to compare the student responses. The instrument contained reworded items from both studies along with a few new items to help bind the two together. The outcome of Cohen and Cornwell's study resulted in similar values to the other two studies and supported the generalization of students finding piracy and computer crimes to be acceptable, even hinting at faculty and administrators who also participated in piracy. The solution suggested by the authors was simply to further educate students about the illegalities of software piracy.

Demographic Profiling

One of the first actions in investigating software piracy by students is identifying the student piracy population. Chiang and Assane (2002, 2007, 2008) conducted multiple studies regarding the demographic composition of students most likely to violate copyright. Using predictive modeling in 2002, the authors concluded that young Caucasian and Asian males in technology-related majors were the most likely to share files. Such findings were supported in other studies (Higgins, Wolfe, & Ricketts, 2008). Gopal et al. (2004) further supplemented Chiang and Assane's (2002, 2007, 2008) findings by recognizing that the amount of media downloaded illegally correlated to a person's income. Considering that college students tend to lack their own income, it is not surprising that they have been considered to comprise the largest proportion of online piracy. Furthermore, Gopal et al. (2004) noted that the economic factor ceases to exist for “known” or familiar songs. In other words, students are more likely to pay for songs they know about than new or unfamiliar songs. Hohn, Muftic, and Wolf (2006), in their research on demographic factors for an institution where piracy was rampant, also agreed with the findings. Even when 80.7% of the surveyed population pirated some form of digital media, males and students with lower incomes were more likely to pirate than were females and students with higher incomes. Rahim, Seyal and Rahman (2001) also produced results that agreed with these studies using students from Brunei along with Gan and Koh (2006) in Singapore and Chiou, Huang, and Lee (2005) in Taiwan. These studies aided in identifying the global nature of the piracy problem.

This demographic profile was further supported by Chiang and Assane (2008) and Al-Rafee and Cronan (2006) who also added that females were more concerned with the risk factor and, thus, more likely to use legal alternatives. The willingness for a legal alternative was also supported by Chiang and Assane (2007) who used regression modeling techniques to conclude that students were less likely to infringe if cheaper alternatives or download services such as Apple Corporation’s iTunes were provided. Though the later studies have been more appropriate considering the rapid changes in technology over the decade, the original surveys given to students in Chiang and Assane’s (2007, 2008) studies were from 2003 when mainstream legal alternatives were not as developed.

Mishra, Akman, and Yazici (2006), obtained differing demographic results with their study of IT professionals. Though males pirated more than females, there was no significant difference between the two. Age, income, and experience were found to be significant contributors to piracy, but education showed no significant impact. In contrast, Higgins and Makin (2004) found that the typical demographic variables of age, gender, and computer use were insignificant in their self-control theory model.

Sims et al. (1996) performed one of the first studies related to profiling software pirates outside of computer-related majors. Their aims were to find specific characteristics that could easily identify links between the unethical behavior and various demographic characteristics including age, if the person was in college, gender, and computer familiarity. In regard to age, gender, and familiarity with computers, it was determined that software pirates were generally under the age of 24, male, and were not heavy computer users. Despite the fact that the majority of their hypotheses sound appropriate, the hypothesis that students with less computer familiarity were more likely to pirate was opposite of the general beliefs. The researchers reasoned that more experienced computer users would show more respect for the work needed to create software. The connection between the students in post-secondary institutions was used because at that time students typically learned the needed skills in college with their superior network resources, and was also where the pirate mindset tended to set in. The sample population consisted solely of business majors, which were not the majors typically targeted for piracy at the time (Chiang & Assane, 2002, 2007, 2008; Siegfried, 2004). Their results, however, showed some differences compared to the studies conducted by Chiang and Assane (2002, 2007, 2008) and Siegfried. For business students, males still pirated more than females, but students over the age of 24 pirated more than their younger counterparts. The age difference also reflected the notion of more graduate students pirating than undergraduates. Finally, students who were heavier computer users were more likely to pirate than less avid computer users. These results support other research because graduate students could come from backgrounds outside of the business college and may have learned of piracy from their undergraduate program.

Long before music piracy became the primary focus of digital piracy, software piracy had become a problem. Software piracy by the average user began with the desktop computer and Microsoft. When Bill Gates and Paul Allen wrote the programming language, BASIC, for the Altair computer system, computer enthusiasts bought the Altair system for the sole purpose of obtaining BASIC. Furthermore, people began making copies of the software so that others did not need to purchase the poorly-designed Altair to obtain it. Gates was infuriated by these actions because it violated the terms of his deal with the makers of the Altair. He wrote his infamous "An Open Letter to Hobbyists" in which software piracy and the links between piracy and theft were made (Siegfried, 2004; Wallace & Erickson, 1992). Siegfried's study was considered an update to older views of software piracy that may no longer be valid. Prior to Siegfried's work, it was found that students shared roughly the same views on software piracy regardless of computer experience. Income was a driving force, and women were less likely to engage in software piracy than men. Though works by other researchers (Chiang & Assane, 2007, 2008) still supported such claims, one could infer that changes to the digital landscape, such as free versions of popular software programs, would alter download habits. Ultimately, Siegfried concluded that the attitudes showed very little change and supported the overall literature base.

Identifying Ethics, and Motives

Taylor (2004) conducted a study to connect software piracy and ethics between standard business majors and music business majors using a five-point Likert scale questionnaire. Overall, those surveyed agreed with the standard premise that students believe piracy was a faceless crime and hurt few if any. Though music business majors were more likely to view piracy as unethical, when both majors were combined, the results were fairly neutral. Furthermore, students from either major who never pirated music thought that piracy was unethical and hurt the music industry.

Rob and Waldfogel (2006) conducted a study based upon the download habits of students and the value they placed on music they either purchased or illegally downloaded. The goal of this study was not to simply look at downloading habits among students but rather to determine if the students' downloading habits affected album purchasing. The survey asked about whole albums either purchased or downloaded in 2003 along with a list of hit albums from 1999. By having the two lists, Rob and Waldfogel were able to explore a theory that music could be viewed as "(1) an experience good, (2) subject to depreciation as the listeners grow tired of music, or (3) both" (p. 44). Under this theory, students would download or purchase an album, enjoy the album, and grow tired of the album to the point of never listening to it again. The researchers tested this theory in their 2003 survey that was used to investigate students' habits. The list of songs from which to choose contained a list of new music and the top albums of 1999, allowing a distinction between new music a student may instinctively download and older music that students may have tired of previously. The significance of this viewpoint also lends itself to a reason behind student downloading. If a student purchased an album thinking it would be good, only to realize otherwise, that student wasted money on an album. If the student downloaded the same album, the music was simply deleted. Although the purchase scenario resulted in a sale for the record label, it also provided dissatisfaction for the student. The download scenario resulted in no sale for the record label, but the student’s dissatisfaction was mitigated by not wasting money on a sub-par album. At the same time, if an album was generally popular via means such as the Billboard charts they would be more widely available than a less popular or more obscure track (Bhattacharjee, Gopal, Letwachara, & Marsden, 2006a). Rob and Waldfogel concluded that such an analysis tended to become obfuscated when facing individuals who both downloaded and purchased music. These individuals would contribute to a positive trend on both sides and were equally likely to experience the same after-effects of music deprecation. They also noted that their population was not a representative sample so the findings could not be generalized to the entire student population. Furthermore, it was noted that students do not want to waste money on a bad album, or an album that features only one or two good songs. Thus, downloading becomes more of a “try before you buy” scenario acting more on utilitarian methodologies to maximize the individual’s happiness. Even with the justification of trying to save money, deontological and virtue ethics still support that the act is immoral (Edgar, 2003; Johnson, 1994).

Jung (2009) researched student ethics not only from the perspective of software piracy but also from privacy violations and plagiarism viewpoints. Using a predominantly female population of Tokyo college students, Jung looked for differences in the ethical responses among three scenarios. Both the software piracy and plagiarism scenarios yielded a perception that both were relatively harmless. The scenario that involved a privacy violation, where one person acts in a way that may incriminate another, was less likely to occur compared to piracy and plagiarism. Based on these results, it was concluded that more anti-piracy and anti-plagiarism measures needed to be taken and ethical measures needed to be further emphasized.

A study by Gupta et al. (2004) explored student software piracy along with ethical considerations related to the issue. Based upon some of their research, it was viewed that piracy, while immoral, has a lesser severity and level of harm than did other, more heinous acts such as breaking into a store and stealing a physical good. Their study aimed to connect the perception of software piracy with a student's habits in terms of ethics, legality, criminality, parties harmed, and social impact. Those surveyed were 90% male, about half were under the age of 25, and the majority of the respondents were college educated. It was found that persons less concerned over ethics were more likely to pirate software. Furthermore, the social landscape of websites that encourage software piracy further strengthened the belief that piracy was acceptable. In fact, the researchers noted the strong correlation between the belief and their survey question that mentioned the ease of pirating because a person could not get caught. The legal aspect, however, did not correlate with the social one. The researchers did mention that while this result was contrary to the norm, the study had taken a more ethical focus which could have resulted in skewed results. Also, limitations such as a non-random sample and the aforementioned gender skew hindered representation. In their conclusions, the authors addressed difficulties that arise in convincing those who already pirate software to no longer do so. They also expressed their belief that from a policy perspective piracy is a paradox, because the government cannot accept piracy as legal even though piracy has beneficial side effects in some cases. Similar to Rob and Waldfogel's (2006) implications, a free demo of music would allow a potential customer to determine if an album is worth purchasing. Gupta et al. (2004) suggested that software companies put more emphasis into trial and beta versions of commercial software. Hence, free samples appear to be one outlet to help curb digital piracy. Finally, the authors have stated their beliefs that the public will not view software piracy as an ethical concern. This would indicate that there may be a need to teach ethics as early in life as possible. In a later study, Coyle, Gould, Gupta, and Gupta (2009) reconfirmed this viewpoint while taking into consideration other factors such as the legal aspect and past/present/future factors. They found, in support of earlier researchers, that ethical and legal aspects were predictive of past and future intentions.

Matching to Psychological Models

Logsdon et al. (1994) took one of the first looks into the connections between software piracy and morality. The authors based their moral theory on Kholberg's (1969) six stages of moral development which comprise three levels of moral development--preconventional, conventional, and postconventional--each with two stages. People progress forward through the six stages over time, and can only base decisions on two adjacent stages at any time. The researchers also utilized Rest's (1986) Defining Issues Test as a valid and reliable framework to measure morality on Kholberg's model. The sample used in this study, consisted of 363 valid respondents from a Southwest university in business and engineering fields. Using Likert scale responses, the authors planned on connecting results from the Defining Issues Test with responses related to a student's tendency to pirate software. According to the survey, the majority of students tended towards a participatory attitude in regard to pirating software. When these data were correlated with the results of the Defining Issues Test, a weak to nonexistent correlation arose. Looking at the morality component separately, most of the responses reflected a feeling that software piracy caused little harm and that there was a weak association to the software companies. Thus, though students may have possessed strong moral values, they did not necessarily treat software piracy as an immoral act. This early study emphasized a need to educate students that copying software is the equivalent of stealing a physical object. That same need has been repeatedly reinforced in more recent studies (Cheng, Shang, & Lin, 2008; Goles et al. 2008; Kini, Rominger, & Vijayaraman, 2000; Simpson, Banerjee, & Simpson Jr., 1994).

LaRose et al. (2005) explored the concept of piracy through means such as Social Cognitive Theory (Bandura, 1986) and expected outcomes, alternatives, and potentially more useful, reasonings behind pirating. One predicted outcome was downloading becoming habitual and repetitive to the point where the student no longer thought about the act. LaRose et al. also argued against studies focused on ethics and morality because they only focused on the self-regulation and judgmental processes. Such a focus could backfire and further encourage piracy through beliefs of "lax norms for conduct, such as the perception that 'everyone is doing it' or that media conglomerates are undeserving of sympathy, as these perceptions lend an aura of social acceptability" (LaRose et al., p. 5). The survey involved 265 students from an introductory communication course in a Midwestern university. The respondents were predominantly white males, and 82% were considered active downloaders with mp3 collections ranging up to 30, 000 songs with a median collection of 200. The goal of the study was to find trends between piracy and expected outcomes, self-efficacy, lack of self-regulation, and moral values. Based on the results of the study, the social component of file sharing and the habitual nature of downloading were determined to be important factors in a student's propensity to download. This also matched the results found by Higgins (2005). LaRose et al. also found that moral acceptability acted as a negative predictor to file sharing. Through these results, it was found that students under the classification of heavy file sharing met both musical and social needs which overshadowed the legal discouragement and placed a new perspective on piracy where the act was not so much committed as a crime but rather as a way of fulfilling a social need. Since the study took place in late 2003 after the RIAA began its legal campaign, there was some question as to how much the campaign would influence downloaders. The study revealed that only seven students, five light downloaders and two heavy downloaders including the individual with over 30, 000 songs, would consider stopping. Fear from lawsuits did little to affect the heavy downloaders, but university sanctions were determined to pose more of a threat.

Sinha and Mandel (2008) further supported LaRose et al.'s (2005) viewpoint by determining that (a) increasing the risk of getting caught would do little to change how much a student would be willing to pay for music; (b) that risk takers may actually pirate more in an increased risk scenario; and (c) cheaper, downloadable alternatives were more effective in decreasing the willingness to pirate. The study by Coyle et al. (2009) also supported these results. In its entirety, the LaRose et al. study added a refreshed viewpoint on the topic of student software piracy and could be helpful in arriving at a better solution to the problem. Kuo and Hsu (2001) conducted a study based on Social Cognitive Theory and an ethical computer self-efficacy component. Conducting the study on 209 college students, the researchers concluded that their model could link into other parts of the social cognitive theory model such as self-esteem, and self-image.

Taylor, Ishida, and Wallace (2009), experimented with Social Cognitive Theory and instead developed a modified version of Perugini and Bagozzi's (2001) Model of Goal-directed Behavior. Their results showed that the modified model contained the robustness to explain why someone would or would not engage in digital piracy for both movies and music. The modified model, however, was new and would require further testing to ensure that the model was truly generalizable beyond the study population.

Cronan and Al-Rafee (2008), utilized Ajzen's (1991, 2002) Theory of Planned Behavior which is "one of the most influential and popular conceptual frameworks for the study of human action" (Ajzen, 2002, p. 665). Based on a modified model used by Dubinsky and Loken (1989) and Randal and Gibson (1991), the instrument used was designed to predict past behavior measuring attitude, subjective norms, perceived behavioral control, past piracy behavior, and moral obligation. Past piracy behavior showed the strongest influence followed by moral obligation and perceived behavioral control. Based on the results, the researchers determined that software security mechanisms would be breached eventually and that ethics may yield better results. These results were consistent with the beliefs of modern organizations (Common Solutions Group, 2008; EFF, 2008).

Douglas, Cronan, and Behel (2007) explored equity theory as a possible deterrent to software piracy. They hypothesized that if all sides believed that they were treated in an equitable and fair manner they would be satisfied. Inequality examples included legitimate consumers experiencing dissatisfaction with software DRM that punishes the legal user more than the pirate that gets around it, and the software companies' perception of lost profit from piracy. In this study of college students, equity was found to be an important factor in software piracy and it was recommended that companies should look into alternatives to current deterrent methods to provide a more equitable solution. For the music industry, finding equity and gaining trust would be quite beneficial (Ouellet, 2007).

Hinduja (2008) suggested that deindividuation theory could lead to an all-encompassing explanation of why students pirate. As the name implies, deindividuation theory states that:

> An individual can feel extricated from responsibility for his or her actions simply because that person no longer has an acute awareness of the identity of self and others (individual and corporate entities) and of the social environment that provides the context for the behavior. (Hinduja, p. 392)

Considering that the Internet allows for increasingly anonymous interactions, one could easily become absorbed and lose his or her sense of self as a user and thus become another unknown in cyberspace. Hinduja believed that this anonymity and feeling of being hidden within the Internet acts as a catalyst towards piracy and other malicious behavior. Using a sample of 433 students from a large Midwestern university in the Summer 2000 semester, the researcher surveyed students to determine any link between anonymity, pseudonymity, and the propensity to pirate software. Based upon the results, the majority of the respondents were white males with little value towards either anonymity or pseudonymity. Thus, no significant differences were found between anonymity and intent to pirate. Hinduja, however, thought that the insignificance did make sense in the long term because someone who is prone to pirating will still do so. The one major problem with this research was the sample set. The Summer semester is typically the semester of lowest enrollment of the academic year. Taking the sample in 2000 meant that other factors such as the RIAA's crackdown had not yet come into effect (EFF, 2008). If this survey were to be repeated with those factors in place, there is a chance that anonymity and privacy would play a more important role than during the time of Napster's operation.

Taking an entirely different approach, Wagner and Sanders (2001) used religion as a factor for ethical behavior and more importantly software piracy. With a useable sample of 167 undergraduates at a large institution, Wagner and Sanders used single-item measures for religious variables and compounded measures for ethical behaviors. With the exception of a piracy at home/work scenario, it was found that a connection between ethics and religion exists. Considering that religion is a major source of ethics knowledge (Edgar, 2003), these results make sense.

Criminology and Self-Control

From a criminology perspective, Higgins (2005) conducted a study that aimed to determine if a link between piracy and self-control existed. According to self-control theory, the less self-control persons have, the more likely they will commit some form of crime. These people would not require any reason to commit their act beyond self-interest and share the following traits: "impulsiveness and insensitivity; an attraction to easy and simple tasks, risks, and physical activities; and little long-term planning" (Higgins, 2005, p. 3). Higgins (2005) indicated that the low self-control in software pirates could stem from those who refuse to wait to purchase an album or software, or just impulsively do so. The study involved a self-reported questionnaire taken by 318 validated respondents in an Eastern university during the Fall 2003 semester. Four courses were used in this study, two from a general education course that all students could access, and two from Justice Administration courses. Unlike other studies discussed in this section (Chiang & Assane, 2002, 2007, 2008; Gopal et al. 2004; Gupta et al. 2004; Logsdon et al. 1994; Rob & Waldfogel, 2006; Siegfried, 2004; Sims et al. 1996), the sample contained a predominantly female population as opposed to a male-dominated one. To obtain a ranking on software piracy, Higgins (2005) used a five-point Likert scale to rate how likely a student would be to pirate software under a given situation along with ethical considerations. A four-point Likert scale was used to obtain other piracy-related data and the self-control information. Higgins (2005) also factored in the effect of peers on software pirating for the survey. A follow-up study by Higgins (2007) sought to combine self-control theory with Ajzen's (1991) theory of planned behavior. Self-control was found to be an important predictor, but motivation played a stronger role. It also found that low-self control did correlate with motivation.

Another follow-up study by Higgins, Wolfe, & Marcum (2008) further solidified the importance of self-control theory as a link with digital piracy. Because digital piracy may be viewed as a social activity, considering such a factor makes sense and is supported in the literature reviewed (Gupta et al. 2004). The results of the study uncovered the pirating peers variable as a confounding factor that interfered with the results for the self-control variable. It was also discovered that ethics did play an important factor in the intent to pirate. However, considering that the sample contained mostly females who are known to be less likely to pirate and be more concerned about the penalties (Chiang & Assane, 2007, 2008; LaRose et al. 2005; Siegfried, 2004), such results cannot apply to the entire nation. In contrast, Limayem, Khalifa, and Chin (2004) found that ethics alone did not play a large role in the intent to pirate and that monitoring software was still needed. Though this conclusion supported the need for ethics, it was more closely aligned to the conclusions reached by the Common Solutions Group (2008).

Higgins, Fell, and Wilson (2006, 2007) expanded on Higgins's (2005) work by further exploring self-control and possible connections to social learning theory. Social learning theory is concerned with an individual's association with groups that exhibit deviant behavior. It is theorized that the individual would learn the group's deviant behavior and become more likely to participate in criminal activities. Based upon the social connections found by Higgins (2005) and LaRose et al. (2005), social learning theory could further expand the understanding of digital piracy and group behavior. The sample for this study was constructed similarly to Higgins's (2005) prior study using four classes open to all students and three classes for only Justice Administration majors during the Fall 2004 semester. This resulted in a total sample size of 392 students. Measures for piracy intentions and self-control were constructed similar to the 2004 study. The social learning component used a composite of six questions. The authors took the survey data and created four models to determine which connection worked best. The first model simply showed the goodness of fit for the variable. The second model demonstrated that low self-control does indeed link to social learning theory which then links to digital piracy. The third model showed that both low self-control and social learning theory connected to piracy independent of one another, and the fourth model showed that an interaction effect between low self-control and social learning theory was present. When comparing the models, the second model demonstrating that low self-control does indeed link to social learning theory which then links to digital piracy, proved to be the most significant. It was thought to have the potential to further aid university administrators in developing appropriate policies to handle digital piracy on campus.

Qualitative Studies

A qualitative study by Einav (2008) helped further support the study from LaRose et al. (2005) and Coyle et al. (2009) by exploring why the students share video media. As one of the few qualitative studies, Einav's work provided further, more intricate details than the quantitative studies. Students were found to share video files mainly for convenience and immediacy, being able to view the programs when they wanted without having to wait for a pre-determined time. For the movie perspective, downloading for quality control and overall content were equally important. Some students wanted to know if a particular film was worth their money. If they liked the film, they were willing to pay for the better theater quality version, and save money by not paying to see a horrible film. Surprisingly, cost was the least likely reason to share video files. This is contrary to many of the findings for music and software piracy (Chiang & Assane, 2002, 2007, 2008; Gopal et al., 2004; Gupta et al., 2004; Higgins, 2005; Higgins, Fell, & Wilson, 2006; Logsdon et al., 1994; Rob & Waldfogel, 2006; Siegfried, 2005; Sims et al., 1996). From the ethical standpoint, the students considered:

> big media companies as money making conglomerates, full of executive earning six figure salaries, who are making a hefty profit as is. They also believe that when they pay, their money doesn't channel directly to the artists but to the managers and offices that want to increase their profit. (Einav, p. 155)

Along with misconception that television is free, this adds a component that follows the economic modeling of artists making more money from their concerts than from album sales in contrast to the recording industry's profiting from album sales (Gayer & Shy, 2006; Liebowitz, 2004). Blythe and Wright (2008) conducted their own study that supported the findings of Einav. Although this study included subjects who were not students, the results showed little difference. Furthermore, though some respondents acknowledged the fact that they were stealing music, they believed it was faceless and not really stealing because copies were created and nothing was ever taken. Some respondents were critical of the recording industry as a moneymaking conglomerate that created nothing but manufactured pop and artists who had already found fame and fortune. Blythe and Wright use the responses to suggest an alternative to litigation, failed scare tactics, and labeling copying as piracy. By increasing the enchantment factor and making music an even more enjoyable experience, the industry could find profit in alternatives to selling recorded media. Such findings would agree with Gayer and Shy's (2006) alternative sales theory conclusions. Such conclusions could potentially mean that students are more in tune with the industries than companies may believe and that their support is more for the artist who provides the source of entertainment than the record label, movie studio, or software/video game publisher and possibly through means other than sales of songs.

At the same time, the student responses from qualitative studies (Blythe & Wright, 2008; Einav, 2008) could also be interpreted as responses akin to Sykes and Matza's (1957) neutralization theory. Neutralization theory is a behavioral concept in which people find a way to rationalize or neutralize their actions to escape blame or make an illegal act seem moral. Sykes and Matza describe five situations: (a) denial of responsibility where the act is neutralized to an outright denial or not being in full control; (b) denial of injury where the act is downplayed to something more moral, i.e., stealing becomes borrowing; (c) denial of the victim, similar to denial of responsibility, focuses on people rather than property, and the victim is typically portrayed as deserving of the act; (d) condemnation of the condemners where a person shifts blame to a group that tries to control the act; a person caught for digital piracy may refocuses attention to the RIAA and "unethical ways;" (e) Finally, appealing to higher loyalties is exemplified when people put loyalties to smaller groups ahead of those of the state, or nation. Ingram and Hinduja (2008) found that neutralization theory created a strong framework for analyzing piracy among college students. These researchers also agreed with the many claims of piracy being faceless and ethical (Blythe & Wright; Einav; Huang, 2005).

Digital Rights Management: A Problematic Solution

Now knowing what motivates students to pirate, the next step is to determine what will serve as deterrents to piracy. One of the most common practices to prevent copyright infringement on digital media has been utilizing some form of Digital Rights Management (DRM). From a general perspective, DRM is a piece of code in a file or software that places restrictions on what the user may do with the file as defined by the copyright holder. In software, DRM could (a) require having the original disc in the computer while using a program, (b) prevent a disc from being copied, or (c) limit the number of installations the user may perform (Waterman, Ji, & Rochet, 2007). If DRM that prevents copying is properly executed, it would encourage more people to purchase the legal version (Chiu, Hsieh, & Wang, 2008). Within the realm of digital music, DRM may anchor a file to a music service such as iTunes so that it could not be played outside of the scope of the services (Jaisingh, 2007; Rupp & Estier, 2003).

Einhorn and Rosenblat (2005) took a deeper look into DRM and the concept of versioning. Similar to seeing a movie in multiple formats, versioning allows the copyright holder to provide the same file with differing rights at prices that reflect what is allowed. Thus, a song that only allows the user to play it on a proprietary program may cost less than the same song that also allows the user to burn it to a CD. The researchers discussed various combinations and their effectiveness. For example, Apple's FairPlay DRM system has allowed for unlimited CD burning, compatibility with the iTunes software, and transfer of songs to up to three hard drives. The revamped Napster provides commercial-free streaming radio with unlimited downloads service. This provides users with an alternative way to listen to music. Penn State used DRM to its advantage when it struck a deal with the new Napster and opened an account that allowed all students unlimited mp3 downloads while they were students at the institution. When students left, they paid for the tracks they wished to keep (Jochaim, 2004). This provided the best balance of both legal downloading and having a whole library at a student's fingertips for free.

Another important component to DRM that Einhorn and Rosenblat (2005) discussed was interoperability between different programs. In some cases, a DRM scheme will be compatible with one program but not another. For example, consider a file that will only play on Microsoft's Windows Media Player but not Apple's iTunes due to DRM restrictions. To the student, this would mean having to use two different media player programs for an album. Furthermore, that student will not be able to play the album on an iPod. This situation could become problematic if approached incorrectly (Jaisingh, 2007). If a university were to invest in a download service that contained too many restrictions, or were to restrict usage on the most popular means of listening to music, a student might refuse to use the service and pirate a DRM-free version of the song. Since 2007, Apple's iTunes service provides DRM-free songs at a higher price than their DRM tracks as a result of consumers' dislike for DRM. As Lincoff (2008) revealed, however, the DRM-free songs that come from EMI, one of the four major recording labels, actually contains a subtle DRM that watermarks the file with information tying back to the purchaser of the file. If one of these "DRM-free" songs was discovered by EMI on a torrent site, the label easily uses the DRM information to find the original owner. Lincoff, however, has not perceived watermarks as a threat because "Eventually, the means by which to delete personally identifying information from these music files will be publically available on the Internet; as will the EMI recordings themselves, truly free of DRM" (Lincoff, p. 15). In essence, according to Kierkegaard (2006), all DRM contains some form of restriction, and there will always be someone to find a way around it. Thus, either finding the right balance of DRM that protects the copyright owner but does not punish the legitimate user, or exploring another method of licensing and distribution becomes paramount to finding a universal solution. Otherwise, the digital landscape may become littered with the remains of various DRM songs from defunct music services.

Further negative press for DRM came from the type of DRM used by Sony Corporation to protect its albums in 2005. Prior to 2005, Sony implemented a technology known as MediaMax which restricted the number of copies a user could make of a CD. Unfortunately, whenever users placed a CD with the technology into their computers, the software automatically loaded onto their machines before they could accept the End-User License Agreement and would remain on the hard drive indefinitely. It also collected personal data despite the agreement stating otherwise. These software problems were unknown until J. Alex Halderman, a Princeton doctoral student, discovered them and published a paper about them. The findings devastated MediaMax's parent company, SunComm and forced Sony to start over (LaBelle, 2006).

In 2005, Sony implemented a program known as XCP which worked similarly to MediaMax, but the End-User License Agreement only appeared the first time a user inserted a CD with the technology in a computer. The next CD with XCP technology would not generate the agreement. This was problematic if the user neglected to read the agreement initially. Though the software worked in a stricter manner than MediaMax, it still collected user information contrary to the agreement and also installed a rootkit onto the computer. Rootkits are pieces of software that operating systems and anti-virus software cannot detect and are typically used as a backdoor for viruses, trojan horses, and other malicious code. When computer security analyst, Mark Russinovich, discovered the rootkit on his computer and traced it to a CD with XCP, Sony ran into major trouble. Not only did Russinovich discover the rootkit, but he soon learned that trying to removing it further compromised the system. The situation was further heightened by a virus that exploited the rootkit in November of 2005, and the public became displeased. Although Sony initially denied the severity of the rootkit, customers demanded removal of both MediaMax and XCP. Unfortunately, the patch to remove the programs only further compromised users' machines. On November 1, 2005 class action suits against Sony and the manufacturers of both MediaMax and XCP were filed and eventually settled on December 28, 2005 (LaBelle, 2006). One method to overcome piracy is to forge trust between the customer and the company (Oullet, 2007). Sony, by its actions, did just the opposite and if anything further galvanized the public's dislike of DRM.

The Influence of the Recording Industry

Since 2003, the Recording Industry Association of America (RIAA) litigiously pursued people who shared an excessive number of files with the intent of scaring other file sharers into compliance. The Electronic Frontier Foundation (2008) released a white paper focusing on RIAA actions over the first five years of the litigation campaign. In 2003, RIAA began filing subpoenas through clauses in the Digital Millennium Copyright Act (DMCA). Eventually, in January 2004, the organization started filing actual lawsuits known as the “John Doe” cases. These cases were named as such because the offenders could only be identified by their Internet Protocol (IP) address. Compliance from the offender’s Internet service provider (ISP) was required to provide real information. Throughout the course of litigation, the EFF reported that roughly 30,000 lawsuits were filed between January 21, 2004 and October 2007. The amount of money obtained by the recording industry varied from $3,000 settlements to judgments of approximately $40,000. In one of the first cases with a trial by jury, Jammie Thomas-Rasset lost her case. This resulted in damages of $222,000 . She then decided to go through a retrial based on the grounds that the jury had been misinformed by the judge. The retrial concluded with the same judgment, but with a verdict of $1.92 million--a far worse outcome (Karnowski, 2009).

In 2009, the second RIAA case with a trial by jury involving Joel Tenenbaum, a Ph.D. student at Boston University. Tenenbaum’s case was hyped by having Harvard Law Professor Charles Nesson as his attorney. Nesson’s original fair use defense was thrown out for being too broad which left him and Tenenbaum on the losing side of an uphill battle (Anderson, 2009a). When Tenenbaum took the stand, he admitted to using P2P, downloading and seeding songs, and initially lying during the discovery process. Ultimately, the court handed Tenenbaum a guilty verdict, and the determination of the size of the fine fell to the jury for a decision. Guidelines for fines distinguished between types of infringement. For cases where copyright infringement was considered as unwilling, i.e., people who did not realize they were infringing, the jury was able to award damages from $750 to $30,000 per song. If the defendant was willing, the maximum amount increased to $150,000 per song. In the Tenenbaum case, the jury awarded damages totaling $675,000, or $22,500 per song for 30 songs that were willfully infringed. Considering the potential maximum award of $4.5 million, Tenenbaum was fortunate. Given his online habits, the trial was conducted in the presence of a rather sympathetic jury.

> . . .Tenenbaum had used a variety of different peer-to-peer programs, from Napster to KaZaA to AudioGalaxy to iMesh, to obtain music for free, starting in 1999. And he continued to infringe, even after his father warned him in 2002 that he would get sued, even after he received a harshly-worded letter from the plaintiffs' law firm in 2005, even after he was sued in 2007, and all the way through part of 2008. (Sheffner, 2009a)

Considering that Tenenbaum continued pirating until the legal system forced him to stop implies that threats will not deter all students. One of the original missions of a post-secondary institution has involved creating graduates of moral character. If students follow a similar thought pattern to that of Tenenbaum, the universities may be failing to meet this significant section of their mission. This lack of ethics also supports the conclusions drawn by the Common Solutions Group (2008).

Despite the outcome, Nesson still looked to challenge the copyright law. At the time of the present study, he wished to challenge the issue of fairness and the constitutionality of the large range of awardable damages in the digital age. He has expressed the belief that such a penalty works for corporations but is too strict for the average person. Unfortunately, some of the abnormal tactics that Nesson attempted in Tenenbaum's trial caused others to question his motives. Due to the hardships faced in the first trial, Tenenbaum's appeal may be a more difficult task to achieve. In the worst case, however, Tenenbaum could declare bankruptcy to avoid paying the $675,000 (Anderson, 2009b).

Though these two lawsuits at first glance would seemingly be sufficient to deter a file sharer, the EFF (2008) has stated that the majority of cases, where all except Joel Tenenbaum and Jammie Thomas-Rasset were tried without a jury, were successfully defended against on grounds of merit. With such results, the RIAA was losing standing on the issue and needed to change tactics once again. In February of 2007, the recording industry decided to target ISPs and force them to deal with the offending individuals. Hence, major ISPs and more importantly, universities, were required to monitor usage of their users. Institutions such as Stanford have also indicated that disciplinary action will be pursued in addition to the fees the RIAA requests. At the present time, students were able to go to the website http://www.P2Plawsuits.com to pay a reduced, fixed settlement fee instead of fighting the settlement in court.

Lincoff (2008), in his research, indicated that the recording industry has done damage to itself by engaging in litigation and overall P2P crackdown. Though “the ratio of illegal to legal song downloads was 40:1, and 20 billion recordings were downloaded that year without authorization” (Lincoff, p. 5), Lincoff has attributed the RIAA problem to reliance on a business model not suited for digital goods. The public has viewed music as a free good considering any person may listen to music while in a car, at the store, or at an event. Music has been characterized differently compared to other cultural content. Because of this, most of the effort the RIAA has taken to stop P2P distribution has resulted in a backlash and a slowed growth. Lincoff discussed what he considers to be the addiction of major labels to the sales-based revenue model, but also has noted that current copyright laws would prevent any change from occurring. Easley (2005) similarly discussed an industry’s use of a “monopoly” on a product to charge indiscriminately and often more than the product was worth in order to recoup production costs. Weakening copyright laws endanger intellectual property and permit piracy to operate legally, but strengthening copyright laws too much discourage new work because of infringement fears. Thus, an amicable medium needs to be determined in order to compensate for the complications which have arisen due to the digital age.

One solution matches the views of the Electronic Frontier Foundation (2008) and involves a right to digital transmission that would require a license fee for every transmission regardless of type (download, stream, etc.). Also, the license fees would only apply to digital services, so consumers would pay only the standard Internet fees and the fees to use a particular music service. If consumers wished to transmit the file to another party, however, they would be subject to the license fee unless the site to which they wished to upload had already paid. Though the darknets for illegal activity may always exist, there would be less protest against any litigation against said networks if licenses were easily available and affordable (Lincoff, 2008). If such a system were implemented, post-secondary institutions could easily strike deals with services that would allow unlimited downloads. Unlike the Penn State arrangement with Napster (Joachim, 2004; Spanier, 2004), students would have no need to pay for songs before leaving the institution because the service would have previously paid the fee.

Finding Profit Despite Piracy

Despite the negative effects brought about by piracy, one must also consider the potential for economic benefit in a different legitimate sector. In a study by Hui and Png (2003), the question of music piracy causing an increase in the purchase of CD players was raised. They believed that though piracy caused a significant economic effect based upon reported numbers by the industry. In their opinion, the figures were likely to be skewed when accounting for a scenario where all pirated copies were nonexistent and the legitimate version must be purchased. For some cases, the user only used a software program or album because a pirated version was available. Furthermore, a reported loss of sales by an industry was skewed because a proportion of the lost sales would never result in sales and would lead to clearly overstated figures. Based on the proposed question, piracy could boost sales of related products such as CD players for pirated music CDs or mp3 players for digital downloads. Hui and Png also associated piracy rates to price drops. If people know that a product may decrease in price, they will delay purchase and in some cases pirate the media in the interim. Thus, while piracy remains a criminal activity, price points may also affect whether the consumer plans on purchasing or pirating. Sundarajan (2004) noted pricing music becomes more difficult when DRM is considered. Lowering the overall price would help compensate for the DRM restrictions but may also alienate customers if the DRM is too restrictive.

Hui and Png's (2003) explored music CD and CD player sales in 28 countries throughout the world with varying piracy rates between the years of 1994 and 1998. Considering that the range of data collection includes the time period prior to the appearance of Napster, pirated CDs may have originated from older download sources or simple CD copying. The correlation between pirated CDs and CD player ownership, however, did not prove significant and ruled out Hui and Png's hypothesis. Because the time range did not factor in Napster or the introduction of broadband Internet, the authors suggested that this type of study be replicated at a future time with more current data.

Takeyama (1997) also considered the piracy loss figures from software associations to be inflated. Takeyama's hypothesis was contrary to the belief that piracy hurts the profits of software companies. He believed that under the right conditions piracy may help increase profits. Takeyama split the population into high and low demand customers. Under the traditional model, companies would need to reduce their prices over time in order to compensate for piracy, which would drop at a faster rate compared to a non-pirated product. This would also result in a drop in inventory surplus to compensate for the lack of purchases. Under the high and low demand model, a company would be focused on selling the product to only high-demand customers without making any changes in prices. Although low-demand customers would likely resort to piracy to obtain the program, it would be recognized that they were never part of the original demand. Since the company would maintain the original price, no extra demand at a lower price would be created and the company could then make a profit in spite of the pirates (Bhattacharjee et al. 2006b).

Gopal and Sanders (2000) also supported this concept by their focus on price as a national or regional issue rather than a concern of individual industries. At the present time, software companies were charging different prices to different industries under contractual agreement. For education, colleges and universities have been able to sell software at a cheaper price as a result of this practice. If companies adjust prices to fit a given area's economy, more people could be inclined to purchase the legitimate version rather than to obtain the pirated one. Furthermore, the low-demand bracket could even be given the opportunity to download free abridged versions of programs designed to fit their needs. A notable example of this method includes Adobe Acrobat Reader, an abridged version of Adobe Acrobat that allows the user to view files created with the Acrobat software without having to pay for it (Gopal, Bhattacharjee, & Sanders, 2006; Liebowitz & Watt, 2006; Peitz & Waelbroeck, 2006). The only disadvantage to any of these suggestions is that, on average, the music industry has been able to recover costs on about 10% of all artists. Such a model also explains why the record companies have been so adamant about anti-piracy (Leyshon, Webb, French, Thrift, Cewe, 2005). Although the concept of piracy has continued to be considered immoral, implementing the aforementioned business model would help alleviate the claim that the software industry loses money because of piracy. Because the music industry produces cheaper products than the software industry, this model may not be effective. At the same time, equilibrium must be found between punishing the copiers and supporting the companies. Otherwise, a risk of piracy spilling over from the low-demand to the high-demand side may surface (Banerjee, Banerjee, & Raychadudhuri, 2008; Chang, Lin, & Wu, 2008; Wu & Chen, 2008).

Since Napster's creation, the music industry continually views mp3s and illegal downloading as the blame for decreasing record sales. The decrease in sales, however, could stem from other reasons that began before Napster's creation. The rate of music singles per capita experienced a downward trend beginning in 1973, recovered slightly in 1989, and remained relatively steady until another decline began in 1998. The 1989 recovery came from the printing of CD-based singles which only stalled the decline for nine years. In terms of sales, the music industry has always shown atypical trends when media formats change. Originally, consumers would own a combination of 8-tracks and vinyl records due to portability reasons, but when the cassette offered better portability, consumers transitioned to the new format. Once again, when CDs became the new media of choice, consumers switched formats causing another spike in sales (Liebowitz, 2004). Liebowitz also stated that the average person will take about five years to convert their libraries from one format to another, but this phenomenon was only apparent during the cassette to CD transition. Looking at other factors that could contribute to the decline in sales, other industries such as movies and videogames insignificantly correlated, and blank cassettes made little impact during the cassette era. One may venture to guess that modern music does not hold the same interest as older material. In contrast, however, concert sales showed large increases in 2000 and 2001. Such a phenomenon may support Hui and Png's (2003) claims about piracy indirectly helping another industry. If a student were to illegally download an album and enjoyed the music, that student could potentially attend that artist's concert and pay for the music live and in person. Liebowitz (2004) also discovered that age demographic of music purchasers between 1995 and 2001 began to flatten with a decrease in younger groups and an increase in older groups. Though Napster's presence may be the first to take blame, the decrease first occurred between 1995 and 1998. Mp3s definitely made an impact in the sales decrease, but Liebowitz (2004) implied that they may have served as a catalyst in this situation.

Zentner (2008) further explored these implications for piracy and profit by conducting a study between 1998 and 2002 of music specialty stores. The goal was to see if both legal and illegal online downloads affected the number of music stores. It was found that the introduction of broadband Internet, along with the presence of a university, affected the survival rates of music stores. However, during this period of time, more music stores were created than closed. Such findings reinforce Liebowitz' (2004) position that though digital goods are transitioning in, physical media has not disappeared entirely.

To further explore the connection between copying and increased concert sales noted by Liebowitz (2004), Gayer and Shy (2006) conducted their own analysis on the connection. In their analysis, they examined different conditions that could cause either individual artists or the publishers (RIAA) to consider legal action. By intentionally disconnecting the artist and publisher profits, the researchers hoped to show that piracy generated an increased interest in the artist leading to increased concert sales that assisted the artist. According to Dejean (2009), however, the result was a decrease in record sales which hurt the publishers. Through economic models, Gayer and Shy did prove such an occurrence. In situations where piracy existed, the artist profited more from concerts than did the publishers from album sales. Logically, this makes sense because the publisher's monopoly on the album is challenged by the illegal downloads but the artist receives enhanced exposure. In situations where piracy has been non-existent, the opposite is true. Publishers make more money from album sales, but fans of the artist will not keep pace with the pirate model. The only flaw with the author's model is that side effects or artist viewpoints on having their material pirated have not been considered. Regardless, the conclusions drawn by Gayer and Shy, Liebowitz (2004), and Hui and Png (2003) provide evidence that piracy, while technically illegal, may create some good in a related field. Ouellet (2007) provided further support by discovering that song experience also factors into the decision of piracy. If a record company provides a better and more trustworthy first album of an artist, the public may reciprocate that trust and purchase legally. Furthermore, a poor product will always yield more loss to piracy than one of a better quality (Chellappa & Shivendu, 2005).

Duchêne and Waelbroeck (2006) showed that independent artists could also find success if they provided tracks for free. Free download could lead to a successful album by downloading, listening, enjoying, and purchasing. This concurs with the viewpoint of Hilton (2006), who supported the general good by noting a 2005 presentation from Lawrence Lessig, founding member of the Creative Commons licensing scheme and board member of the EFF. Lessig demonstrated how "remixing" works where multiple copies of previous works could come together to create an entirely new and original piece. These conclusions support those who view the RIAA as a greedy conglomerate that could care less about the artist, and they provide artists alternative routes to profit from their work. This would not, however, solve any issues involving software piracy.

Bakker (2004) explored the economic issue by comparing both legal and illegal download services. Though P2P networks are widely used for file sharing, they may not offer the same features as a legal download service such as iTunes. It was found that the amount of content offered on P2P programs such as Gnutella or Kazaa could range between 500 and 900 million files compared to iTune's 400,000 songs at the time of the study. The legal route is obviously more expensive to users but guarantees the proper file, album art, and other perks. Despite the P2P networks' vast file database, users need to sift through the results to find the appropriate song as not all of the files are music and there is bound to be mislabeled material. To the advantage of P2P, it allows live streaming of audio which permits audio to download to users' computers in real time making their media player similar to a radio station. These side features will be what marks the difference between success and failure for the future of online services.

Policies of the Higher Education Act

With the RIAA's change in tactics to let ISPs handle informing and identifying infringers, postsecondary institutions have become the recipients of the brunt of the work. Due to lack of funds and exceptional network resources at most colleges and universities, college students have become the largest group of file sharers and copyright infringers (Chiang & Assane, 2007). Thus, when the RIAA decided to switch its focus in 2007, the majority of the attention went to universities in order to target the largest percentage of the population (EFF, 2008). Some institutions, such as the University of Florida, initiated their crackdown on student copyright infringement prior to the shift in focus. The University of Florida developed their own software to detect usage of P2P across the campus network known as Integrated Computer Application for Recognizing User Services (ICARUS). Though the software has been successful in decreasing the usage of P2P networks, students are unhappy with the outcome. This is especially true since institutions such as Pennsylvania State University found more creative means by forming a deal with the reformed Napster to provide free downloads to students as long as they remain enrolled as students (Joachim, 2004). Chiang and Asane (2007) discovered that by giving students more favorable alternatives, they were less likely to pirate. This could result in a less invasive way to counteract piracy if properly executed.

Penn State's arrangement with Naptster in 2003 allowed all students access to Napster's premium services such as audio streaming and unlimited free downloads while they were students. In order for students to take their music off their computer, however, an additional fee must be paid to burn a CD or put music on an mp3 player. Although the university has offered a legal incentive to the students, Penn State still employs the three strikes rule seen in many other institutions (Easly, 2005; Spanier, 2004). Spanier also noted that in other institutions the student senate voted to implement P2P blocks upon the realization that illegal file sharing placed major strain on the campus networks. Other institutions implemented bandwidth caps and a detection software known as CopySense to prevent P2P traffic before it begins.

When the RIAA did switch its focus, there was also a push to force postsecondary institutions to implement some form of copyright infringement prevention via the 2008 update of the Higher Education Act (EFF, 2008; Liebowitz, 2008). This legislation required universities to utilize some method of preventing copyright infringement by presenting the policies on at least an annual basis (Higher Education Act of 2008, §487). Although such a policy may be viewed as excessive or expensive by smaller institutions, it could also lead to some more focus on student ethics. For example, the University of Central Florida (2009) has a three-strike P2P policy. All three strikes involve halting the offender's Internet access. The first strike gives the student a simple written warning with no disciplinary action. The second strike comes with a warning, but the student cannot restore Internet access without first completing a class about computer misuse. The third strike results in disciplinary action. These steps, however, only happen when the university is notified by a copyright holder.

Since updates to policies tend to take time in order to contain any ramifications for when an institution fails to follow suit, the new copyright rules have not yet been made compulsory. Worona (2008) and the Common Solutions Group (2008) believe that it will come soon. Institutions such as Michigan State University (2009) have already followed part of the revisions by posting their annual disclosure as per the first part of revision. Michigan's disciplinary policy follows an almost identical pattern to that of the University of Central Florida. Following Chiang and Assane's (2007) assertions that students would be less likely to pirate in light of free legal alternatives, Michigan State University offers none at the present time but has periodically searched for such opportunities.

From the perspective of "defying" the P2P rules, a Harvard Law professor, in the Tenenbaum case, has defended one of the university's students as well as challenged the statutes that were added to the 2008 version of the Higher Education Act. The outcome of this case could affect how university libraries could operate in the future (Fitzpatrick, 2009). The professor, Charles Nesson, has asserted that the RIAA has improperly used the statutes. However, at the start of the trial on July 27, 2009, Judge Nancy Gernter threw out Nesson's proposed fair use defense at the last minute. This action was justified because the approach was so broad that it would challenge copyright laws in their entirety. She also stated that fair use was only valid if the claim was along the line where the defendant, "'deleted the mp3 files after sampling them, or created mp3 files exclusively for space-shifting purposes from audio CDs they had previously purchased'" (Anderson, 2009a) or in a situation where the infringement occurred before laws were in place. Thus, while this case aimed to further damage the RIAA's legal grip, it only helped to strengthen it. In actuality, the original win for the RIAA in the Jammie Thomas-Rasset case only served to bolster reliance on the traditional business model. Any loss of a trial by the RIAA would have served as a catalyst for the adoption of new and altered models and copyright rules (Lincoff, 2008).

Creative Commons

Creative Commons is a non-profit organization that provides a free alternative to common copyrights. Instead of reserving all rights of a work under a standard copyright, a Creative Commons license allows the user to reserve only some rights and allow other people to use their works for “remixing” and general sharing and blurring the lines between protection and public domain. A user could simply use Creative Commons to make a work public domain, or allow Internet users to share or make derivative copies of a work based upon the restrictions of the license issued. If a license contains a restriction, it may be waived if permission from the owner is granted (van Eechoud & van der Wal, 2008). Though Creative Commons may sound as if it is a replacement to copyright, it simply provides an extra layer of protection. If one of the restrictions of a Creative Commons license is violated, the owner may still use protection from a copyright. Since only some instead of all rights are reserved, copyright law still applies to those rights. A Creative Commons license, however, could be deadly if used for the software industry or outside of the public sector. Any works created in the public sector could find some benefit if the proper license is used. For example, a work under the Attribution--NonCommercial--Share Alike license allows for people to make copies of the work provided they properly give credit and make derivatives of the work. They cannot, however, use the work for any commercial applications unless they obtain explicit permission from the owner of the work (van Eechoud & van der Wal, 2008). Because of the sharing application, private industries would follow a similar scheme and in effect legalize piracy of their goods. Therefore, industries could explicitly allow copying for uses such as education or remixing. Convincing private industry to take on an alternative copyright scheme would be a monumental task.

Software Deterrents to Piracy

In 2006, the Electronic Frontier Foundation (EFF) (2006) performed a study of the flaws in many of the P2P monitoring software systems. According to the EFF, all types of monitoring software or software alternatives have either contained an exploitable loophole or have restricted student rights on some level. For example, firewall software may block P2P traffic across a specific port, but the savvy student could take a few routes to circumvent the restriction. A student could simply change ports to one that the software is not blocking, which could start a massive “cat-and-mouse” scenario. Furthermore, a student may also hide the data in a port that a firewall will never block such as port 80 for standard web traffic (Nyiri, 2004). Though content-monitoring software has been considered to be the primary means to stopping piracy, file-sharing programs and crafty students can use SSL encryption to hide their tracks. Because the connection is encrypted, a monitoring program would only see nonsense due to the encryption. The EFF has also mentioned traffic-shaping programs that can alter the amount of resources for specific functions, but it also falls prey to the aforementioned circumvention methods. From a student rights perspective, students will not be comfortable knowing that their institution is tracking their every move online. In other cases, the measures could also generate false positives where a student is downloading a file through P2P for educational use as described through the fair use doctrine.

Considering the vast size of a campus network, it is foreseeable that there is a massive amount of traffic flowing through it. With that considered, IT professionals need to use some form of software in order to filter through the equally massive raw data. Though some software packages will do their job,

> . . . many of the solutions generate only a slightly smaller amount of data than the raw network. The next group of companies sells a product that takes the output of the first layer and tells you what your problems really are. A third group of companies sells yet another layer of products to finally produce actionable items. (Rosenblatt, 2008, p. 9)

Thus, while IT software products may be effective, they can easily become numerous and costly (Rosenblatt). With different copyright monitoring solutions available, determining the best one is at the very least time consuming. The Common Solutions Group (2008) is a collective of IT professionals from 30 universities, 28 of which are research institutions. Common Solutions Group has further supported the EFF's findings with its own study. In this study, three major copyright-prevention software packages: CopySense, cGrid (formerly ICARUS), and Clouseau were considered. It was found that CopySense and Clouseau both relied on the vendor for blocking parameters. Students may bypass CopySense by downloading files that are not registered into the CopySense database or use SSL encryption. Clouseau sets its parameters by allowing and blocking vendor-set communication routes which operators may not modify. Though blocking whole communication channels sounds ideal, some channels may already have legitimate and legal uses through the campus. Since the network operators have no control, another piece of software may become worthless. Finally, cGrid was determined to be the most advanced of the three programs but was also the most expensive and resource intensive. cGrid differed from the others by reporting patterns rather than using outright suppression but could also be configured to act similarly to the other two programs in the ICARUS incarnation (Nyiri, 2004). This caused added network strain and more network administrators to interpret cGrid's output. It was concluded that while this type of software would improve in both quality and price in the future, the current offerings were expensive and inefficient. More importantly, the universities involved in the study concluded that software alone will not end student copyright infringement violations. They expressed the belief that constantly educating and reinforcing ethics to students would yield better results. Though the software approach appeared effective in 2004 (Spanier, 2004), the improving technology and student craftiness eventually rendered the software ineffective.

In Gopal et al.'s (2004) study of piracy's economic impact, the authors found that two broad types of controls exist to help combat piracy. The first control was the deterrent control that contains methods that attempt to deter users from pirating media. Legal action, educational, and media campaigns are just some of the general categories of these deterrents (Djekic, & Loebbecke, 2007). According to the authors, deterrent controls do not directly influence but attempt to indirectly dissuade a person with threats. At the time the article was written, the RIAA was beginning its legal campaign (EFF, 2008) which was the first and primary deterrent control for music piracy. Another deterrent control is one may that be self-inflicted by the copying community--computer viruses. Viruses, however, may only act as an effective deterrent to students if they are also bothered by legal action. Those who do not care about the threat of legal action will feel the same about viruses (Wolfe, Higgins, & Marcum, 2008).

Preventative controls operate from the viewpoint of making the process too time, labor, or financially intensive to make pirating less worthwhile (Djekic, & Loebbecke, 2007). Although this has been a common practice in the software industry, the music industry has also embraced these practices. Such practices include DRM and similar fingerprinting techniques to make digital files harder to share, and software encryption to make copying files off of CDs more difficult. Like the P2P prevention programs previously discussed, all preventative controls contain an exploitable weakness that a determined individual may avoid. The only difference comes from the increasing difficulty in overcoming these barriers. Considering the speed with which technology progresses, such a situation may never occur. Dejekic and Loebbecke, in their study of preventative controls for computer software, provided proof that preventative controls are ineffective and that software companies would be wise to invest in deterrent controls.

Software Deterrents as Ethical Beings

When a piece of software is designed to interact with people or run autonomously, artificial intelligence (AI) must be incorporated. Depending on the level of AI required for a program, a piece of software may simply run a task at a given time or be required to make decisions based upon specified criteria. In some cases, these decisions will contain ethical ramifications. Stahl (2004) explored the computer's ability to act as an autonomous moral agent--an entity capable of making moral decisions. To do so, he looked into the connection between an autonomous moral agent and the Moral Turing Test. The Moral Turing Test is derived from the classic Turing Test which investigates a computer's ability to imitate human thought.

One instance of conducting a Turing Test was documented by Moor (2001) to test Allan Turing's original prediction in the 1950s that computers could easily imitate human thought by the 21st century. The test involved 10 different judges, including an author, a graduate student, and an undergraduate student, all of whom had no technical background. Each of the 10 judges conversed with 10 people (respondents) through a computer terminal. Of the 10 respondents, six were computers and four were human beings. After five minutes of interaction, the judges needed to decide whether the entity on the other side was a computer or a human. At the end of the study, all of the judges correctly identified the computers, but some mistook the humans for computers, providing evidence that computers have yet to reach the point of imitating human thought. Allen, Varner and Zinser (2000) supported these results through the failures of the Moral Turing Test which took the same principals of the Turing Test but restricted it to moral principles. Problems with the Moral Turing Test have come from computers potentially acting more moral than human beings, and computers being held to higher moral standards than humans. Although monitoring software has not been needed to interact with users as described by Moor, the act of disconnecting users who transfer copyrighted material remains an act of morality. With the general weaknesses of current detection software, new versions could potentially take the idea of the Moral Turing Test and improve the software to be more effective (Common Solutions Group, 2008).

Classical Ethics

Considering that ethics has been viewed as a critical component in solving the piracy problem (Common Solutions Group, 2008; Coyle et al., 2009; Einav 2008; LaRose et al., 2005; Siegfried, 2004), some of the classical ethic theories have been explored in this section of the review. In classical ethics, there have been four main theories: Ethical Relativism, Utilitarianism, Deontological Theories, and Virtue Ethics. Each theory has positive and negative aspects when compared to what is believed to be normal and appropriate in Western society (Johnson, 1994). The three theories have been reviewed in detail in order to obtain a better understanding of ethics.

Ethical Relativism

The concept of ethical relativism places ethical concepts relative to a group. What one nation believes as proper behavior, another may perceive as barbaric. Relativism may even be filtered to a person-by-person basis. Thus, ethical relativism may be summarized as "'There are no universal moral rights and wrongs. Right and wrong are relative to one's society'" (Johnson, 1994, p. 20). At the same time, there is no way to prove this claim properly because while one's society and environment help shape one's ethics and changes in the environment may alter one's ethics, underlying beliefs and morals may be unrecognized. From this perspective, two people from differing cultures may have opposite opinions as to the ethics surrounding abortion or computer piracy, but they may share similar moral beliefs as to appropriate punishment for murderers or the value of a human life. This creates confusion and defines the scope of ethical relativism. If focused on controversial topics in ethics, relativism works. When applied in a larger, more global setting, relativism may contradict itself. Johnson further highlighted the contradictive elements by using the example of selling modern computers to Hitler before America's involvement in World War II. Under ethical relativism, one would need to determine if the use of the computers would fit the needs of the current society of Germany. Unfortunately, ethical relativism cannot account for rebellions against the norms of a society. So, if the German people were rebelling, they could be considered to be wrong minded, because they did not follow the current societal norms. Because of all the contradictions, coming to a conclusion would be more difficult than the concept initially implies. For computer piracy, one may see a similar conflict of two groups. One group believes piracy is wrong because it is contrary to the current societal model. The other group believes it is time to change. With both groups as part of the same society, the same conflict as presented in Johnson's example can be observed in terms of ethical relativism and a potential rebellion.

Utilitarianism

Theories which seek to maximize pleasure and minimize pain began with Epicurus. Though his theory was easily misinterpreted, it focused on maximizing long-term pleasure through leading a thoughtful, prudent lifestyle. This pleasure versus pain belief was the classical precursor to utilitarianism (Edgar, 2003). Utilitarianism seeks to perceive ethics in a different manner to avoid the conflicts created by ethical relativism. The driving force of utilitarianism is to find solutions that maximize the level of happiness for those affected. Thus, utilitarianism is best defined as "Everyone ought to act so as to bring about the greatest amount of happiness for the greatest number of people" (Johnson, 1994, p. 24). In order to determine if something is ethically sound from a utilitarianism perspective, value must be applied to any object or concept. These could take on either an intrinsic value or an instrumental value. Instrumental goods gain value as a means to an end that would lead to happiness. Intrinsic goods are valued for what they are with happiness being the definitive intrinsic good. An example of this is using money, an instrumental good, as a way to obtain a college degree, another intrinsic good. Furthermore, that degree may become an instrumental good to obtain a further intrinsic good such as a job. Eventually, by obtaining these instrumental and intrinsic goods, one will eventually obtain happiness. Hence, when one must make an ethical decision, the amount of happiness one can derive from each outcome becomes the primary factor. It should be noted, however, that utilitarian happiness focuses on happiness as a whole rather than personal happiness. This eliminates any selfish elements that may exist. Similar to ethical relativism, utilitarianism also has conflicts. Rather than the theory conflicting with itself, utilitarians present two conflicting interpretations. Rule-utilitarians focus solely on the rules and the effects they would have on society's overall happiness. Anything not leading to happiness would therefore lead directly to pain or unhappiness. Act-utilitarians, focus more on the act than the rules. An example of this would be deciding that lying would bring more happiness than the truth in a particular situation even though telling the truth is the common rule in the society (Johnson).

Despite the fact that utilitarianism is characterized by a "happy air," it features some situations that are difficult to rationalize. Such situations emerge when a solution sacrifices the happiness of a few to bolster the happiness of the masses. Johnson (1994) used the example of a hospital having a kidney dialysis machine. Though the machine could save lives, the hospital could not afford to treat the number of patients who needed the dialysis. The hospital would need to make decisions that would impact whether a particular patient lives or dies based on what each patient would contribute to society in order to maximize the overall happiness benefit the machine provided. Where utilitarianism has failed has been in ignoring the value of human life. A derivative of utilitarianism known as Kantian theory, however, stated that individuals must only exist as an end and that all individuals are equal. To apply Kantian theory in Johnson's example, randomly selecting people where every person had an equal chance of being selected would be the only plausible conclusion.

Deontological Theories

Deontological theories operate by focusing on the nature of a person's action as opposed to focusing on the effects of the action within society as described in ethical relativism and utilitarianism. If a person's actions are acceptable to and expected by another person or society, an act is considered acceptable. If, however, a person's actions are to avoid an expected outcome or to obtain some form or reward, the act is not acceptable. One major difference between the other two theories discussed in this section and deontological theories is that some actions will never fall under acceptable terms. For example, any action that involves intentionally taking a life at any cost is always morally wrong. Deontologists usually find conflict with utilitarians over the utilitarian view of making happiness the ultimate goal in life. They believe that if happiness was society's ultimate goal a person's mind would naturally work towards it. In reality, the focus lies more on a person's capacity to make rational and moral decisions. Rather than treating happiness as the ultimate goal, one sets an ultimate goal through the decision making process. Finally, one of the most important aspects of deontological theory involves treating people as equals and never as means to an end. This concept resembles Kantian theory, which is a type of deontological theory (Johnson, 1994).

Johnson (1994) provided an example of deontological theory involving researcher-subject confidentiality. In this example, a researcher must make a choice regarding the use of graduate assistants to input sensitive data from interviewed subjects. The researcher, having guaranteed anonymity to each of the subjects, would need to input and recode data into a computer program. Although allowing the graduate students to input the data would speed the process and allow the researcher to get to more important analyses, allowing another party to input data would pose a risk of a data leak. This view, however, still reflects thinking under a utilitarian perspective. Johnson stated that a deontological perspective would view each promise of confidentiality as a promise that participation in research would not affect a participant's ability to continue pursuing their own goals. By breaking that promise and allowing graduate students to input the data, the researcher no longer treats the subjects as an end. Deontological theories and utilitarianism greatly differ in the theoretical sense, but they can come to the same conclusions most of the time.

Deontological theories, as the name suggests, bring together a number of theories that place more emphasis on the consequences than on individual actions. Stoicism is a theory based upon the world being in a constant state of change, yet there is an underlying rationale. Because one cannot control nature, the best course of action involves being in harmony with it. This could involve finding others who bring good will, help bring good will to society, or any other action that one may view as bringing society closer to the flow of nature. Stoicism also calls for people to take a stoic stance on life which means that emotions should be repressed at all times. Deeming an act right or wrong closely follows a person's intentions in performing an act, because the outcome cannot be predicted. From some aspects, stoicism may be the simplest form of a deontological theory (Edgar, 2003).

As mentioned earlier, Kantian theory is a deontological theory that is derived from pieces of utilitarianism and stoicism. Kantian theory, devised by Immanuel Kant, adds a degree of certainty to ethics. Kant believed that good intention was the only form of good that did not require some form of pre-qualification. Even if an attempt were to fail, any good intentions behind said action still make it "good." Kantian theory also links the concept of good to a sense of duty. This means that one requires a proper motive behind an action in order for it to be considered a good action. Furthermore, any emotions or enjoyment associated with the action are considered irrelevant by Kantian theory, because enjoyment is no different than an animal trying to avoid pain and seek pleasure (Edgar, 2003). This in turn, violates the key principle of utilitarianism which aims to seek happiness, the ultimate pleasure. The outcome of an action does not affect whether it was good or bad. Edgar used an example of two people donating to a charity. One person donates using earned money, and another donates with stolen money. Although both actions achieved the same outcome, donating with stolen money began as a bad and amoral intention. Examined from a utilitarian perspective, both actions would be considered moral because happiness was derived from the end result. Another example that further explains Kant's attack on utilitarianism involves three programmers who completed the same tasks but took different moral paths. One programmer avoided doing anything amoral out of fear of being apprehended, another took on the task because of its underlying cause, and the last programmer took on the task because it was part of the contract and the contract needed to be fulfilled. Once again, the first two programmers held utilitarian views. One tried to avoid pain, while the other sought and gained pleasure. The third programmer took on the task as a responsibility out of a sense of duty, a good fit with Kantian theory. What makes this example different from the previous one is that the underlying causes are less pronounced and therefore more realistic in most cases. In a real-world situation, however, making such distinctions becomes impossible because persons rarely perform acts purely out of duty. Kant defended this point by positioning his theory as a model and cautioned that other factors need consideration in real-world situations.

Kant considered what he called a rational being to do only what is good, but most people fall under the category of imperfect rational beings and may take other factors into consideration. This consideration has fueled the arguments related to the problems of Kantian theory when it has been applied to typical everyday scenarios. In order to counterbalance and make the theory more practical, Kant devised a number of imperatives. Imperatives provide a similar feeling to that of a command. Unlike the rational beings who would state that they would do something, imperfect rational beings would state that they ought to do something. By using the phrase “ought,” a person justifies what should be done but also recognizes that there are some limitations that could prevent or hinder the action. Imperatives also come in two distinct types--hypothetical imperatives and categorical imperatives. Hypothetical imperatives represent an end and the means to achieve said end. Categorical imperatives take the form of an action and the commands to execute the action. Regardless of the type, however, imperatives will always be represented by a formula that states “‘If you want A, then do B’” (Edgar, 2003, p. 66). Kant also developed categorical imperatives which are imperatives that fall within a definable universal law. Any actions that could be defined by a universal law are considered moral, and those that fail to fit into a universal law are not moral. These categorical imperatives, however, become useless for trivial matters such as pushing a chair back under the table after use. Furthermore, almost all actions that are universalized will contain at least one exception (Edgar, 2003).

Virtue Ethics

All of the theories discussed thus far in this section contain at least one inadequacy when applied to common, real-life scenarios. Virtue ethics is viewed as a model that could correct the inadequacies found in Kantian theory and Utilitarianism. Virtue ethics, originally created by Aristotle, combine a view on good character along with a good life for a human. The concept of means and ends is simply activities performed by one for the sake of another and activities performed for oneself. Aristotle also defined happiness as an act of the soul that reflects human virtue. For any act to be virtuous, one must "(1) know that what you are doing is virtuous; (2) choose the act; (3) do that act for its own sake; and (4) act according to a fixed, unchanging principle, or out of a fixed character" (Edgar, 2003, p. 70). In essence, an action must be taken voluntarily in order to be viewed as moral or immoral. Any actions that could not be traced to a particular source are ignored due to lack of control. Thus, committing a heinous act that was forced by another is ignored under virtue ethics, but committing the same act because of self-inebriation would not. Because virtue ethics involves viewing the good as an end, choices weigh heavily on the means to achieve the good and developing good actions from said choices. A person may forget a piece of knowledge at any point, but moral conduct, such as knowing that robbing a bank is wrong, never leaves a person's memory (Edgar, 2003). With this in mind, it becomes apparent that when looking at digital piracy some learning is acquired through incorrect moral guidance, and trying to change one's viewpoint can become an extremely difficult task. If students enter a post-secondary institution with a pre-conceived notion that digital piracy is acceptable, trying to teach them otherwise will pose more challenges than will be posed by students who do not share that opinion or lack an opinion. What also makes the ethical component difficult is that under virtue ethics and deontological theories such as Kantian theory, digital piracy is immoral. However, under utilitarianism, digital piracy is moral because students use the means of illegally downloading to obtain the end of software or music which leads to happiness

Ethics and Computers

Rogerson (1996) recounted a speech given by professor Terrell Ward Bynum where he argued that information technology (IT) plays one of the leading roles in shaping and changing society. Compared to other societal revelations such as the Industrial Revolution, IT was thought to create a larger impact because of its ease to seep into a person's life. Furthermore, human values would exhibit the most change from IT. Bynum provided examples of IT slowly seeping into society through the ease of news travelling from person to person and the functionality IT provides for disabled people. Looking at these implications from both utilitarianism and Kantian theory, the two ethical theories share similar outcomes. From the utilitarian perspective, because IT will allow more people to take care of themselves who previously were unable, more people will find a way to achieve happiness. From the Kantian perspective, allowing IT to grant more people autonomy and control of their lives is an ethical and moral act. Regardless of the theory used, people need to consider the impacts and implications of a new form of technology (Rogerson). P2P technology and digital media easily fall into this category. Both are relatively new technologies and both have significantly impacted the way people live their lives. The impact and implications of such technologies, however, may not have been thoroughly considered, and actions may be required in light of current events. In the next section, the realm of computer ethics, an applied ethical theory that is specifically formulated for computer usage, from its basic concepts, alternatives, and teaching methodologies in the university, will be explored.

Computer Ethics

Considering the level of harm a person could cause with a computer, having an appropriate code of ethics becomes paramount to keeping the virtual population safe. As with an offline society, unsavory characters always exist but when factoring in the global scale of the online society, strong ethics may be the only way to safely police the Internet. Forester and Morrison (1994) indicated that computer safety requires education in three principles: encouragement of more ethical behavior, better understanding of social problems brought on by computers and the digital age, and sensitivity towards computer-related moral dilemmas that will surface over the course of people's lives. Forester and Morrison viewed these principles from the perspective of a computer science program, and they believed that simply adding a required course on computer ethics to the curriculum was not sufficient to solve the problem. In actuality, they advocated that ethics should be integrated and be a recurring theme throughout all computer science courses. They recognized, however, that not all computer science professors possessed the preparedness to teach ethics in such a manner. Finally, Forester and Morrison noted that teaching ethics and morality was not a cure for all the ills of the virtual society but could significantly contribute to alleviation of many problems.

One of the most pressing issues in ethics has involved transitioning classical ethics theories into a less-defined environment:

> 1) it is logically argumentative, with a bias for analogical reasoning, 2) it is empirically grounded, with a bias for scenarios analysis, and 3) it endorses a problem solving approach. . .4) it is intrinsically decision-making oriented. . .5) it is based on case studies. (Floridi, 1999, pp. 37-38)

Although computer ethics follows three general guidelines of classical ethics in points one through three, it also utilizes the driving force of point four and the methodology in five. With the addition of the other two factors, it also uses the driving force of computer ethics built itself as a more applied version of ethics focusing more on real-world applications than a theoretical nature. According to Floridi, this applied viewpoint of computer ethics, known as microethics, is the common viewpoint, and even though the moral implications created by computers have no non-digital equivalents little consideration goes into a theoretical component. Floridi believed that the classical theories will never fully satisfy all the conditions behind computer issues or may even risk placing computers in an anthropomorphic light. Though the earlier discussions of deontological theories such as Kantian theory appear initially to apply to issues such as copyright infringement, any form of computer crime typically follows a person-to-computer path rather than the person-to-person view detailed in deontological theories. Virtue ethics, another viable ethical viewpoint, also faces the same problems of focusing on people rather than the damages that indirectly affect people. Brey (2000) supported the viewpoint that computer ethics focused heavily on application, but argued against Floridi who advocated that applied ethics could affect policies and practices if properly applied. Though applied theories require a foundation of theoretical ethics to function properly, they do not require the reliance on any particular type of ethical theory. In other words, a theoretical base used for digital piracy may not be applicable for hackers who would require the implementation of a different ethical theory. Brey also discussed applications of computer theory, noting that many seem to have ignored computer ethics' ability to solve a preexisting problem caused by a policy vacuum as well as to make the computer portion transparent so that only the ethical portion remains visible. In the case of digital piracy, this would involve removing all the computer and technological components to boil the act down to outright stealing.

Disclosive Computer Ethics

Brey (2000) proposed that computer ethics should be divided into two groups, disclosive and non-disclosive computer ethics. Disclosive ethics pertain to "disclosing and evaluating embedded normativity in computer systems, applications and practices" (Brey, p. 127). Disclosive ethics are comprised of a two-step process of finding a theory or moral definition behind a problem followed by an application based on the previous step. This approach, however, forces a dependency on a moral theory that may not always be available. Furthermore, even if a theory exists to explain an issue, there is always a chance that not everyone will agree with the theory's relevance. A theory may contain preconceived views regarding a computer component that may sound viable yet is impractical in an applied situation. Nondisclosive computer ethics are preexisting situations that would be handled in a more traditional manner.

In order to truly be effective with disclosive ethics and help ease the issues that arise, Brey (2000) suggested a three-level approach. The first level is the disclosure level which is where the disclosive ethics procedure is performed. The second level is the theoretical level where moral theories are developed and refined based upon the discoveries in the disclosure level. The last level is the application level where a solution based on the theory in the other two steps is devised and implemented. By using this methodology, a multi-disciplinary approach can take place because there is a need for computer experts to comprehend and explain the technology in question to philosophers and ethical theorists so as to reach an appropriate conclusion. In the case of nondisclosive computer ethics, the problem at hand and its moral implications were previously defined at an earlier point in time and thus do not require the need of a disclosure level. In a nondisclosive situation, information has already been obtained by researchers at the disclosure level. Thus, only the theoretical and application levels are needed in order to successfully solve a situation. Brey's methodology is used to find a middle ground in the computer ethics debate by not forcing a particular theory into a situation where theory may not apply to all computer situations.

Information Ethics

Floridi (1999) suggested that instead of computer ethics, information ethics should act as the theoretical component for people-to-computer relations. Although information ethics may not contain the application component of computer ethics, it at least connects the ethical standards to a moral subtext. Under information ethics data, users, and any other entities are treated equally when considering moral standing. Some situations may result in regressing to a by-person situation similar to utilitarianism or a deontological theory, but the overall perspective permits actions in an object-oriented view. Consequences are always anticipated to the best of one's knowledge. Though this fails to truly integrate a moral component, it does contain an ontological component that finds moral actions ones that are "impartial, universal and 'caring'" (Floridi, p. 45). This component ultimately takes the place of theoretical cores such as Kantian theory's moral imperatives. Floridi validated this theory against the classical theories by noting it had a number of controversial components and contained value beyond the computing field as did classical theories. Even though classical theories have not been associated with computing, they have been associated with different fields of study. As an example, Floridi described a child playing destructively in an abandoned junkyard. Even though nothing in the junkyard is alive or contains anything that would cause harm to another, the child's enjoyment is a destructive behavior. Utilitarianism cannot properly explain why the action is wrong, but at the same time the child is obtaining happiness by the destructive acts. This actually mirrors Johnson's (1994) example about the doctors and the dialysis machine. Virtue ethics state that the action is morally wrong because of the effects of the act on the child, but an argument surfaces asking if the morally reprehensible act could actually lead to preventing something worse in the future. Under information ethics, the child's acts are immediately viewed as immoral out of disrespect to the objects in the junkyard, and the actions simply create more chaos in the junkyard with all the broken parts (Floridi, 1999). Tavani (2002) posed a slightly different view on the issue by stating that it is possible for Information Ethics to be incorporated but not as a new type of methodology. Relating this argument to the field of student copyright infringement, a student downloading through a P2P network would cause disrespect for the piece of media and by proxy the people who created the media. This would cause more chaos in the industry by adding yet another unauthorized copy.

Teaching Computer Ethics

The Association for Computing Machinery (ACM), one of the major organizations in the field of computer science, has historically advocated the teaching of ethics to computer science students. Teaching ethics to students, however, has always posed a challenge. Werth (1997) proposed a potential methodology to successfully teach ethics. An appropriate introduction to the topic would begin with basic issues of what composes computer ethics, its importance, and topics such as intellectual property, privacy, types of computer crimes, and the social implications of all of the ethical procedures. Beyond the introductory material, appropriate definitions would be provided to help clarify the meanings of terms such as morality and ethics along with problem-solving techniques to allow a student to determine all of the moral and ethical implications that revolve around devising a solution to a given scenario. Werth also discussed some newer approaches to teaching computer ethics. One alternative, paramedic ethics, looks less at traditional ethics. Rather, the focus is on how to solve problems that may show up in a work environment when multiple routes of differing ethics may be chosen. Although such a method may not deter a student from choosing to pirate media, it would provide the student with helpful business skills for the future. Another alternative method known as Project ImpactCS aims to effortlessly integrate ethical topics with their social impact. The curriculum would contain the principles and skills from both the ethical and social strata and address the responsibility the student would undertake. By properly integrating these five areas, students would develop an appropriate context to make appropriate choices. If such a curriculum could be modified to fit with students from outside the computer science major, it could help create more law-abiding students who are less likely to pirate if they know all the ethical and social implications behind their actions.

Another problem with teaching computer ethics has been noted relative to the number of ethics courses in college programs. Nicholson and DeMoss (2009) examined both the existence and presence of ethics and social responsibility-centric courses in business colleges. A total of 405 business curriculum administrators from

380 institutions in North America were surveyed. In terms of field within the college of business, there was a relatively equal representation of accounting, finance, management, and marketing programs. Contrary to the belief that business schools implemented ethics courses in their programs, it was found that the colleges inadequately implemented ethics at the graduate student level. In the majority of responses, ethics was rated higher in importance than social responsibility even though social responsibility was becoming more important in business curricula. As a result, it could be said that business colleges needed to place more of a focus on ethics and social responsibility and to identify instructors qualified to teach the subject in a field where such subjects are important. Between public and private institutions, private institutions appeared to better integrate the two topics into the curriculum. This study focused on ethics in general as opposed to computer ethics The results of the study indicated the difficulty that computer ethics courses might find in making their way into curricula given the lack of traditional ethics courses.

Student Ethics Studies

In one of the first studies on computer ethics and students, Slater (1991) revealed that "information systems and business students appear to worry less about computing ethics than do today's executives" (p. 90). He reflected on a study conducted at James Madison University where over half of 300 students between the ages of 19 and 45 had admitted to using computers for some form of unethical use including software piracy. Some students had indicated they would purchase at least one copy of a program and make copies for other computers they use with the hopes of promoting the product in the future, but they could not deny that piracy took place. Slater also made apparent the now common student belief that computers add a layer of anonymity which makes the crime appear faceless. Slater believed that ethics must be taught from an earlier age, and the younger the better but also indicated that partnerships between IT and students would be the only way ethics will actually be applied beyond academic coursework.

Slater (1991) identified an initial problem of students using computers for unethical reasons. In a study conducted by Athey (1993), the ethical beliefs of students were compared to those of experts in the field for the purpose of determining the ethics gap between the professionals and the students and determining curricula to fill the gap. In the study students were compared by gender, income (low, middle, high), and major (computer science and computer information systems). The experts were those professionals who first examined ethical scenarios in the computing field. Of 19 different scenarios presented in the survey, females and males disagreed with seven and eight of them respectively. By major, males and females disagreed equally with 10 scenarios each, and the economic groups fared about the same. Despite all the disagreements, there were seven scenarios where all student groups agreed with the experts. Athey concluded that the scenarios should be addressed in course curricula. Although this study was not directly focused on digital or software piracy, it did provide insight into students' ethical perspectives. If students act in unethical ways due to constant exposure, stronger ethics curricula should be developed for not only computer science or computer information services students, but for the entire campus population .

Leonard and Haines (2007) conducted a study in which they attempted to determine if any differences in ethical beliefs were present when students completing a survey alone or in a group. After completing the survey alone online at computer stations, the group was divided into smaller groups of five to nine depending on the size of the group being tested at the time and allowed to chat online with group members while taking the second survey. The results of the two surveys showed that the virtual group actually strengthened the responses. If the general response to a question was considered ethical on the individual test, the group test results leaned further towards ethical and vice versa. Though the main constraint in this study was the use of students rather than IT professionals with experience, this did provide evidence regarding the influence of group behavior on decisions.

Thong and Yap (1998) conducted a study to test the ethical decision-making process theorized by Hunt and Vitell's (1986) deontological-based model. Though they did not analyze the entire model, they found that the model adequately described the ethical decision-making process in Information Systems students (Liang & Yan, 2005). Shang, Chen, and Chen (2008) followed up on Thong and Yap's work by surveying students with a similar model. They provided a scenario and alternatives of varying ethical value alongside intentions based upon a seven-point Likert scale. They found that people who pay for the use of P2P systems feel less guilty about piracy even if sharing on the P2P system breaks copyright laws. They also came to the generally shared conclusion that piracy was rationalized by students and was not considered to be a problem to them. Shang et al.'s instrument, however, was flawed in that it contained 110 items, many more than most students would want to complete.

CHAPTER 3: METHODOLOGY

Design of the Study

Prior studies reviewed in the literature focused on finding trends regarding students and digital piracy with similar results (Chiang & Assane, 2002, 2007, 2008; Gopal et al., 2004; Gupta et al., 2004; Higgins, 2005; Higgins, Fell, & Wilson, 2006; Logsdon et al., 1994; Rob & Waldfogel, 2006; Siegfried, 2004; Sims et al., 1996). Research into a different population may provide a different viewpoint on the digital piracy problem. Because IT professionals in the university were been directly involved in implementing, maintaining, and overseeing campus networks, their opinions on digital piracy and techniques used to thwart it were of interest in further understanding the problem.

The present study utilized quantitative methodology with a survey to obtain a number of descriptive statistics. The survey instrument was administered through a website on a personal, private server in order to improve safeguards against potential third-party tampering. By manually designing the webpage for the survey instrument, a correctly completed survey was guaranteed with a number of validation safeguards. The items themselves were based on (a) issues defined in the literature review and (b) an automated morality framework that questions if monitoring software could mimic human ethical behavior (Stahl, 2004). The finalized data were analyzed through SPSS software to obtain the needed results to answer the research questions.

Population

The population consisted of the IT department's security officers for the 11 Florida State University System (SUS) institutions. Each IT department contained at least one administrator for each institution who was knowledgeable about the operation of copyright infringement detection software. Because IT departments were responsible for the deployment and maintenance of monitoring software, they were an ideal group to survey regarding the effectiveness of monitoring software.

The role of the IT department chief security officer or information security officer was relatively new at the time of the present study, but its importance has increased as universities became more connected with the digital age. Information security officers are in charge of determining university security policy and are at the forefront of the campus network's security. Their duties include but are not limited to incident management, policy development, forensics, risk assessment, and coordination with law enforcement (Goodyear et al., 2009). They were the individuals who develop policies such as the University of Central Florida's (2009) three-strike policy for P2P usage and make sure the policy was enforced. Furthermore, the information security officer also possessed the authority to monitor the network to ensure that all users followed campus policy and disconnect or restrict access to offending users.

Sample Limitations

Because of the small number of information security officers in the Florida State University System, the sample consisted of the entire population, making it a census. As a result, the census was representative of the Florida State University System, but not representative of all universities in the nation. A total of 10 sample points were taken rather than 11 because two institutions share the same Internet connection. Furthermore, a 100% response rate to the survey instrument was a requirement of the researcher in order to compensate for the small population.

Instrumentation

Considering this study was the first of its type, an original survey instrument was constructed. Due to the lack of prior research in this area, the researcher relied upon the theory of automated morality as a framework for the instrument. The theory of automated morality explores computer software as a moral agent, an entity capable of making moral decisions. According to Stahl (2004), a program would be considered a moral agent if it can pass the Moral Turing Test, a test that determines whether or not software could pass for a moral being by an independent observer. In the end, the amount of trust the information security officer instills in the monitoring software reflects to what extent the software serves as a moral agent and reflects the software's overall effectiveness.

Information security officers possess the authority to monitor the campus network and remove any offenders based on policies that the officers helped develop (Goodyear et al. 2009). The Common Solutions Group (2008) looked at three programs that scour the network for data transfers that contain copyrighted material. Realistically, the information security officer cannot spend the entire day scanning the network for infringing material, so using an automated program to scan was a logical choice. The Common Solutions Group, however, based its analysis of the programs on infringements discovered and the ease of modifying the criteria. Furthermore, the software will also go so far as to restrict access to devices identified, one of the other main authorities of the information security officer. This lead to the question of whether or not the software was capable of making ethical decisions in the same manner as an information security officer when handling network violations. The instrument (Appendix A) consists of a web-based questionnaire. This method of surveying was chosen because web-based questionnaires provide a more enhanced method of presentation and collection than other survey methods. Although Dillman (2000) stated that web surveys may become problematic from a technological and computer penetration standpoint, the population was from a technologically-oriented profession, and such problems did not hinder the study. The questionnaire was hand-coded and run on a private server to further ensure compatibility with other computers along with improving overall security. Using this method, the questionnaire results were available as soon as the respondent completed the survey.

The questions on the instrument consisted of a total of 36 items. Of the 36, there were five yes/no items (3, 5, 6, 34, and 35), five multiple-choice items (1, 4, 30, 31, 32), three numerical fill-in items (2, 8, 33), two free-response items (7, 36), and 20 items using a five-point Likert scale. Items 1 and 35 also contained a fill-in response based on the respondent's prior answer. Furthermore, item 2 was not answered if the respondent specified "no monitoring software," and items 7 and 35 were not answered if the respondent answered no to items 6 and 34 respectively. All Likert scale items were positively worded so no special coding was needed, and they all contained a "not applicable" response to accommodate those to whom the item did not apply.

The 36-item survey was divided into four sections. After the respondents logged in to the survey via credentials provided in an e-mail, they proceeded to answer questions in the first section geared towards the policy aspect of copyright monitoring software (Higher Education Act of 2008). The second, and longest, section (Items 8-20) of the instrument related to challenges to implementing monitoring software such as price, staffing/training, overall acceptance of the software, and relative effectiveness of the software. Section three (Items 21-28) explored the alternatives to monitoring software ranging from ethics, alternative programs and deals, or just stricter standards. Both sections two and three were designed using

Likert scale questions. The final section inquired about demographics. As Dillman (2000) noted, demographic information is best left to the end of the questionnaire. The demographics section also contained a comment box for the respondents to add their own thoughts in order to further enhance the study.

Reliability and Validity

In order to properly utilize any type of instrument, reliability and validity must be determined. Validity represents how independent variables represent their dependent variables. In the case of questionnaires, validity reflects how selected questions correlate to their all-encompassing section. The higher the correlation, the more valid the questionnaire is (Thurstone, 1931). If low validity is present, questions in the survey may need to be either regrouped or reworded. Once the questionnaire is confirmed as a valid instrument, the next step involves confirming reliability. Reliability is the measure of consistency in an instrument. Though an instrument may prove to be valid, inconsistencies may surface over time as the population changes or the instrument measures a new population (Thurstone, 1931).

A pilot study was conducted in order to determine the instrument's ease of use and general usability. In most cases, a pilot study will utilize a separate sample of the population. Because the sample size was the same size as the population for this study, other people with reasonable knowledge of computing systems were sampled. The pilot study consisted of six people with strong knowledge in computers and networking, including one graduate of the University of Central Florida Computer Science program, and an owner of a large website. The study also included computer security officers from Florida community colleges. IT professionals in all 28 community colleges were contacted and nine responded stating that they were willing to participate in the study. Of the nine who agreed, three completed the study and one declined upon reading the questions. One of the main concerns of the individual who declined and also mentioned by two of the three completers was that Florida community colleges are non-residential and tended to see the problem on a smaller scale as compared to universities (J. Ward, personal communication, November 24, 2009).

Once the pilot data were obtained, a Cronbach's alpha test was performed to determine the reliability and validity. Cronbach's alpha is a split-half test that is able to determine if individual factors in an instrument properly contribute to the entirety of the instrument (Cronbach, 1951). Thus, if all of the questions in the instrument properly correlate to the specific group they were originally intended for, then the instrument is valid. The alpha level of .858, showed a strong level of reliability, but was not the most accurate value due to the small sample. Furthermore, the actual study also suffered from this problem due to a low sample size.

Statistical Procedures

Variables

The study consisted of a number of descriptive variables. First and foremost, the monitoring program variable was the most important as it represented which software, if any, the institution used. Other initial descriptive variables included when the software was implemented, opinions on the 2008 Higher Education Act, and other restricted uses. These variables all contributed to a general picture of each campus's IT department. The next set of descriptive variables addressed challenges. These variables included price, staffing, training, software effectiveness, and software acceptance. The challenge variables provided a guide to addressing potential problems with the software programs. The final set of descriptive variables referred to the alternatives of ethics, legal incentives, and legal action: (a) Ethics addressed respondents' viewpoints on ethics as a solution, (b) legal incentives addressed the respondents' viewpoints on alternatives such as discounted software or music, and (c) legal action reflected the respondents' views on current codes of conduct. The relation between variables, survey questions and research questions is shown in Table 1.

Table 1

Research Questions Variable Map

Variable	Question
RQ #1: Policy	
Implemented Policy	1, 2, 4, 5
Other Policy	3, 6, 7
RQ #2: Challenges	
Costs	9, 10
Staff Size	8, 11
Staff Training	12, 13, 14
Ease of Use	15, 16, 17
Acceptance	18, 19, 20
RQ #3: Alternatives	
Ethics	24, 25, 28, 29
Legal Alternatives	21, 22, 23
Legal Actions	26, 27

Note: Items 30-36 reflect demographic questions and do not tie into any research question.

Research Questions

1. What steps, policies, and measures have the 11 institutions that comprise Florida's State University System (SUS) taken to prevent copyright infringement as defined by Section 487 of the 2008 Higher Education Act?

To answer the first question, a combination of answers from the survey and searches for policy on each campus's website were incorporated to determine if the 10 SUS institutions shared similar policies and technology for preventing copyright infringement by students. The general policies and practices were collected and categorized to provide a general view of how each institution operated. Another key factor to answering the first question was the timing with which each university initiated the use of P2P monitoring software. Institutions such as the University of Florida designed their own tracking software in 2004, four years before the mandate (Joachim, 2004). If all of the institutions implemented software before the mandate, it would become a somewhat moot point. This was addressed by items 1, 2, 4, and 5. Some universities already followed the mandate, but the mandate may add difficulty to any proposed policy changes. Items 3, 6, and 7 accounted for other policies that may not be derived from the Higher Education Act but still relate to restrictions that might hamper a student's online freedoms.

2. What are the challenges in implementing the mandates stated of Section 487 of the 2008 Higher Education Act that require the introduction and implementation of tracking software?

The second research question was answered through the determination of factors such as the ease of operation and maintenance, cost, and utilization of personnel. Items 9 and 10 related to the cost of operating and maintaining the software which may pose a major problem when shrinking budgets are considered (Green, 2008). Items 8 and 11 represented staff size, and items 12, 13, and 14 represented the amount of training staff members would require to use the software. These factors contributed to the cost and overall usefulness of the software. The ease of operation and overall quality of the monitoring program was explored by items 15, 16, and 17. Based on the findings of the Electronic Frontier Foundation (2006) and the Common Solutions Group (2008), most methods to block piracy contain a number of backdoors that the savvy student may take advantage of. Finally, items 18, 19, and 20 measured the overall acceptance of monitoring software. The Common Solutions Group, and the majority of researchers on piracy, have expressed the belief that software alone would not be enough to deter students from piracy.

3. What alternatives, if any, were considered or are currently being considered to discourage piracy by college students at a lower cost than monitoring software?

Finally, the third question was answered by analyzing the responses to the remaining nine non-demographics items. These items elicited data regarding the viability of alternatives and identification of those universities that were actively considering policy changes. By analyzing similarities and differences between the universities, a clearer picture of P2P software and copyright infringement problems within the Florida State Universities was revealed. Items 24, 25, 28 and 29 addressed whether ethical issues should be considered as a viable alternative. This set of questions also paired with the acceptance piece of Research Question 2 to link with the IT professionals' overall level of trust in the monitoring software (Common Solutions Group, 2008; Coyle et al., 2009; Einav 2008; LaRose et al., 2005; Siegfried, 2004). Items 21, 22, and 23 generated data regarding legal alternatives to piracy. The survey did not mention any specific vendors, but did inquire as to attitudes of the institution towards providing less expensive alternatives. In these instances, according to Spanier (2004) and Easley (2005), students are more likely to take the cheaper alternative. Finally items 26 and 27 served as a measure of the extent to which current legal action and policy affected the students.

Statistical Analysis

Because this type of study was still in its infancy, the majority of the analysis utilized descriptive statistics. Data obtained also served as a baseline for future studies in this area. Variables were represented by a combined scale score derived from the Likert scale survey items or as individual variables for non-Likert scale items. The data in Section 4 of the survey and survey item 1 enabled demographic descriptions to indicate any preliminary differences between demographics and software used.

Authorization to Conduct the Study

In order to conduct any form of study on human subjects, authorization from the Institutional Review Board must be obtained. Because the study involved only public employees rather than protected classes such as children or prisoners, the IRB expedited process was utilized. Permission from the IRB review board to conduct the study is provided in Appendix B.

Turnitin

The University of Central Florida required all students to submit their dissertation and thesis through the Turnitin program as a safeguard against plagiarism. Papers received through this process obtain a score that reflected the amount of text found in other submitted documents. An acceptable score defined by the graduate advisor for this program was between zero and ten percent. This manuscript was approved as original work by the researcher’s graduate advisor. After submitting this work to Turnitin, the document received a score of 18%. By removing all bibliographic materials and quotations, the score was reduced to 6%.

Data Collection Plan

The process of collecting the needed data began with identifying the appropriate contacts at each of the 11 universities. The appropriate individual to contact was determined by information on the university’s website and individuals at each department’s front desk. With the contact information gathered, the 10 individuals were pre-contacted via phone and e-mail as shown in Appendix C to ensure that they were willing to participate and were knowledgeable enough to answer the questions in the survey. Each contact, upon approval, was then e-mailed an official contact letter as shown in Appendix D with a link to the survey, a user name, and a password. The respondents then completed the questionnaire within a two-week time span. At the conclusion of the study, a response rate of 100% was obtained. Thus, all results will have the maximum sample value of 10.

CHAPTER 4: DATA ANALYSIS AND FINDINGS

The findings of the study are presented in this chapter. The chapter has been organized around the three research questions used to guide the study.

Research Question 1

1. What steps, policies, and measures have the 11 institutions that comprise Florida's State University System (SUS) taken to prevent copyright infringement as defined by Section 487 of the 2008 Higher Education Act?

This question accounted for two major variables: Implemented Policy, and Other Policy. Implemented Policy explored the current policies each SUS institution was currently implementing. The variable was divided into four sub-variables as shown in Table 2.

Table 2

Frequency for Implemented Policy

Variable	Value	Frequency
Program	None	7
	cGrid / ICARUS	2
	Other	1
HEA Impact	No effect	1
	A little effect	8
	A noticeable impact	1
Ease of Altering	Yes	1
	No	9

Note: n for all variables is 10.

The sub-variable program is an indicator variable of the monitoring program used by each of the institutions as specified by the Common Solutions Group (2008). Two institutions used cGrid/ICARUS, one used a program called BlueCoat Systems, and the remaining use nothing. One of the cGrid institutions also utilized Copysense for student housing. Both cGrid users started their use of the software in 2004 and 2007, while the institution running BlueCoat started in 2006. The sub-variable HEA Impact discussed how large of an impact implementing the changes mandated by the 2008 revision of the Higher Education Act would have on institutions. This sub-variable was supplemented by the sub-variable Ease of Altering which asked how much of an impact in terms of major changes to the network adding monitoring software would have. Of the 10 institutions, one thought that the policy change would have more than a minimal effect, and one also stated that implementing the software would have a major impact on how the network operated. These two responses were not from the same institution.

The second variable, Other Policy, explored other policies that involve blocking non-P2P connections. Table 3 shows the results of the two sub-variables.

Table 3

Frequency for Other Policy

Variable	Value	Frequency
Utilize non P2P	Yes	2
	No	8
Other Bans	Yes	8
	No	2

Note: n for all variables is 10.

The first sub-variable, Utilize non-P2P, was designed to determine if the same monitoring software was used for more than blocking P2P traffic. Only two of the 10 institutions utilized monitoring software this way. Other Bans inquired if other policy bans such as disallowing servers in student dorm rooms had been implemented. Of the institutions, eight utilized such bans. Reasons included security issues, preventing piracy, and controlling network load.

Table 4 shows the policy structures of dealing with P2P violations. Six institutions utilized some form of "strike" policy with active network monitoring, shutting down a student's connection the moment P2P connections were detected; two took a passive approach, only reacting if P2P violations were made known to them from a source like a DMCA notice; and one institution required students to install a piece of code on their computer that actively checked for P2P connections and programs. One institution's policies could not be found, but were probably more in line with the passive approach.

Table 4

Count of P2P Policy Types

Policy	Count
Three Strikes	3
Two Strikes	2
Zero Tolerance	1
Passive Monitoring	2
Policy Key Ban	1
Unknown	1

Note: n = 10

Research Question 2

2. What are the challenges of implementing the mandates stated in Section 487 of the 2008 Higher Education Act that require the introduction and implementation of tracking software?

This question explored the challenges IT departments would face or expect to face with the implementation of monitoring software. The variables were comprised of combined 5-point Likert scale questions. Each individual question ranges from 1 (Strongly Disagree) to 5 (Strongly Agree). The combined scale of Cost was 2-10; while

Training, Ease, and Acceptance resulted in a combined scale of 3-15. The variable Staff consisted of a single question. These five variables were then split by the demographics variables: Gender, Degree Earned, Participant in a Professional Organization, and Length in Position. These demographics were selected because they were the ones most likely to show differences between demographic groups. The salary demographic contained three in the $70,000-$89,000 group and seven in the $90,000-$109,000 group. The salary group was dropped because there was little variance across each of the possible groups.

Without analyzing the data by demographics, Table 5 shows the results lie roughly in the middle of each variable's scale with the exception of Acceptance being slightly above average at 9.90. Across all of the variables, the confidence intervals spanned between two and four points, providing a fairly tight grouping.

Table 5

Challenge Statistics Unsplit

Variable	Mean	*SD*	*SE*	Lower Bound	Upper Bound
Costs	4.56	1.667	0.556	3.27	5.84
Staff	2.89	1.167	0.389	1.99	3.79
Training	8.89	1.616	0.539	7.65	10.13
Ease	8.11	2.571	0.857	6.13	10.09
Acceptance	9.90	1.912	0.605	8.53	11.27

Note: n = 10 for Acceptance. n = 9 for all other variables

Without analyzing the data by demographics, the results lie roughly in the middle of each variable's scale with the exception of Acceptance being slightly above average at 9.90. Across all of the variables, the confidence intervals spanned between two and four points, providing a fairly tight grouping.

Table 6 shows the five variables split by Gender.

Table 6

Challenge Statistics by Gender

	Male		Female	
Variable	Mean	*SD*	Mean	*SD*
Costs	4.33	1.966	5.00	1.000
Staff	2.67	1.211	3.33	1.155
Training	9.17	0.753	8.33	2.887
Ease	8.83	2.229	6.67	3.055
Acceptance	10.57	0.787	8.33	3.055

Note: n = 7 for males and n = 3 for females. n = 6 for males on all variables but Acceptance

The differences between most of the means were fairly similar. Males had higher average scores for Training, Ease, and Acceptance while females had higher average scores for Costs and Staff. Ease and Acceptance had the largest differences of over two points. Training (s = .753) and Acceptance (s= .787) for males had the lowest standard deviation implying less spread between the responses.

Table 7 shows the differences in responses between different degree types. All respondents had earned either a Bachelor’s or Master’s degree. The mean responses were fairly equal between groups, but there was less spread in the responses by those with Bachelor’s degrees for Training (s = .500 for Bachelor’s, s = 2.191 for Master’s) and Acceptance (s = .957 for Bachelor’s, s = 2.251 for Master’s). Conversely, there was less spread from those with Master’s degrees for Costs (s = 2.449 for Bachelor’s, s = .707 for Master’s).

Table 7

Challenge Statistics by Degree Earned

	Bachelor’s		Master’s	
Variable	Mean	*SD*	Mean	*SD*
Costs	4.00	2.449	5.00	0.707
Staff	2.75	0.957	3.00	1.414
Training	9.25	0.500	8.60	2.191
Ease	8.50	2.517	7.80	2.864
Acceptance	10.75	0.957	9.33	2.251

Note: n = 4 for Bachelor's and n = 6 for Master's. n = 5 for Master's on all variables but Acceptance

Table 8 shows that being a participant in a professional organization had little effect when compared to non-participants.

Table 8

Challenge Statistics by Professional Organization

	Participant		Non-Participant	
Variable	Mean	*SD*	Mean	*SD*
Costs	4.43	1.902	5.00	0.000
Staff	3.00	1.000	2.50	2.121
Training	8.86	1.773	9.00	1.414
Ease	7.71	2.690	9.50	2.121
Acceptance	9.71	2.289	10.33	0.577

Note: n = 7 for participants and n = 3 for non-participants. n = 2 for non-participants on all variables but Acceptance

Table 9 shows very little difference between the variables in the two experience groups other than the variable Ease which was rated 2.50 points higher in the 10-15 Years group.

Table 9

Challenge Statistics by Length in Position

	3-6 Years		10-15 Years	
Variable	Mean	*SD*	Mean	*SD*
Costs	4.20	1.924	5.00	1.414
Staff	3.40	0.894	2.25	1.583
Training	8.80	2.168	9.00	0.816
Ease	7.00	2.646	9.50	1.915
Acceptance	9.00	2.345	10.80	0.837

Note: n = 5 for 3-6 years and n = 5 for 10-15 years. n = 4 for 10-15 years on all variables but Acceptance

Sub-Variable Frequencies

The frequencies of the sub-variables that make up the five variables are presented in the following section. Figures and narrative discussion are used to present the results of the analyses.

According to *Figure 1*, three respondents thought that monitoring software was not appropriately priced, while three could not say if the price was appropriate. Furthermore, only three of the 10 believed that they had enough funding to purchase monitoring software at this time.

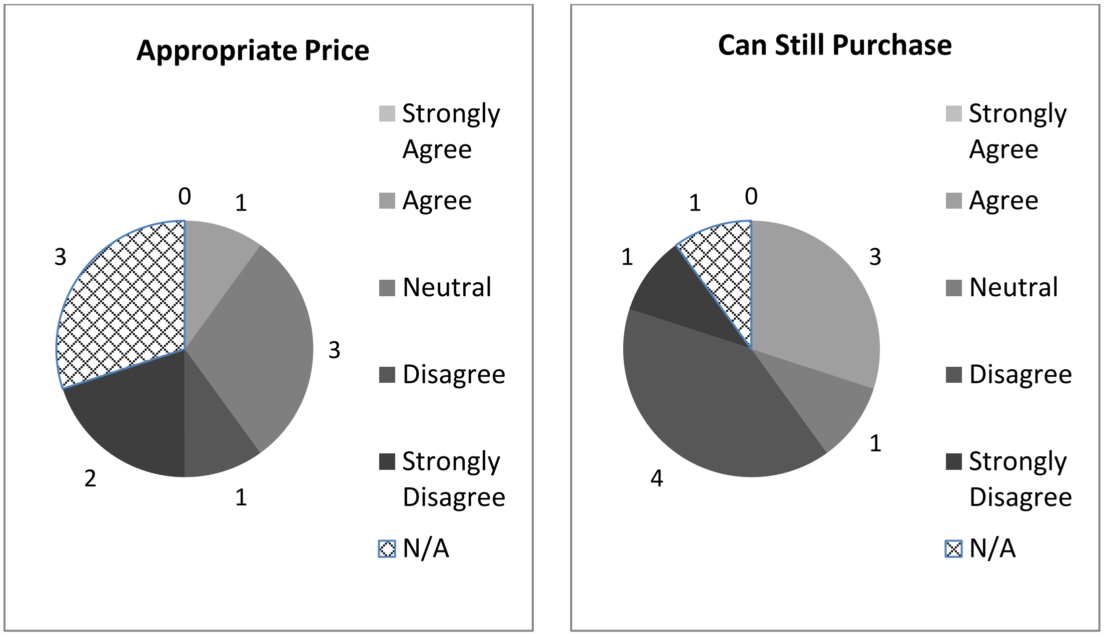


Figure 1. Frequency for Costs Sub-Variables

As *Figure 2* shows, the respondents were divided in their opinions as to whether or not their staffs were appropriately sized. Most of the respondents that felt they were understaffed employed between two and three people. Two institutions employed up to five individuals. In terms of training, half of the respondents indicated that finding staff members who were knowledgeable in monitoring software was difficult. This was further complicated by eight respondents agreeing that training was required but also indicating that monitoring software did not require extensive knowledge.

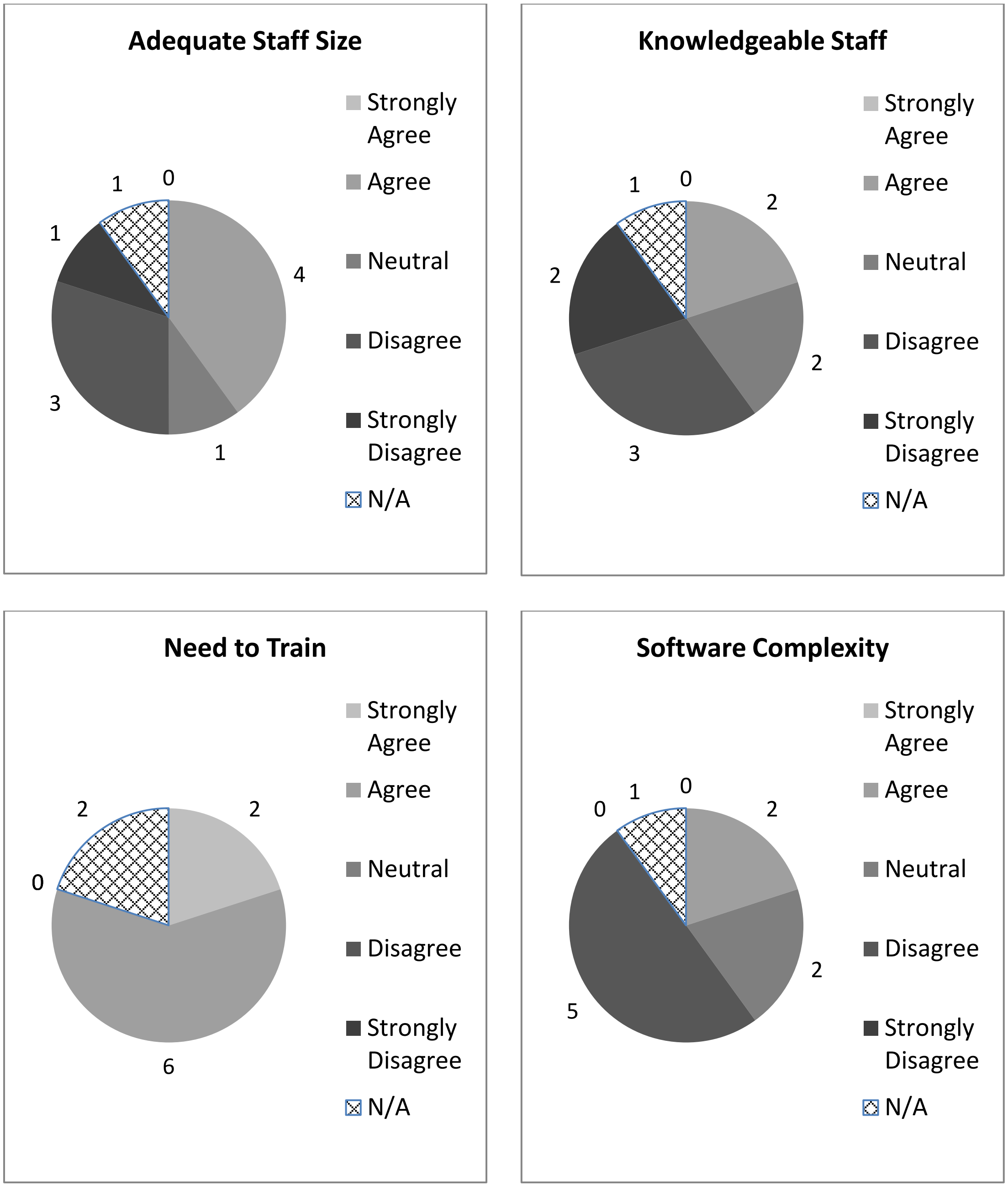


Figure 2. Frequency for Staff and Training Sub-Variables

As shown in *Figure 3*, half of the respondents stated that monitoring software generated false positives. Only one respondent indicated having experienced or thought he would experience, network conflicts when implementing monitoring software. Only two respondents stated that monitoring software cannot detect P2P traffic masquerading as a different traffic type.

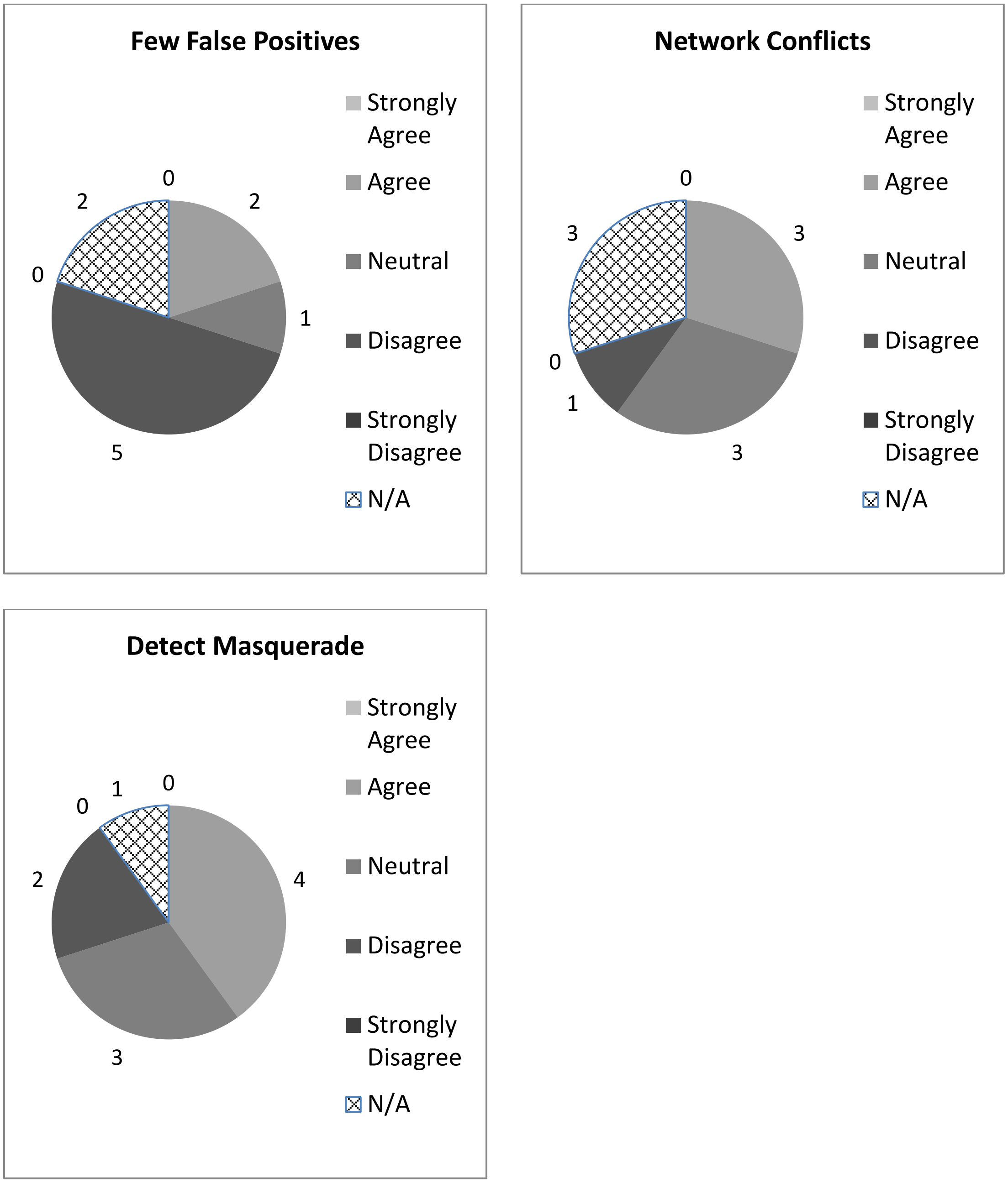


Figure 3. Frequency for Ease Sub-Variables

As shown in *Figure 4*, nine of the 10 respondents agreed that encryption was a major problem for copyright prevention. Only one respondent did not feel that monitoring software was an effective tool. At the same time, a single respondent agreed that software should make the final judgment on disconnecting a user.

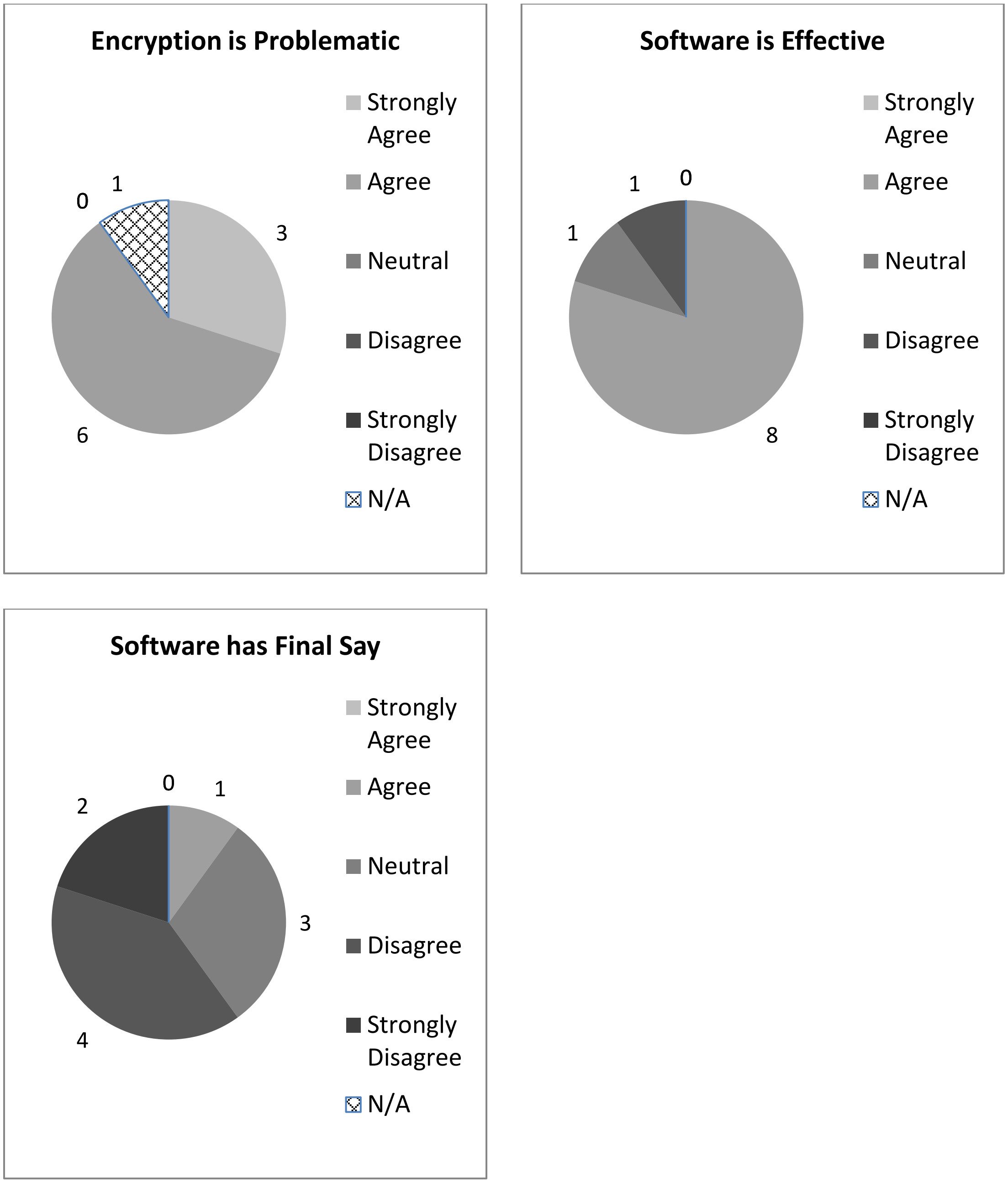


Figure 4. Frequency for Acceptance Sub-Variables

Research Question 3

3. What alternatives, if any, were considered or are currently being considered to discourage piracy by college students at a lower cost than monitoring software?

This question was used to investigate methods of combating digital piracy that were most viable in a university setting. The variables were comprised of combined 5-point Likert scale questions. Each individual question ranged from 1 (Strongly Disagree) to 5 (Strongly Agree). The combined scale for Ethics was 4-20; Legal Alternatives ranged from 3-15, and Legal Actions ranged from 2-10. These three variables were then split based on the demographics variables: Gender, Degree Earned, Participant in a Professional Organization, and Length in Position.

Table 10 displays combined scores for Ethics, Legal Action, and Legal Alternatives. The combined scores for Ethics and Legal Action show an above-average mean of 14.00 and 7.50 respectively, while Legal Alternatives is slightly above average at 9.80. The confidence intervals ranged between two and three points for all variables suggesting a fairly accurate mean.

Table 10

Alternative Statistics Unsplit

Variable	Mean	*SD*	*SE*	Lower Bound	Upper Bound
Ethics	14.00	2.108	0.667	12.49	15.51
Legal Alternatives	9.80	1.873	0.593	8.46	11.14
Legal Actions	7.50	1.780	0.563	6.23	8.77

Note: n = 10 for all variables.

When split by gender as shown in Table 11, females had higher means in Ethics and Legal Alternatives and males had higher means in Legal Actions.

Table 11

Alternative Statistics by Gender

	Male		Female	
Variable	Mean	*SD*	Mean	*SD*
Ethics	13.71	1.799	14.67	3.055
Legal Alternatives	9.57	1.902	10.33	2.082
Legal Actions	7.86	1.464	6.67	2.517

Note: n = 7 for males and n = 3 for females.

As indicated in Table 12, Ethics and Legal Actions were identical between Bachelor's and Master's degree holders. The differences between means for Legal Alternatives, the only variable that was not equal, were so minute that they could be considered equal as well. This implied that the type of degree earned did not affect the views of respondents on these topics.

Table 12

Alternative Statistics by Degree Earned

	Bachelor's		Master's	
Variable	Mean	*SD*	Mean	*SD*
Ethics	14.00	2.309	14.00	2.191
Legal Alternatives	9.75	2.062	9.83	1.941
Legal Actions	7.50	1.915	7.50	1.871

Note: n = 4 for Bachelor's and n = 6 for Master's.

Table 13 indicates non-participants were more in favor of Legal actions, while participants were more in favor of Ethics and Legal Alternatives. The differences, however, were not significant.

Table 13

Alternative Statistics by Professional Organization

	Participant		Non-Participant	
Variable	Mean	*SD*	Mean	*SD*
Ethics	14.29	2.430	13.33	1.155
Legal Alternatives	10.00	1.915	9.33	2.082
Legal Actions	7.14	2.035	8.33	0.577

Note: n = 7 for participants and n = 3 for non-participants.

Table 14 shows minor differences, if at all, between the three variables when organized by length in position.

Table 14

Alternative Statistics by Length in Position

	3-6 Years		10-15 Years	
Variable	Mean	*SD*	Mean	*SD*
Ethics	14.40	2.608	13.60	1.673
Legal Alternatives	9.80	1.095	9.80	2.588
Legal Actions	7.40	2.408	7.60	1.140

Note: n = 5 for 3-6 years and n = 5 for 10-15 years.

Sub-Variable Frequencies

The following section explores the sub-variables that comprise the three variables in this section. Figures support narrative discussion regarding each of the variables.

Figure 5 shows that all of the respondents stated students would resort to P2P once they left the restrictions of the university campus. Additionally, nine of them believed that students had little concern over the consequences of their actions. As to whether ethics would help stem piracy, the respondents were divided with four agreeing, five disagreeing and one remaining neutral as to whether ethics would help stem piracy. In regard to its impact on monitoring software, four respondents agreed and six disagreed that such action would lessen the need for monitoring software.

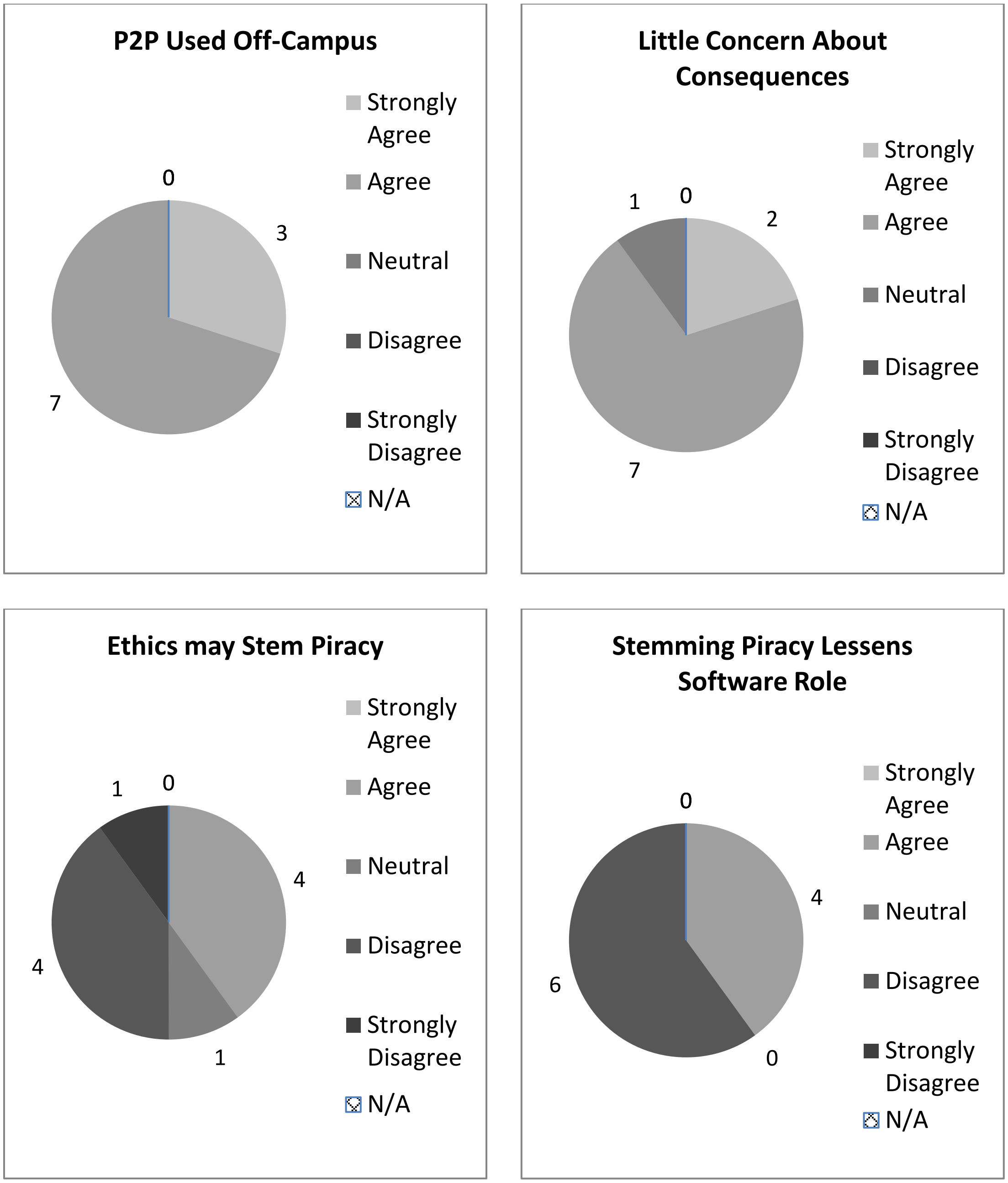


Figure 5. Frequency for Ethics Sub-Variables

As seen in *Figure 6*, the respondents were divided in regard to whether legal alternatives such as downloads would encourage students to obtain goods via legal means. Seven of the IT security directors, however, believed that having more legal means of obtaining goods would decrease the need to find them illegally. Four respondents stated that their institutions were in the process of obtaining means of providing discounted goods. Five remained neutral on the issue.

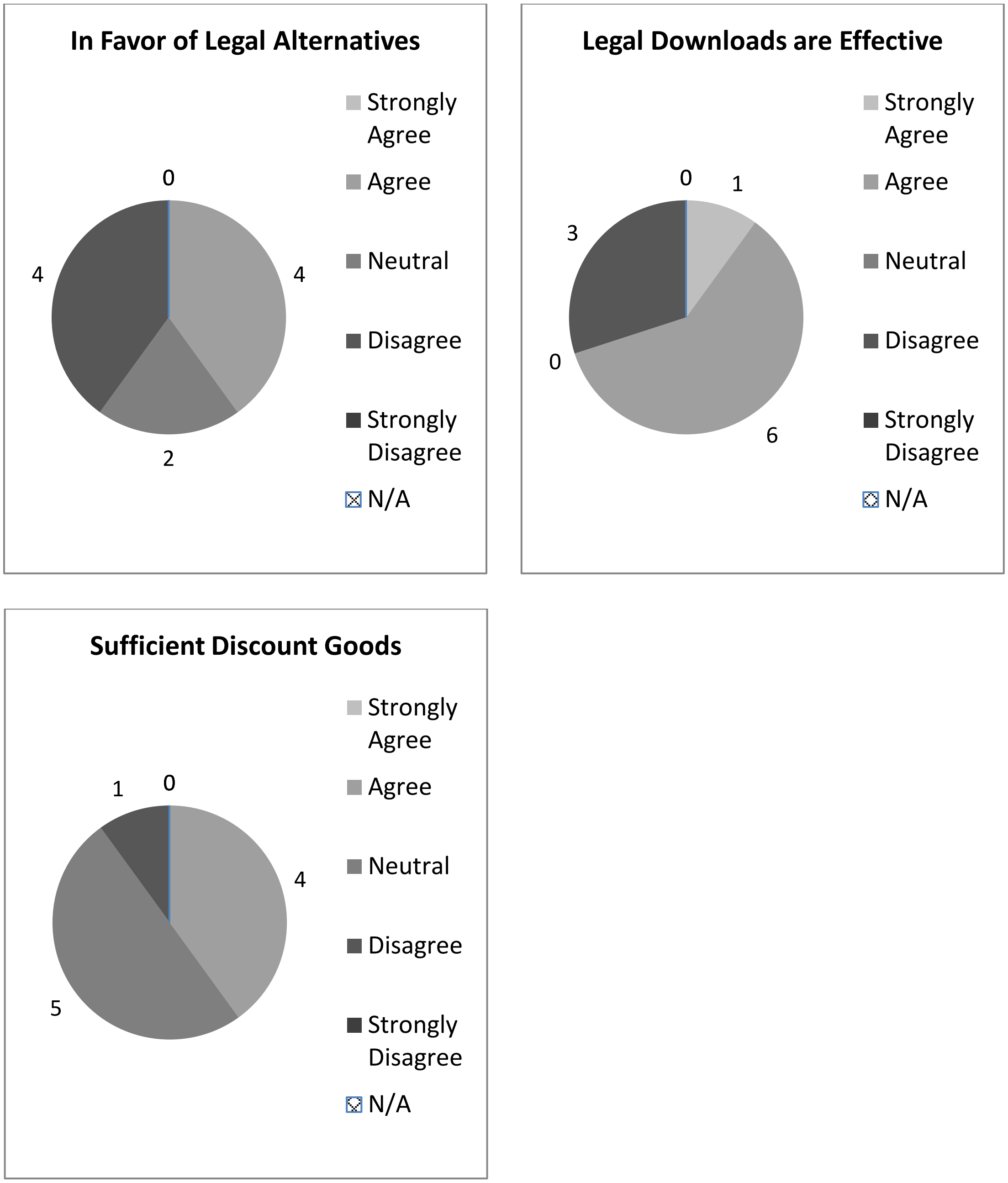


Figure 6. Frequency for Legal Alternatives Sub-Variables

Finally, as shown in Figure 7, six of the respondents agreed that repeat offenders were rare occurrences. All but two agreed that students care more about their Internet connections than the act of piracy itself.

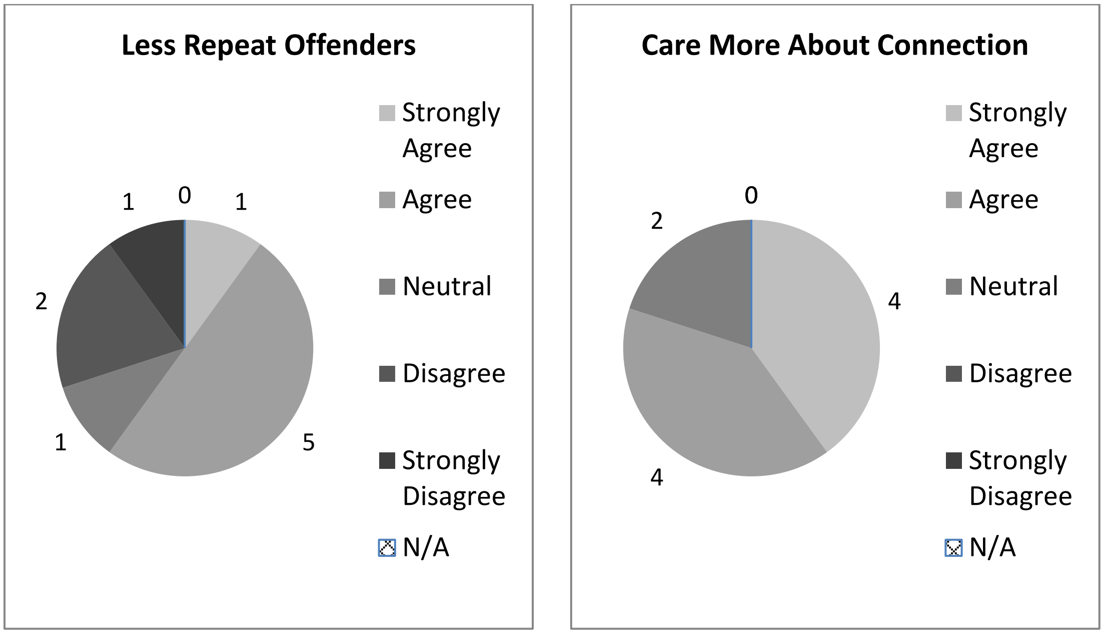


Figure 7. Frequency for Legal Actions Sub-Variables

CHAPTER 5: DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

In this chapter, the results of the data analysis presented in Chapter 4 are discussed as they relate to the literature review, and the findings are summarized. Implications for practice, policy and future research are prior to concluding the chapter.

Discussion

This section further explores the results of the data analysis presented in Chapter 4. The discussion has been organized around the three research questions which guided the study.

Research Question 1

This research question sought to determine how new policy changes would affect the 11 Florida State University System institutions. Only two of the institutions used the software that was described by the Common Solutions Group (2008), and one of the two utilized two of the programs in different areas. cGrid works to flag rogue network connections for the IT professionals to handle rather than automatically disconnecting upon detection. The one “other” response utilized BlueCoat Systems which is a packet monitoring software similar to cGrid (Nyiri, 2004). Although the majority of the institutions did not utilize content monitoring software packages similar to Copysense, they could be utilizing comparable packages but did not treat them as “content monitoring software.” On the contrary, one institution stated, when contacted for the study, that students were not monitored.

The results as to whether the Higher Education Act revision has an impact on the institutions were as expected by the researcher. If the institution already had a plan in place, the only reason to change it would be if the system no longer functioned as intended. Furthermore, most of the institutions’ networks had been designed in such a way that if a change were made, there would not be a heavy impact on the functionality of the rest of the network. Putting these two variables together, it could be implied that the universities in the SUS were properly prepared for the revision.

Server-banning policies were also investigated to determine how an institution handled a non-P2P piracy situation. One institution banned student servers in order to prevent outside network attacks. If a student were to run a server with poorly maintained security, it would become an easy attack vector for a hacker to penetrate the network and cause extensive damage. Another institution only banned servers in student housing for the aforementioned reasons. This means that students could run servers in other parts of the campus--potentially under the supervision of a network expert. These results were in line with those of Joachim (2004), where servers were banned at institutions even though companies such as Yahoo and Google began as student-run dorm servers. From the time Yahoo and Google started to the present, however, the Internet grew significantly. This makes issues such as network security and network load larger problems than they once were.

Six institutions reported using active monitoring strategies that involve locking down computers when P2P connections or any other harmful activity were detected. These policies also give the user between one and three “strikes” of increasing severity. This is the type of monitoring policy typically discussed in the literature (University of Central Florida, 2009; Michigan State University, 2009). Two institutions utilized more passive methods in which the institutions did not actively monitor for P2P connections and only reacted if notified via DMCA or another source. In essence, this places the students on an honor system, but any infringement treated as a single strike policy. One institution uses a hybrid policy that places a software key on the computer that monitors for P2P programs and activities. Students must accept the key before being able to connect to the network. If students are detected, their connections are locked until the offending programs are removed. This provides a way for students to be policed in a way that relieves the IT staff of some duties.

Research Question 2

The second research question was used to explore the challenges in implementing and maintaining monitoring software. There were 13 items (sub-variables) divided into five groups (variables). All but one of the items (staff size) were Likert scale items and were added together to form a combined scale. Costs and Staff were around the midpoint of each scale, with the other three variables were slightly above the midpoint of their respective scales. Even after dividing the data among four demographics (gender, highest degree, whether or not they were part of a professional organization, and length in position), the combined scales did not deviate much from the combined version. The only notable exception was the Ease variable by length in position. Those who were in their positions longer believed the programs were easier to work with than did those who were newer to their positions. This could be caused by IT personnel having experienced programs that were less user-friendly earlier in their careers. Also, the small sample size is likely to have had an impact on some of this phenomenon, particularly since one respondent responded "N/A" for the majority of the questions that applied to this section.

When looking at the individual items on the survey, the data becomes considerably more meaningful. For the two items that comprised the Costs group in *Figure 1*, the majority of respondents disagreed that monitoring software was affordable and purchasable. This reaction is in agreement with the warnings of

Worona (2008) who expressed concern over the high price of monitoring software in the current economic climate. In the case of the Florida universities, the majority of the institutions already had some provision in place, but depleting budgets could hinder future upgrades and replacements.

Staff and maintaining a properly trained staff is another part of the financial burden. While it was agreed that the software's use was straight-forward, the perception was that new staff would still require training in order to properly operate it. Also, despite the fact that the initial cost of the software is a single occurrence, staff members are long-term investments. Most of the respondents who stated they did not have an adequate staff size had between two and three people who would utilize the software in some capacity.

Though the cost of the software is one problem, the reliability of the software is a different issue. Most of the respondents agreed that their solution generated false-positive situations (a case where a condition is believed to be true when it is not) when monitoring. This acts as a measure of the overall worthiness and value of the software. As discussed in the theoretical framework, the more erroneous or missed detections, the less valuable and reliable is the software (Wallach et al., 2008). Contrary to what the Common Solutions Group (2008) and the EFF (2006) believe, some campus networks can detect masquerading data. This implies that the software, while functional, may not be the most reliable tool available to the IT department, and it may take time to develop a suitable replacement.

Wallach et al. (2008) stated that one of the most important components of software ethics is the trust put into the software. The Acceptance variable was used to explore situations that would make the monitoring software seem less useful and more of a burden to the IT professionals. Respondents overwhelmingly agreed that encrypted connections will always prove problematic in preventing piracy. This was in agreement with warnings from researchers and authors (EFF, 2006; Nyiri, 2004). At the same time, the IT directors indicated they agreed that software monitoring was an effective tool for combating digital piracy, but generally disagreed that software should make the final decision. As Friedman and Kahn (1992) and Stahl (2004) discussed, a computer may only emulate ethical behavior. Furthermore, the emulation is only as good as the programming. Thus, it could be implied that these types of programs are not mature enough to make their own decisions without the intervention of an IT professional. These findings may appear to be contradictory, but it really reveals how much trust the IT professionals have in the systems. Although the software has been effective at performing its task, it has not proven effective enough to be granted total control over the networks. This is congruent with the expressions regarding the evolution of piracy prevention software by the Common Solutions Group (2008).

Research Question 3

The third, and final, research question was used to examine the viability of other methods compared to current procedures. This included expanding the teaching of ethics in the classroom, providing more legal alternatives to illegally downloading material such as discounted software, and the current process of legal actions which include DMCA notices and student disciplinary action. These three sections were made into variables comprised of four, three, and two questionnaire items respectively. As shown in Chapter 4, each of these combined responses resulted in above-average scores for their respective variables. This could easily provide support for a second form of intervention beyond monitoring. When the data were divided among the factors of gender, degree earned, membership in professional organizations, and length in position, the differences were minor and varied little from the results of analysis of the aggregated data. This implied that the chosen factors had little effect on these fields.

All participants responded to the items in this section completely and without use of the “Not Applicable” response, making the responses for the three variables more reliable. The first variable in question was the Ethics variable. It combined the opinions of a student’s potential unethical behavior with opinions about ethics as a solution. The responses for the two variables related to student behavior were almost unanimously agreed upon. All of the respondents felt that students would begin using

P2P once they were out of the limitations placed by the institution. Furthermore, all but one respondent agreed that students had little concern over the consequences of digital piracy. Unfortunately, this type of behavior relates directly to findings from LaRose et al. (2005) and situations such as the Tenenbaum Trial (Anderson, 2009a, 2009b). Even with all of the security measures in place, the students viewed it as a temporary block until they reached a site where they could download. All of the respondents had strong feelings about how strongly students will act with and without P2P restrictions, but they were divided in regard to the effectiveness of ethics as a tool to combat piracy. Considering the majority of the researchers who had focused on student ethics advocated for it in some form (Cronan & Al-Rafee, 2008; LaRose et al.; Taylor et al., 2009), this response was surprising. At the same time, ethics has not been perceived to be a stand-alone measure. It is possible that the responses acquired in the present research reflect this viewpoint. Colleges and universities have been known for teaching ethics and values to students as well as providing traditional academic curricula. Considering that digital piracy is an ethical issue, the fact that students refuse to change their opinions on the matter is somewhat alarming. Universities may need to consider treating digital piracy in a fashion similar to other popular educational topics such as drinking.

Respondents were divided in their opinions as to whether providing discounted legal goods would serve as a deterrent to piracy. Although researchers have found that some pirates illegally download in order to act out against the larger corporations, many simply pirate for the sake of pirating or for social reasons (Einav, 2005; Higgins, 2005, 2007; Higgins, Fell et al., 2006, 2007). Since discounted legal goods may account for only one of these groups, it could explain the diversity of opinion in the data. When looking at legal downloads from a perspective of simply cutting down piracy, most of the respondents were in agreement. This could be attributed to a belief that anything that could reduce piracy would be effective to some degree. With some companies providing free or heavily discounted software, e.g., Microsoft providing students Windows 7 for $30 for a limited time, or Adobe providing student-license versions of their products which provide the same product at 80% of the cost, students who may pirate these programs for their personal use may reconsider. Those who pirate for the sake of pirating will not be likely to be impacted by such options. Finally, the respondents were divided in their opinion as to whether a sufficient number of goods were available at discounted prices would impact on decisions to pirate. This difference could be dependent on the number of goods the institutions offered. In the case of the neutral and disagree responses, this could be a signal for these institutions to look into potential arrangements such as that of Pennsylvania State University with Napster or the provision of discounted goods such as those available from Microsoft and Adobe.

Finally, the impact of Legal Actions on piracy was examined. Most of the respondents agreed with the concept that students cared more about losing their Internet connections than any legal consequences that may result from the infraction. This also linked directly to respondents' perceptions that students had little concern over the consequences of their actions. This finding provided further support for teaching students more about the ethics and consequences of digital piracy and illegal downloading. Students who were caught downloading illegally tended to avoid a subsequent offense at the majority of the institutions. Although a student not involved in a second offense is a positive notion, it is unclear if the student truly learned anything from what transpired. The student could as easily have decided to go off-campus for any P2P needs, counteracting any teachings from what transpired. Since there is no way to track students after they leave the campus, finding a method to address this situation would be difficult.

Significant Findings

The majority of the findings in the study were as anticipated. It was anticipated that at least two of the institutions interviewed used one of the programs listed in survey item one because cGrid/ICARUS was developed by the University of Florida (Joachim, 2004). What was surprising, however, was that the majority of the institutions did not utilize a content monitoring program. It is possible that these institutions utilized other methods not mentioned on the survey instrument--namely packet shaping. Since packet shapers only look at the type of traffic flowing, they are not considered content monitoring programs. What makes packet shaping programs more powerful than content monitoring software is that their use extends beyond detecting copyrighted material. The monitors look at the packets of data going through the network and identify programs by the patterns of packets sent through the network. Thus, the students would have some form of privacy while the IT department can watch for malicious programs across all regions of the network. Regardless, even if alternate methods to content monitoring software are used, the EFF (2006) has stated that there are ways around any method. Another significant finding involved the level of preparedness the institutions showed. With the exception of one institution, all of the institutions appeared ready or unfazed by the requirements of the 2008 revision to the Higher Education Act. In a sense, it showed that the legislation is a moot point for at least the universities in the Florida State University System. Most institutions have already implemented policies for P2P transactions, and the law is just there to prevent the institutions from backing away from the legislation. This scenario also helps further the notion that associations such as the RIAA are trying to push their private agenda into the public realm.

For the different policies each of the 10 institutions use, the most interesting one is the institution that uses the policy key. This could potentially be a method that allows the students more freedom and a sense of privacy while the campus can still maintain an active watch for illegal activities. Active monitoring is still an effective technique, but a passive method may give students less of a sense that there is someone monitoring their activities.

The reaction the institutions had in regard to the costs of monitoring software was as expected. It fit with the ideas of the EFF (2006) and the Common Solutions Group (2008) that the software is too pricy for what it really does. Though this will not affect the software that the institutions have already purchased, they will eventually need to purchase either a new version of the current software or a fresh program that just appeared on the market. When this time comes, there is no guarantee that institutions will have the same budget that they have today and most likely will be have smaller ones. Between shrinking budgets and increasing software prices, the institutions may encounter further problems unless one of the two factors changes. The other problem with implementing new software comes from staff training. It is already difficult to find knowledgeable staff for the IT department, and any new personnel would still need to be trained to use the software. Most of the IT personnel stated that the software was not complicated, but training new personnel or the entire department in the case of a new program would still cost time and energy. Green (2008) stated that some universities can spend around $500,000 annually between software licenses and staff members on P2P compliance alone.

Perhaps some of the most surprising outcomes for the second research question came from the questions in the ease grouping. Most of the respondents stated that their monitoring techniques make mistaken judgments more often than 'rarely,' which damages the accuracy of the products or techniques being used. Though no method will ever be perfect, it does mean that there could be a greater risk of someone being detected by mistake or someone sneaking through the defenses. On the note of detection, some institutions can discern P2P traffic if it masquerades under different ports. Considering masquerading was described as one of the major workarounds to P2P blocking, knowing that some setups can detect such a phenomenon leaves pirates with one less technique to use. Encrypted connections, however, still pose a major and potentially unsolvable problem. Taking into account that all of the respondents, with the exception of one "not applicable" response, were in agreement as to this problem, it can be concluded that sneaking through encryption channels will always play a major role in the digital landscape. Most of the institutions did feel they used an effective solution despite any potential glitches and oddities that may occur. Since numerous authors addressed ethics as a major component in the digital piracy solution, this stance is somewhat surprising. At the same time, one may venture to say that monitoring provides an appropriate short-term prevention method. As expected, however, most of the institutions disagreed with the notion of the software making the final call on any decisions. This indicated that monitoring software, while considered to be effective, is not ready for operating autonomously in users' minds. Given the flaws in detection, this is to be expected. It also helps support the notion by the Common Solutions Group (2008) that this type of software still has a long way to go before it reaches a truly trustworthy level.

The notion of monitoring software acting as a short-term solution was further supported by the findings in the ethics-based item. The institutions were unanimous about students utilizing P2P off-campus outside of the eye of the software, and that students held little concern over the consequences about piracy. This would imply that in the long term, software has been relatively ineffective in changing the habits of students. What was surprising, however, was the division of the IT directors in regard to the use of ethics in preventing piracy. Considering that many authors advocated for the importance of ethics, the Florida SUS division of opinion was unexpected. It could mean that though considered to be important, ethics has not had the intended impact that the researchers were expecting (Cronan & Al-Rafee, 2008; LaRose et al., 2005; Taylor et al., 2009). It could also mean that implementation of ethics in an institution is difficult and may be costly in the long run. Considering that most of the solutions used to combat piracy have not been directed to content monitoring, the disagreement with the role of software being lessened makes sense. There are still other security issues prevalent in a campus network such as network attacks through open ports that the current solution still combats.

In regard to the use of discounted products or legal downloads, the disparity of opinion as to legal downloads effectively reducing piracy and the similarly divided results of providing legal alternatives as a solution to piracy appear to be odd results. In actuality, this could be classified as supporting the notion that while the solution may not be an ideal or effective one, anything that could potentially reduce piracy is better than nothing. Finally, the few respondents who stated that students often repeated the offense of digital piracy was unexpected. There always will be students in any institution like Tenenbaum who will never learn, but this may also imply that the respondents in question have a larger student population to handle.

Implications for Practice and Policy

Having presented a general overview of how the Florida SUS has dealt with digital piracy situations, one can identify several areas in need of improvement. Though ethics may be one of the keys to solving the piracy problem, teaching ethics may be problematic. One institution banned servers after their numbers became problematic. There were teaching attempts, but those attempts did not get through to the students. If an ethics program is constructed, it must be able to do more than simply inform about ethics. In most cases, informational intervention tactics are the easiest to conduct but are the least effective. At the same time, ethics is neither tangible nor concrete. This forces the material to stay in an informational state and be open for interpretation. As shown in the review of the literature by Edgar (2003) and Johnson (1994), ethics can take a variety of viewpoints, and while one could easily explain the ethics of why piracy is wrong, another person can use a different theory to show that it is acceptable. Even when narrowing the discussion to computer ethics, there has been considerable debate on the proper way to handle ethics. One potential solution to this conundrum involves combining both applied computer ethics and theoretical ethics. By blending the two types of ethics together, a better understanding can be achieved. Theoretical ethics provide the basis for why piracy is perceived as immoral while the applied computer ethics provide a way to show how the concepts work in a real-world situation. Considering that there are a plethora of ethical theories, by selecting the theories that best highlight the viewpoints of both sides of the piracy debate students could understand pros and cons to the reasoning behind the pirates and the corporations. This may also lead to students obtaining a better understanding of the issues behind piracy and allow them to make more educated decisions when they encounter a piracy situation.

As with Florida educational facilities in general, more funding should be allocated to the technological requirements of piracy prevention. As institutions become more financially burdened, many departments will feel the pinch. Either departments need to think ahead for future purchases, or the legislature needs to allocate more funding. Although the current methods of digital piracy and P2P prevention are functional today, technology moves at an increasingly fast pace and P2P or its inevitable successor will find its way around the current system. Rumors do exist that heavy P2P may at least be temporarily halted when the IP address system makes the inevitable transition from the current four-number system (IPv4) to a six-number system (IPv6) in order to accommodate the increasing number of Internet devices. This transition will have major effects on the entire Internet and could easily render some products obsolete if they are not designed with the new system in mind. If IT departments are not financially equipped to keep up with the changing technology, regardless of the effects of piracy, campuses could easily be dealt a major blow to their networks. At the same time, there is also an opportunity for the institutions to become innovative. Considering that the University of Florida developed the cGrid/ICARUS system to monitor data packets (Joachim, 2004), there may be opportunities for other institutions to follow suit. Knowing that there are certain problems with their current software, IT departments and academic departments such as computer science could work together to design more effective programs. While the notion of hiring students for such a task may seem counterproductive, there are other students who wish to go into computer security and are less likely to be considered pirates. Hence, heavy scrutiny should be taken if students were hired to assist. If the project is funded by a grant, it would also help alleviate any costs of employing extra personnel. In this instance, the institutions would have the ability to solve their problem in-house.

The final area that could be changed is the private sector's view on piracy itself. A number of authors provided models that show how profit could be made in light of piracy. Furthermore, groups such as the Electronic Frontier Foundation, Creative Commons, and authors such as Lincoff (2008) feel that the nature of the current copyright laws is to blame, and are in dire need of a change. Though copyright reform is a current hot topic, changing the rules behind copyright will not change the fact that unauthorized copies are illegal. Artists and publishers may gain the abilities to waive some of these rights if they choose, but the portions of the copyright that remain will continue to be honored and enforced in the traditional manner. Another area of possible reform is related to convincing organizations such as RIAA and MPAA to give up their current business models that are becoming increasingly dated in light of digital downloads and adopt newer practices. Much of the research presented shows sectors such as the recording industry more adamant to change even though digital piracy actually leads to artists obtaining increased revenue from concert sales at the expense of decreased album sales (Dejean, 2009; Duchêne & Waelbroeck, 2006; Gayer & Shy, 2006; Hui & Png, 2003; Liebowitz, 2004; Ouellet, 2007). Sectors such as the movie industry may have begun to consider alternate ways to maintain a profit in light of piracy with the increase of major films presented in

IMAX format, 3D, or both. These alternate movie formats present the films in a way that a bootleg recording and computer monitor cannot accurately capture. Thus, a person may pirate a film but still go to the theatre to get the full experience. Considering the broad scope that digital piracy encompasses, there are a number of ways the problem could be mitigated. Any of the proposed solutions could help on one of the many fronts, but each one only solves a certain part of the problem.

Implications for Future Research

As a new branch of piracy research, a number of different directions could come from this research. First and foremost, this study was of a general and broad nature, so focusing further into any of the topic areas would provide deeper insight into the problem. This could include studies that involve both student affairs and IT departments to get actual disciplinary numbers in order to compare identification rates between different methods and institution types. Student ethics could also become an area of research. If students could be taught and properly convinced that piracy is morally wrong it would help in its reduction. More specifically, a study on methods of delivering student ethics to an institution would help pave the way for new programs. Research into the inner workings of content monitoring software is also an important route to look at. By comparing the intricate details of what each program does and its overall effectiveness in identifying potential copyright infringement, more effective software could be developed.

In 2010, another type of digital media became important to control in the eyes of the university, textbooks. Because textbooks are typically written by professors, piracy now has a direct effect on institutions of higher education. While students have been a heavily studied population, one potential future study may explore if any differences exist between students wanting to pirate media and wanting to pirate textbooks. This could also help determine if pirates are more prone to illegally download entertainment or anything that is available to them.

One of the more obvious routes for future research involves expanding the scope of the present study. This study focused only on the public universities in the state of Florida. Because only one type of institution was observed, future research could easily explore the workings in other types of institutions such as private institutions. It should be noted, however, that community colleges may not be the best group to study. Based on information gathered from the pilot study, Florida community colleges are commuter institutions only. Therefore, their policies and practices differ greatly from institutions where students live on campus. Some community colleges in other states, however, do have on-campus housing, so with the proper precautions community colleges could still be used in a broader study.

A larger population of institutions should also be considered in future research. With only 10 institutions as a population, the results of this study were not generalizable at all. The small number of institutions also impeded the use of any non-descriptive statistical tests. By expanding the scope to at least a region, a more robust sample could be obtained. Using a larger sample would yield better and more generalizable results. It may also make the demographics portion more statistically relevant. At the same time, a larger sample will require more resources and the high response rate of this study will not be guaranteed.

The survey instrument itself could benefit from improvements in some of the areas. Based on the way the question about the type of content monitoring software used was answered, some changes would be indicated. Either that question should become a free-response section to allow respondents to describe the solutions they use, or it should be altered into different types of solutions such as content monitoring and packet shaping.

Another potential addition is the frequency of receiving DMCA notices. One respondent mentioned that they received approximately one a week. This type of information would be useful if all the institutions provided it. Another potential addition would be an item on the institution's ranking as a pirating school. Some institutions will be more prone to pirating activity than others, and this could easily be a demographic variable to consider and determine if certain solutions work better for schools of certain sizes and base levels of piracy. Although these variables could have been added to this study, the demographics would make the institutions easily identifiable, violating privacy conditions established for the study.

While this study explored student piracy from the IT perspective with students in mind, administrators and faculty are equally at risk of pirating material intentionally or not. Exploration into other education-related copyright policies such as the TEACH Act would further support whether or not a need for copyright reform is truly needed in American culture.

Conclusions

Digital piracy is a problem that may never disappear from society. As long as people want to obtain music, movies, and software without paying for it, there will always be someone on the Internet to provide it. Furthermore, colleges and universities will always be one of the major outlets of digital piracy because of their advanced network resources. Through these resources, students can obtain access to copyrighted material at speeds faster than they could at their homes. Despite digital piracy being a global phenomenon, a combination of the extensive resources and the typical college student's lack of funds makes it more lucrative for a student. Even before programs such as Napster made the act of piracy relatively easy, the type of student who would engage in piracy remained generally unaltered. According to previous studies discussed in the literature review, pirates have always been predominantly computer-oriented majors or students with a high level of computer knowledge.

The students themselves will choose to pirate for a number of reasons. Some will pirate to obtain the digital goods without having to pay for them, others pirate for the sake of pirating, others claim to pirate in order to “preview” the goods before purchase, and some will pirate because they feel like it would bring justice to the good’s “corrupt” parent company (Einav, 2005).

Understanding the mindset of the pirates is one challenge, and a second involves determining the best way to stop piracy. Companies have attempted to stop piracy through adding extra encoding to files which is not always effective and in some cases damages the user’s machine (LaBelle, 2006). Universities also deter students through monitoring software, packet shaping and other network-based methodologies. Unfortunately, none of these methods are perfect. Monitoring can be easily bypassed through encrypted connections, and files can be stripped of their DRM schemes. The recording industry attempted to push litigation in 2003, but the threat of legal action did not deter the determined and only caused the pirates to abandon their current methods to ones that could not be tracked as easily (Nyiri, 2004).

Students like Joel Tenenbaum who continue to pirate despite numerous warnings are prime examples of those who are not fazed by legal threats and will continue to download even after the RIAA apprehends them (Anderson, 2009a, 2009b). It demonstrates a lack of ethics in college students towards the concept of illegal downloading being considered as stealing. Even though students may receive DMCA notices and warnings, students may still feel that downloading is not stealing. This situation calls for reconsideration of teaching computer ethics; however, deciding on an appropriate set of ethics and method to teach them is consistently up for debate making the entire process difficult. Furthermore, there is also the consideration that while piracy is illegal from any angle, the corporations may be pushing some aspects of the issue too far. Many companies claim that piracy caused a loss in sales, such as the software industry reporting a loss of $13.08 billion and the recording industry losing $4.6 billion in 2002, but there is proof that these figures may be exaggerated by people would never have considered purchasing the good and only downloaded it because it was available (Hui & Png, 2003; Liebowitz, 2004). Other researchers also demonstrated ways that business models could be altered to provide profit in light of piracy issues. Thus, there is still a chance that companies are overreacting to the issue.

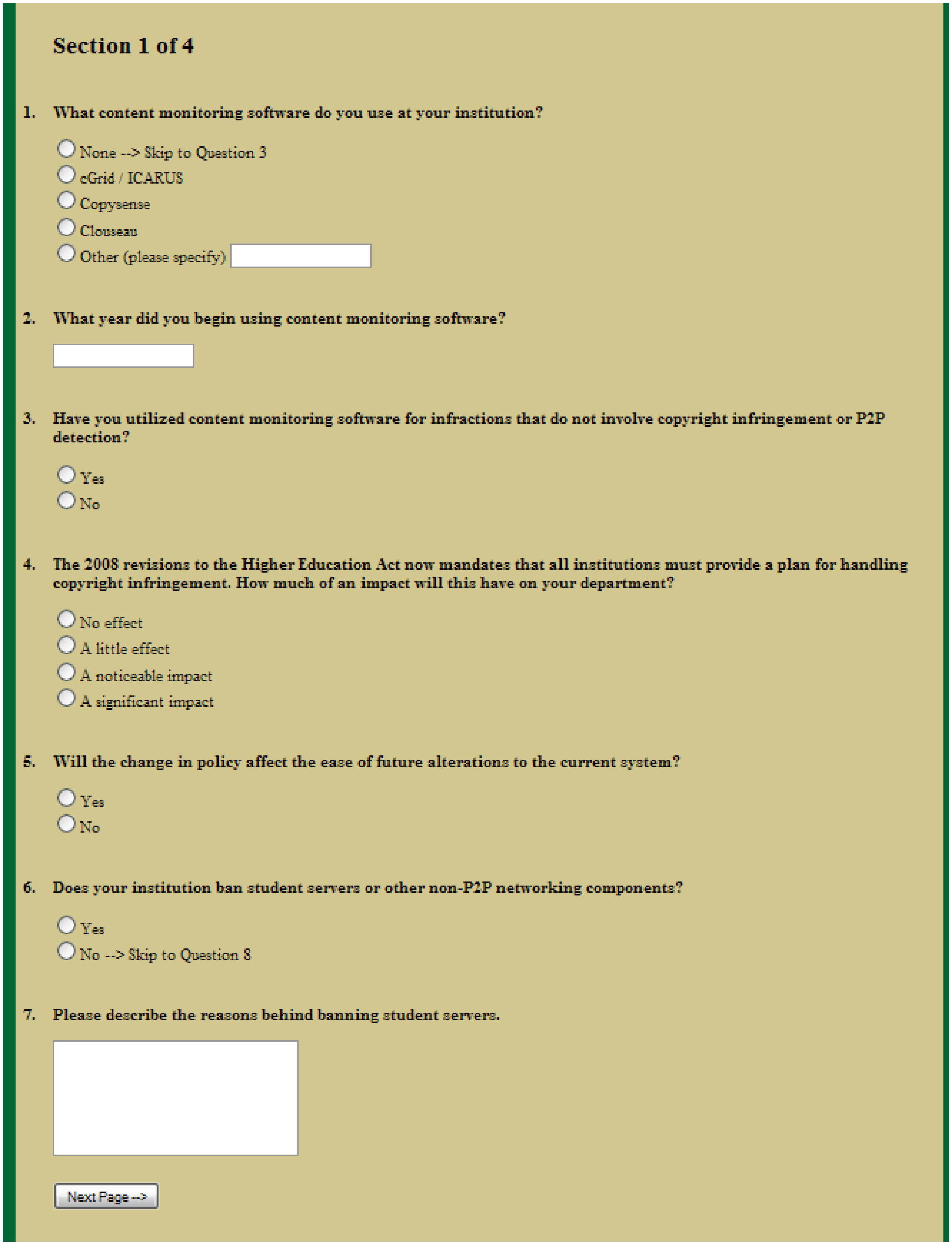
This study encompassed all of these piracy issues in a general study using 10 Florida SUS institutions. Two of the institutions share the same Internet connection.

The researcher utilized a survey instrument and policy analysis to determine the current state of each institution's policies towards digital piracy and the IT methods used to prevent it. This research was timely in light of new changes made in the 2008 revision of the Higher Education Act that has mandated all institutions to implement some form of prevention of digital piracy. By obtaining a general idea of the current state of the Florida public institutions, some initial solutions, if needed, may be derived from the study. The researcher also investigated the opinions of the institutions' representatives on alternative methods of student piracy prevention such as giving students access to digital goods at a cheaper price, implementing ethics, and preserving the traditional method of taking legal action.

At the conclusion of the study, a majority of the institutions were found to not use content monitoring software specifically but to use other software methods to prevent piracy. The institutions were fairly satisfied with these methods though they were not perfect. With that said, most of the institutions indicated they would not rely on the software to the point where it would make all the decisions. If new versions of the products came out or they needed to purchase a new product, most of the institutions would not have the proper funding to make the purchase. Furthermore, while all the institutions agreed that the majority of the students lacked concern over the overall consequences of their actions, they were divided as to the effectiveness of ethics or discounted goods over their current methods. This implied that the institutions know there is a problem but are unsure if a solution that can act as a better long-term deterrent can be implemented effectively.

With students abiding by the rules when they are on campus and disregarding them when they leave, it implied that future research should begin to look at more long-term solutions such as ethics in order to ensure that students will learn and accept the truth about digital piracy and uphold these lessons when they leave the institution. It was also implied that IT departments will need to be properly funded in order to ensure that the institutions can stay up-to-date on their systems since any of the current technology may be circumvented (EFF, 2006). Although digital piracy is a problem that will never disappear, methods to appropriately mitigate the damage do exist. Proper implementation and prevention of these methods, however, will require cooperation from all parties.

APPENDIX A
SURVEY INSTRUMENT



Section 1 of 4

1. **What content monitoring software do you use at your institution?**

   ○ None --> Skip to Question 3
   ○ cGrid / ICARUS
   ○ Copysense
   ○ Clouseau
   ○ Other (please specify) ______

2. **What year did you begin using content monitoring software?**

   ______

3. **Have you utilized content monitoring software for infractions that do not involve copyright infringement or P2P detection?**

   ○ Yes
   ○ No

4. **The 2008 revisions to the Higher Education Act now mandates that all institutions must provide a plan for handling copyright infringement. How much of an impact will this have on your department?**

   ○ No effect
   ○ A little effect
   ○ A noticeable impact
   ○ A significant impact

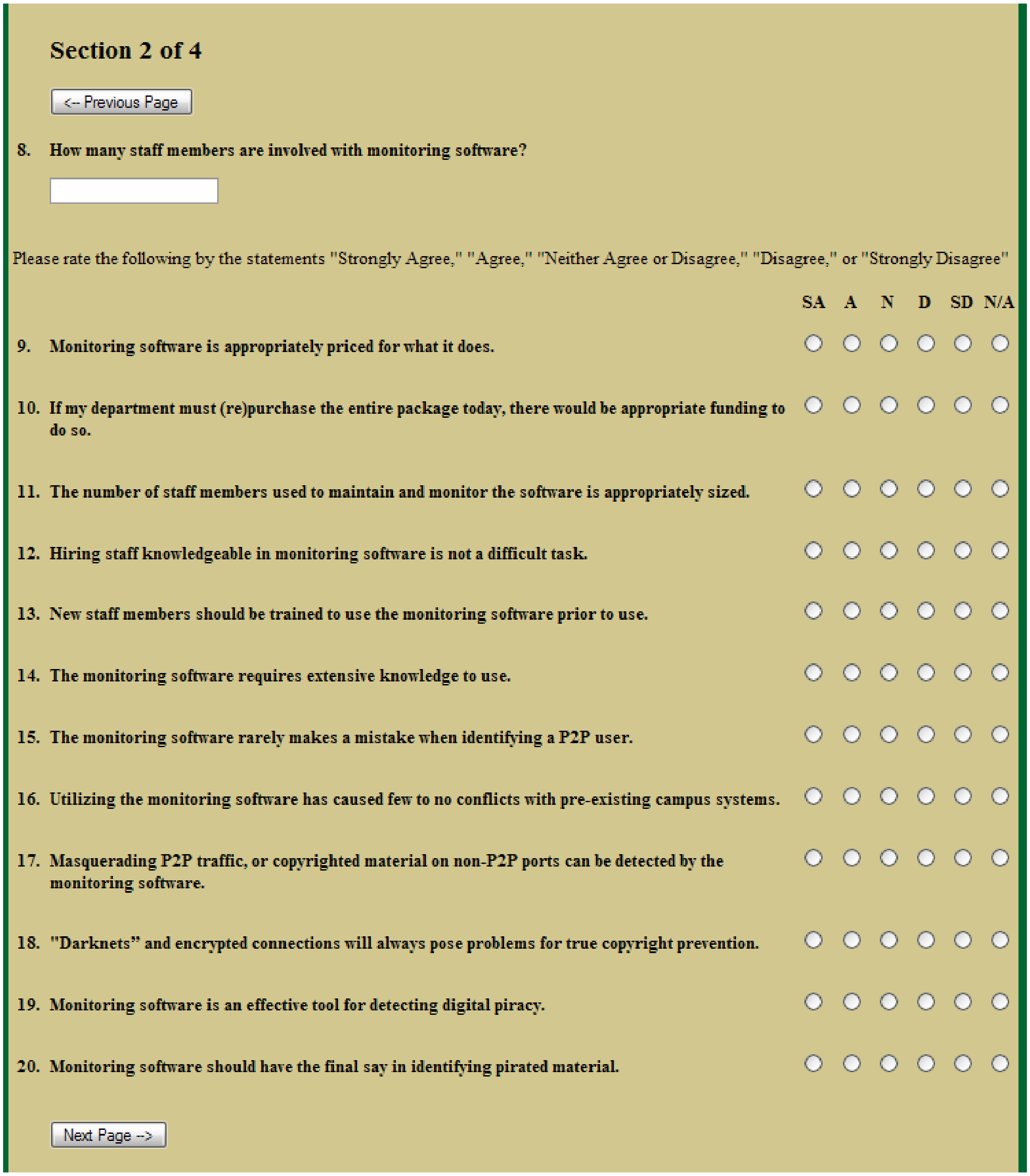
5. **Will the change in policy affect the ease of future alterations to the current system?**

   ○ Yes
   ○ No

6. **Does your institution ban student servers or other non-P2P networking components?**

   ○ Yes
   ○ No --> Skip to Question 8

7. **Please describe the reasons behind banning student servers.**

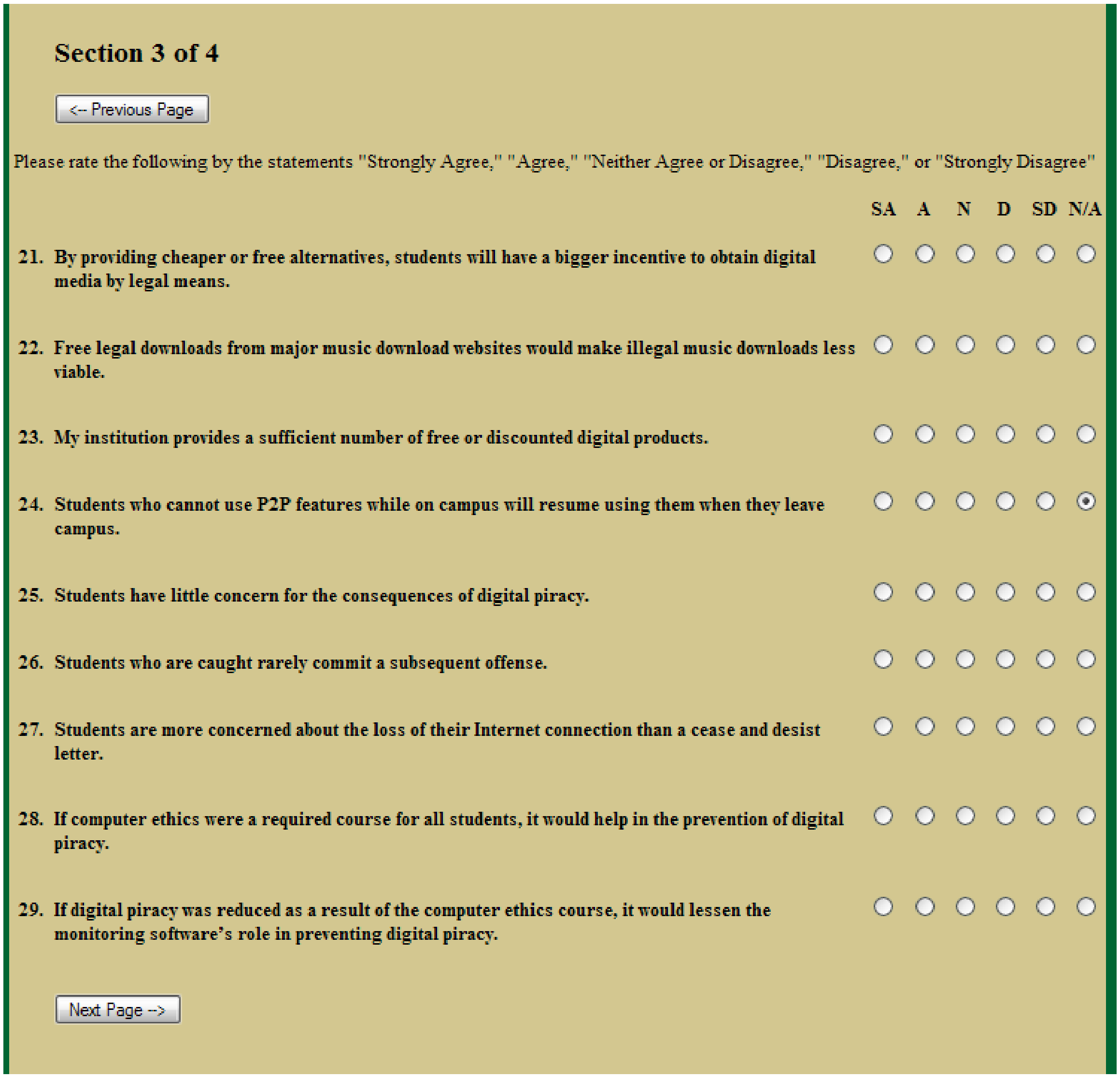


Section 2 of 4

8. How many staff members are involved with monitoring software?

Please rate the following by the statements "Strongly Agree," "Agree," "Neither Agree or Disagree," "Disagree," or "Strongly Disagree"

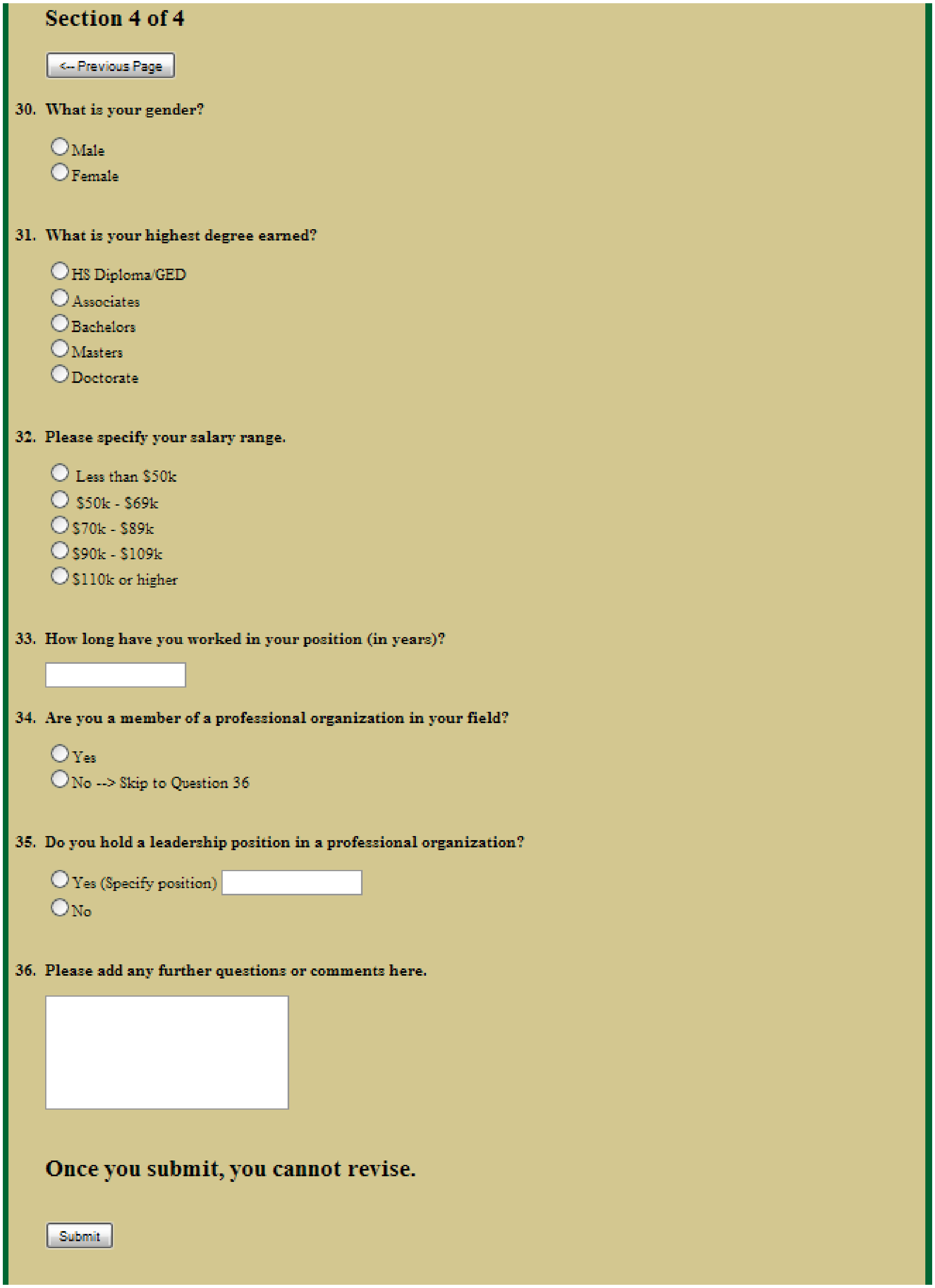
	SA	A	N	D	SD	N/A
9. Monitoring software is appropriately priced for what it does.	○	○	○	○	○	○
10. If my department must (re)purchase the entire package today, there would be appropriate funding to do so.	○	○	○	○	○	○
11. The number of staff members used to maintain and monitor the software is appropriately sized.	○	○	○	○	○	○
12. Hiring staff knowledgeable in monitoring software is not a difficult task.	○	○	○	○	○	○
13. New staff members should be trained to use the monitoring software prior to use.	○	○	○	○	○	○
14. The monitoring software requires extensive knowledge to use.	○	○	○	○	○	○
15. The monitoring software rarely makes a mistake when identifying a P2P user.	○	○	○	○	○	○
16. Utilizing the monitoring software has caused few to no conflicts with pre-existing campus systems.	○	○	○	○	○	○
17. Masquerading P2P traffic, or copyrighted material on non-P2P ports can be detected by the monitoring software.	○	○	○	○	○	○
18. "Darknets" and encrypted connections will always pose problems for true copyright prevention.	○	○	○	○	○	○
19. Monitoring software is an effective tool for detecting digital piracy.	○	○	○	○	○	○
20. Monitoring software should have the final say in identifying pirated material.	○	○	○	○	○	○



Section 3 of 4

Please rate the following by the statements "Strongly Agree," "Agree," "Neither Agree or Disagree," "Disagree," or "Strongly Disagree"

	SA	A	N	D	SD	N/A
21. By providing cheaper or free alternatives, students will have a bigger incentive to obtain digital media by legal means.	○	○	○	○	○	○
22. Free legal downloads from major music download websites would make illegal music downloads less viable.	○	○	○	○	○	○
23. My institution provides a sufficient number of free or discounted digital products.	○	○	○	○	○	○
24. Students who cannot use P2P features while on campus will resume using them when they leave campus.	○	○	○	○	○	●
25. Students have little concern for the consequences of digital piracy.	○	○	○	○	○	○
26. Students who are caught rarely commit a subsequent offense.	○	○	○	○	○	○
27. Students are more concerned about the loss of their Internet connection than a cease and desist letter.	○	○	○	○	○	○
28. If computer ethics were a required course for all students, it would help in the prevention of digital piracy.	○	○	○	○	○	○
29. If digital piracy was reduced as a result of the computer ethics course, it would lessen the monitoring software's role in preventing digital piracy.	○	○	○	○	○	○



Section 4 of 4

30. What is your gender?

○ Male
○ Female

31. What is your highest degree earned?

○ HS Diploma/GED
○ Associates
○ Bachelors
○ Masters
○ Doctorate

32. Please specify your salary range.

○ Less than $50k
○ $50k - $69k
○ $70k - $89k
○ $90k - $109k
○ $110k or higher

33. How long have you worked in your position (in years)?

34. Are you a member of a professional organization in your field?

○ Yes
○ No --> Skip to Question 36

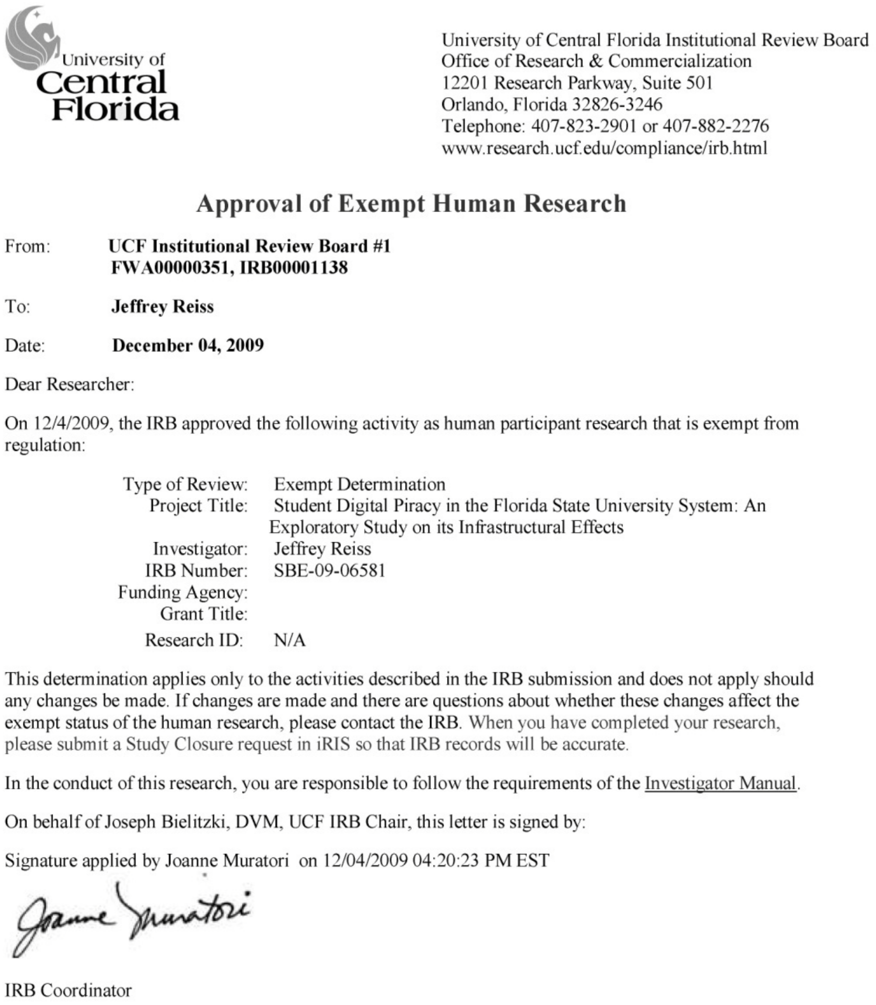
35. Do you hold a leadership position in a professional organization?

○ Yes (Specify position)
○ No

36. Please add any further questions or comments here.

Once you submit, you cannot revise.

APPENDIX C
PRE-CONTACT SCRIPTS



University of Central Florida

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Approval of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Jeffrey Reiss**

Date: **December 04, 2009**

Dear Researcher:

On 12/4/2009, the IRB approved the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination
Project Title:	Student Digital Piracy in the Florida State University System: An Exploratory Study on its Infrastructural Effects
Investigator:	Jeffrey Reiss
IRB Number:	SBE-09-06581
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

On behalf of Joseph Bielitzki, DVM, UCF IRB Chair, this letter is signed by:

Signature applied by Joanne Muratori on 12/04/2009 04:20:23 PM EST

Joanne Muratori

IRB Coordinator

APPENDIX C
PRE-CONTACT SCRIPTS

E-mail Contact:

Hello <Participant name>,

My name is Jeffrey Reiss and I am a doctoral candidate at UCF in the Educational Leadership program. My dissertation topic is on student copyright infringement from the viewpoint of the effectiveness of network monitoring software compared to alternative solutions or combinations. I would like to know if you, or anyone else in your department, would be capable in answering questions about this topic once I finalize my research instrument and obtain the required authorizations within the next few months. At the moment I am trying to gather a list of applicable contacts.

Thank you for your assistance,

Jeffrey Reiss

Phone Contact:

Hi, my name is Jeff Reiss and I am a doctoral candidate at the University of Central Florida in the Higher Educational Leadership program. I'm looking to get the contacts at each of the SUS institutions who have the background knowledge to answer some questions about the effectiveness of network monitoring software for copyright infringement compared to alternative solutions or combinations. I'm having trouble getting through via e-mail. I'm not sending out my short online survey yet, but when the time comes in the next few weeks I want to have a complete list of whom I should contact. If you can contact me with this information by e-mail at [e-mail removed] or by phone at [phone number removed] it would be greatly appreciated. Thank you.

APPENDIX D
CONTACT LETTER

<Participant name>,

I am writing you to ask for your help in a study about the opinions of University IT professionals on network monitoring software and potential alternatives to combat digital piracy. The study is part of an effort to identify better and more effective ways to combat digital piracy. You were selected for this study based upon my pre-contact with you and your willingness to participate in the study.

The results from the survey will be used to help paint a preliminary picture of the state of the IT departments within the Florida State University System (SUS). By understanding how IT departments currently operate to thwart digital piracy conducted by students in light of recent policy changes to the Higher Education Act, public officials could be persuaded to provide more funding to the innovation and implementation of new, more effective methods.

Your responses to the survey will be completely confidential. Your name is not used at all in the survey and any potential identification of your institution will be removed after the completion of the survey. This survey is voluntary. However, you can help me very much by taking approximately ten minutes of your time to share your opinions on this matter. If for some reason you prefer not to respond, please let me know via an e-mail reply to this message.

The survey is located at http://www.stathelpers.com/Surveys/
Your Username is <username>
Your Password is <password> (Password is case sensitive)

If you have any questions or comments about this study, I would be happy to talk with you. You can write me by replying to this e-mail. If desired, you may also contact my advisor, Dr. Rosa Cintron at [phone number removed] or by e-mail at [e-mail removed].

Thank you very much for helping me with this important study.

Sincerely,
Jeffrey Reiss
Doctoral Candidate
University of Central Florida

REFERENCES

Adamsick, C. (2008). “Warez” the copyright violation? Digital copyright infringement: Legal loopholes and decentralization. *TechTrend, 52*(6), 10-12.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50,* 179-211.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Psychology, 32*, 665-683. Retrieved October 3, 2009 from Wiley Interscience.

Allen, C., Varner, G., & Zinser, J. (2000). Prolegomena to any future artificial moral agent. *Journal of Experimental Theory of Artificial Intelligence, 12,* 251-261. Retrieved November 29, 2009 from EBSCO Host.

Al-Rafee, S., & Cronan, T. P. (2006). Digital piracy: Factors that influence attitude toward behavior. *Journal of Business Ethics, 63*, 237-259. Retrieved September 28, 2009 from SpringerLink.

Anderson, N. (2009a). Judge rejects fair use defense as Tenenbaum P2P trial begins. *Ars Technica*. Retrieved August 11, 2009, from http://arstechnica.com/tech-policy/news/2009/07/judge-rejects-fair-use-defense-as-tenenbaum-p2p-trial-begins.ars

Anderson, N. (2009b). Team Tenenbaum to fight on for those "RIAA has screwed over.” *Ars Technica*. Retrieved August 11, 2009, from http://arstechnica.com/tech-policy/news/2009/08/charlie-nesson-still-fights-for-those-riaa-has-screwed-over.ars

Athey, S. (1993). A comparison of experts’ and high tech students’ ethical beliefs in computer-related situations. *The Journal of Business Ethics, 12*, 359-370.

Bakker, P. (2005). File-sharing--fight, ignore or compete ☆ Paid download services vs. P2P-networks. *Telematics and Informatics, 22*, 41-55. Retrieved September 27, 2009 from ScienceDirect.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognative Theory.* Englewood Cliffs, NJ: Prentice-Hall.

Banerjee, D. S., Banerjee, T., & Raychaudhuri, A. (2008). Optimal enforcement and anti-copying strategies to counter copyright infringement. *The Japanese Economic Review, 59*, 519-535. Retrieved October 3, 2009 from Wiley Interscience.

Bhattacharjee, S., Gopal, R., Lertwachara, K., & Marsden, J. R. (2006a). Whatever happened to payola? An empirical analysis of online music sharing. *Decision Support Systems, 42,* 104-120. Retrieved October 4, 2009 from ScienceDirect.

Bhattacharjee, S., Gopal, R., Lertwachara, K., & Marsden, J. R. (2006b). Consumer search and retailer strategies in the presence of online music sharing. *Journal of Management Information Systems, 23,* 129-159. Retrieved October 5, 2009 from Business Source Premier.

Blythe, M., & Wright, P. (2008). Technology scruples: Why intimidation will not save the recording industry and how enchantment might. *Pers Ubiquit Compute, 12*, 411-420. Retrieved September 29, 2009 from SpringerLink.

Brancomb, A. W. (1993). Who owns computer software? *Educom Review, 30*(1). Retrieved August 19, 2009 from ERIC.

Brey, P. (2000). Method in computer ethics: Towards a multi-level interdisciplinary approach. *Ethics and Information Technology, 2,* 125-129.

Chang, M. C., Lin, C. F., & Wu, D. (2008). Piracy and limited liability. *Journal of Economics, 95*, 25-53. Retrieved October 3, 2009 from SpringerLink.

Chellappa, R. K., & Shivendu, S. (2005). Managing Piracy: Pricing and sampling strategies for digital experience goods in vertically segmented markets. *Information Systems Research, 16*, 400-417. Retrieved October 5, 2009 from Business Source Premier.

Chen, Y. –C., Shang, R. –A., & Lin, A. –K. (2008). The intention to download music files in a P2P environment: Consumption value, fashion, and ethical decision perspectives. *Electronic Commerce Research and Applications, 7*, 411-422. Retrieved October 3, 2009 from ScienceDirect.

Chiang, E., & Assane, D. (2002). Software copyright infringement among college students. *Applied Economics, 34*, 157-166.

Chiang, E., & Assane, D. (2007). Determinants of music copyright violations on the university campus. *Journal of Cultural Economics, 31*, 187-204.

Chiang, E., & Assane, D. (2008). Music piracy among students on the university campus: Do males and females react differently? *The Journal of Socio-Economics. 37*, 1371-1380. Retrieved October 3, 2009 from SpringerLink.

Chiou, J. –S., Huang, C. –Y., & Lee, H. –H. (2005). The antecedents of music piracy attitudes and intentions. *Journal of Business Ethics, 57*, 161-174. Retrieved October 5, 2009 from SpringerLink.

Chiu, H, –C., Hsieh, Y., –C., & Wang, M. –C. (2008). How to encourage customers to use legal software. *Journal of Business Ethics, 80*, 583-595.

Christoph, R., Forcht, K., & Bilbrey, C. (1987/1988). The development of systems ethics: An analysis. *The Journal of Computer Information Systems,*(2), 20-23

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*, 297-344.

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

Common Solutions Group, (2008). *Infringement-suppression technologies: Summary observations from a Common Solutions Group workshop.* Retrieved July 29, 2009, from http://net.educause.edu/ir/library/pdf/CSD5323.pdf

Coyle, J. R., Gould, S.J., Gupta, P., & Gupta, R. (2009). "To buy or pirate": The matrix of music consumers' acquisition-mode decision-making. *Journal of Business Research, 62*, 1031-1037. Retrieved September 27, 2009 from ScienceDirect.

Cronan, T. P., & Al-Rafee, S. (2008). Factors that influence the intention to pirate software and media. *Journal of Business Ethics, 78*, 527-545. Retrieved October 3, 2009 from SpringerLink.

Dames, M. K. (2007). Understanding plagiarism and how it differs from copyright infringement. *Computers in Libraries, 27*(6), 25-27). Retrieved September 25, 2009 from ERIC.

Dejean, S. (2009). Empirical studies about piracy. *CESifo Economic Studies, 55,* 326-352. Retrieved October 3, 2009 from ABI

Dillman, D. A. (2000). *Mail and internet surveys* (2nd ed.). New York: John-Wiley & Sons.

Djeckic, P., & Loebbecke, C. (2007). Preventing application software piracy: An empirical investigation of technical copy protections. *Journal of Strategic Information Systems, 16*, 173-186. Retrieved October 4, 2009 from Science Direct.

Douglas, D. E., Cronan, T. P., & Behel, J. D. (2007). Equity perception as a deterrent to software piracy behavior. *Information & Management, 44*, 503-512. Retrieved October 4, 2009 from Science Direct.

Dubinsky, A. J., & Loken, B. (1989). Analyzing ethical decision making in marketing. *Journal of Business Research, 19*(2), 83-107. Retrieved October 3, 2009 from Science Direct. Retrieved October 4, 2009 from Science Direct.

Duchêne, A., & Waelbroeck, P. (2006). The legal and technological battle in the music industry: Information-push versus information-pull technologies. *International Review of Law and Economics, 26,* 565-580.

Easley, R. F. (2005). Ethical issues in the music industry response to innovation and piracy. *Journal of Business Ethics, 62*, 163-168. Retrieved September 28, 2009 from SpringerLink.

Edgar, S. L. (2003). *Morality and Machines: Perspectives on Computer Ethics* (2nd ed.). Sudbury, Massachusetts (Jones and Bartlett Publishers).

Einav, G. (2008). College students: The rationale for peer-to-peer video file sharing. In E. M. Noam & L. M. Pupillo (Eds.), *Peer-to-peer video: The economics, policy, and culture of today's new mass medium* (pp. 149-162). New York: Springer. Retrieved September 27, 2009 from SpringerLink.

Electronic Frontier Foundation. (2006). *When push comes to shove: A hype-free guide to evaluating technical solutions to copyright infringement on campus networks.* Retrieved May 15, 2009, from http://www.eff.org/files/univp2p.pdf

Electronic Frontier Foundation. (2008). *RIAA v. The People: Five years later.* Retrieved June 14, 2009, from http://www.eff.org/wp/riaa-v-people-years-later

Einhorn, M., A. & Rosenblatt, B. (2005). Peer-to-peer networking and digital rights management: How market tools can solve copyright problems. *Policy Analysis*, 534, 1-26.

Fitzpatric, S. (2009). Harvard Law professor challenges anti-piracy statute. *American Libraries, 40*(1/2), 21.

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology, 1,* 37-56.

Forester, T., & Morrison, P. (1994). *Computer ethics: Cautionary tales and ethical dilemmas in computing* (2nd ed.). Cambridge, Massachusetts: The MIT Press.

Friedman, B., & Kahn, P. H., Jr. (1992). Human agency and responsible computing: Implications for computer systems design. *Journal of Systems Software, 17*, 7-14.

Gan, L. L., & Koh, H. C. (2006). An empirical study of software piracy among tertiary institutions in Singapore. *Information & Management, 43,* 640-649. Retrieved October 5, 2009 from ScienceDirect.

Gayer, A., & Shy, O. (2006). Publishers, artists, and copyright enforcement. *Information Economics and Policy, 18*, 374-384.

Goles, T., Jayatilaka, B., George, B., Parsons, L., Chambers, V., Taylor, D., et al. (2008) Softlifting: Exploring determinants of attitude. *Journal of Business Ethics, 77*, 481-499. Retrieved September 28, 2009 from SpringerLink.

Goodyear, M., Salaway, G., Nelson, M. R., Petersen, R., & Portillo, S. (2009) The career of the IT security officer in higher education. Retrieved October 8, 2009 from http://www.educause.edu/library/ECP0901

Gopal, R. D., & Sanders, G. L. (2000). Global software piracy: You can't get blood out of a turnip. *Communications of the ACM, 43* (9), 83-89. Retrieved September 25, 2009 from ACM Portal.

Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. C. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing and Electronic Commerce, 14*(2), 89-105.

Gopal, R. D., Bhattacharjee, S., & Sanders, G. L. (2006). Do artists benefit from online music sharing? *Journal of Business, 79*, 1503-1533. Retrieved October 5 2009 from Business Source Premier.

Green, K. C. (2008). The campus cost of P2P compliance. *The Campus Computing Project.* Retrieved June 27, 2008, from http://www.campuscomputing.net/sites/www.campuscomputing.net/files/Green-P2PCompliance-Oct08_5.pdf

Gupta, P. B., Gould, S. J., & Pola, B. (2004). "To pirate or not to pirate": A comparative study of the ethical versus other influences on the consumer's software acquisition-mode decision. *Journal of Business Ethics, 55*(3), 255-274.

Hayes, D. L., & Fenwick & West. (2001). Advanced copyright issues on the internet--part III. *Computer Law & Security Report, 17*(2), 75-91. Retrieved September 27, 2009 from ScienceDirect.

Hinduja, S. (2008). Deindividuation and Internet software piracy. *CyberPsychology & Behavior, 11*, 391-398.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1-24.

Higgins, G. E. (2007). Digital piracy: An examination of low self-control and motivation using short-term longitudinal data. *CyberPsychology & Behavior, 10*, 523-529. Retrieved October 4, 2009 from Academic Search Premiere.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies, 19*, 3-22.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2007). Low self-control and social learning in understanding student' intentions to pirate movies in the United States. *Social Science Computer Review, 25*, 399-357. Retrieved October 4, 2009 from SAGE.

Higgins, G. E., & Makin, D. A. (2004). Self-control, deviant peers, and software piracy. *Psychological reports, 95*, 921-931.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measures of self-control. *Deviant Behavior¸ 29*, 440-460. Retrieved October 3, 2009 from Informaworld.

Higgins, G. E., Wolfe, S. E., & Ricketts, M. L. (2008). Digital piracy: A latent class analysis. *Social Science Computer Review, 27*, 24-40. Retrieved October 3, 2009 from SAGE.

Higher Education Act of 1965, Cong. §487 (2008).

Hohn, D. A., Muftic, L., & Wolf, K. (2006). Swashbuckling students: An exploratory study of Internet piracy. *Security Journal, 16*, 110-127.

Huang, C. –Y. (2005). File Sharing as a form of music consumption. *International Journal of Electronic Commerce, 9* (4), 37-55. Retrieved October 5, 2009 from Business Source Premier.

Hui, K. & Png, I. (2003). Piracy and the legitimate demand for recorded music. *Contributions to Economic Analysis & Policy, 2*(1), Article 11. Retrieved July 1, 2009 from http://www.bepress.com/bejeap/contributions/vol2/iss1/art11

Hunt, S. D., & Vitell, S. (1986). A general theory of marketing ethics. *Journal of Macromarketing, 6*, 5-16.

Infringement (of copyright). Retrieved July 12, 2009, from http://www.nolopress.com/definition.cfm/Term/23009410-A6AF-4268-B0B6C764FE7B1F1A/alpha/I/

Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior, 29*, 334-366. Retrieved October 3, 2009 from Informaworld.

Jaisingh, J. (2007). Piracy on file-sharing networks: Strategies for recording companies. *Journal of organization computing and electronic commerce, 17*, 329-348. Retrieved October 3, 2009 from Business Source Premier.

Joachim, D. (2004). The enforcers--The University of Florida's ICARUS P2P-blocking software has clipped students' file-sharing wings. Do its policy-enforcing capabilities go too far? *Network Computing*. Retrieved June 16, 2009, from http://cyber.law.harvard.edu/digitalmedia/Icarus%20at%20UF.htm

Johnson, D. G. (1994). *Computer ethics.* (2nd ed.). Edgewood, New Jersey: Prentice-Hall.

Jung, I. (2009). Ethical judgments and behaviors: Applying a multidimensional ethics scale to measuring ICT ethics of college students. *Computers & Education, 53*, 940-949. Retrieved September 27, 2009 from ScienceDirect.

Karagiannis, T., Broido, A., Brownlee, N., Claffy, K. C., & Faloutsos, M. (2004). Is P2P dying or just hiding? Paper presented at IEEE Globecom 2004 in November-December 2004.

Karnowski, S. (2009). Facing the music: $1.9M file-share verdict stuns Minn. mom. *USA Today*. Retrieved June 20, 2009, from http://www.usatoday.com/tech/news/2009-06-18-music-downloading_N.htm

Kierkegaard, S. M. (2006). Outlawing circumvention of technological measures going overboard: Hollywood style. *Computer Law & Security Report, 22*, 46-56. Retrieved September 27, 2009 from ScienceDirect.

Kini, R. B., Rominger, A., & Vijayaraman, B. S. (2000). An empirical study of software piracy and moral intensity among university students. *Journal of Computer Information Systems, 40*(3), 62-72.

Kohlberg, L. (1969). Stage and sequence: The cognitive-developmental approach to socialization. In Goslin, D. A (Ed.), *Handbook of Socialization Theory and Research* (pp. 347-480). Chicago: Rand-McNally.

Klein, B., Lerner, A. V., & Murphy, K. M. (2002). The economics of copyright "fair use" in a networked world. *The American Economic Review, 92*(2), 205-208.

Knaus, W. A., Wagner, D. P., Draper, E. A., Zimmerman, J. E., Bergner, M., Bastos, P. G., et al. (1991). The APACHE III prognostic system. Risk prediction of hospital morality for critically ill hospitalized adults. *CHEST, 100*, 1619-1636. Retrieved November 23, 2009 from http://chestjournal.chestpubs.org/content/100/6/1619.full.pdf+html

Kuo, F. –Y., & Hsu, M. –H. (2001). Development and validation of ethical computer self-efficacy measure: The case of softlifting. *Journal of Business Ethics, 32,* 299-315. Retrieved October 6, 2009 from SpringerLink.

LaBelle, M. M. (2006). The "rootkit debacle": The latest chapter in the story of the recording industry and the war on music piracy. *Denver University Law Review, 84*, 79-134. Retrieved October 5, 2009 from Wilson Web.

LaRose, R., Lai, Y.-J., Lange, R., Love, B., & Wu, Y. (2005). Sharing or piracy? An exploration of downloading behavior. *Journal of Computer-Mediated Communication, 11*(1), Article 1. Retrieved August 31, 2009 from http://jcmc.indiana.edu/vol11/issue1/larose.html

Langenderfer, J., & Cook, D. L. (2001). Copyright policies and issues raised by A&M Records v. Napster: "The shot heard 'round the world" or "not with a bang but a whimper?" *Journal of Public Policy & Marketing, 20*, 280-288. Retrieved October 6, 2009 from JSTOR.

Leonard, L., N., K., & Haines, R. (2006). Computer-mediated group influence on ethical behavior. *Computers in Human Behavior, 23*, 2302-2320.

Leyshon, A., Webb, P., French, S., Thrift, N., & Crewe, L. (2005). On the reproduction of the musical economy after the Internet. *Media, Culture, & Society, 27*(2), 177-209. Retrieved October 5, 2009 from SAGE.

Liang, Z., & Yan, Z. (2005). Software piracy among college students: A comprehensive review of contributing factors, underlying processes, and tackling strategies. *Journal of Educational Computing Research, 33*(2), 115-140.

Liebowitz, S. J. (2004). Will mp3 downloads annihilate the record industry? The evidence so far. *Advances in the Study of Entrepreneurship, Innovation & Economic Growth, 15,* 229-260.

Liebowitz, S. J. (2006). File sharing: Creative destruction or just plain destruction? *The Journal of Law and Economics, 49,* 1-28.

Liebowitz, S. J., & Watt, R. (2006). How to best ensure remuneration for creators in the market for music? Copyright and its alternatives. *Journal of Economic Surveys, 20*, 513-545. Retrieved October 5, 2009 from Business Source Premier.

Limayem, M., Khalifa, M., & Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study. *IEE Transactions on Engineering Management, 51*, 414-425. Retrieved October 5, 2009 from IEEE Xplore.

Lincoff, B. (2008). Common sense, accommodation and sound policy for the digital music marketplace. *Journal of International Media and Entertainment Law. 2,* 1-64.

Logsdon, J. M., Thompson, J. K., & Reid, R. A. (1994). Software piracy: Is it related to level of moral judgment? *Journal of Business Ethics, 13*, 849-857.

Michigan State University website (2009). Notice of written plan for copyright provisions of the Higher Education Opportunity Act of 2008. Retrieved July 29, 2009, from http://www.msu.edu/policy/copyright-plan.html

Mishra, A., Akman, I., & Yazici, A. (2006). Software piracy among IT professionals in organizations. *International Journal of Information Management, 26,* 401-413. Retrieved October 5, 2009 from Science Direct.

Molteni, L., & Ordanini, A. (2003). Consumption patterns, digital technology and music downloading. *Long Range Planning, 36*, 389-406. Retrieved September 27, 2009 from ScienceDirect.

Moor, J. H. (2001). The status and future of the Turing Test. *Minds and Machines, 11,* 73-93. Retrieved November 28, 2009 from SpringerLink.

Nichlolson, C. Y., & DeMoss, M. (2009). Teaching ethics and social responsibility: An evaluation of undergraduate business education at the discipline level. *Journal of Education for Business, 84,* 213-218.

Nimmer, D. (1992). Nation, duration, violation, harmonization: An internal copyright proposal for the United States. *Law and Contemporary Problems, 55*, 211-239.

Norton, Q. (2009, May). Paradise lost. *Maximum PC,* 12.

Nyiri, J. (2004, Spring). The effects of piracy in a university setting. *Crossroads*, *10*(3), 3-3. Retrieved October 1, 2009 from ACM Portal.

Oberholzer-Gee, F., & Strumpf, K. (2009). File-sharing and copyright. Unpublished manuscript, Harvard Business School.

Ouellet, J., -F. (2007). The purchase versus illegal download of music by consumers: The influence of consumer response towards the artist and music. *Canadian Journal of Administrative Sciences, 24*, 107-119. Retrieved October 1, 2009 from Business Source Premier.

Peitz, M., & Waelbroeck, P. (2006). Why the music industry may gain from free downloading--The role of sampling. *International Journal of Industrial Organization, 24*, 907-913. Retrieved October 5, 2009 from Science Direct.

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviors: Broadening and deepening the theory of planned behavior. *British Journal of Social Psychology, 40*, 79-98. Retrieved October 3, 2009 from Academic Search Premier.

Rahim, M., Seyal, A. H., & Rahman, M. N. A. (2001). Factors affecting softlifting intention of computing students: An empirical study. *Journal of Educational Computing Research, 24*(4), 385-405.

Randal, D. M., & Gibson, A. M. (1991). Ethical decision making in the medical profession: An application of the theory of planned behavior. *Journal of Business Ethics, 10*, 111-122. Retrieved October 3, 2009 from JSTOR.

Rest, J. R. (1986). *Moral Development: Advances in Research Theory.* New York: Praeger.

Rob, R., & Waldfogel, J. (2006). Piracy on the high c's: Music downloading, sales displacement, and social welfare in a sample of college students. *Journal of Law and Economics, 49,* 29-62.

Rogerson, S. (1996) ETHicol: Reports on a recent public lecture on computers and human values. *IMIS Journal, 6*(5) 14-17.

Rosenblatt, J. (2008). Security metrics: A solution in search of a problem. *EDUCAUSE Quarterly, 31*(3), 8-11. Retrieved September 25, 2009 from http://www.educause.edu/ir/library/pdf/EQM0832.pdf

Rupp, P., & Estier, T. (2002). A model for a better understanding of the digital distribution of music in a peer-to-peer environment. *Paper presented at the proceedings of the 36th Annual Hawaii International Conference on System Sciences.* Retrieved on July 21, 2009, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.6593&rep=rep1&type=pdf

Schuster, W. V. (1987). Bootleggery, smoking guns and whistle blowing; a sad saga of academic opportunism. *Western Educational Computing Conference*.

Shang, R. –A., Chen, Y. –C., Chen, P. –C. (2008). Ethical decisions about sharing music files in the P2P environment. *Journal of Business Ethics, 80*, 349-365. Retrieved September 28, 2009 from SpringerLink.

Sheffner, B. (2009a). Oy Tenenbaum! RIAA wins $675,000, or $22,500 per song. *Ars Technica*. Retrieved August 11, 2009, from http://arstechnica.com/tech-policy/news/2009/07/o-tenenbaum-riaa-wins-675000-or-22500-per-song.ars

Sheffner, B. (2009b). Tenenbaum takes the stand: I used P2P and lied about it. *Ars Technica*. Retrieved August 11, 2009, from http://arstechnica.com/tech-policy/news/2009/07/tenenbaum-takes-the-stand-i-used-p2p-and-lied-about-it.ars

Siegfried, R. M. (2004). Student attitudes on software piracy and related issues of computer ethics. *Ethics and Information Technology, 6,* 215-222.

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

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

Sinha, R. K., & Mandel, N. (2008). Preventing digital music piracy: The carrot or the stick? *Journal of Marketing, 72*, 1-15.

Slater, D. (1991, October 14).New crop of IS pros on shaky ground. *Computerworld,* 90.

Software piracy: Is it happening in your school or university? (1998). *T.H.E. (Technological Horizons in Education), 25*(9), 66-68. Retrieved September 30, 2009 from ERIC.

Spanier, G. B. (2004). Peer to peer on university campuses: An update. Retrieved July 21, 2009, from http://president.psu.edu/testimony/articles/161.html

Stahl, B. C. (2004). Information, ethics, and computers: The problem of autonomous moral agents. *Minds and Machines, 14*, 67-83.

Sun, J. C., & Baez, B. (2009). Overview of intellectual property. *ASHE Higher Education Report, 34* (4).

Sundarajan, A. (2004). Managing digital piracy: Pricing and protection. *Information Systems Research, 15*, 287-308. Retrieved October 5, 2009 from Business Source Premier.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*, 664-670. Retrieved October 3, 2009 from JSTOR.

Takeyama, L. N. (1997). The intertemporal consequences of unauthorized reproduction of intellectual properly. *The Journal of Law and Economics, 40,* 511-522.

Tavani, H. T. (2002). The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter? *Ethics and Information Technology, 4*, 37-54. Retrieved September 28, 2009 from SpringerLink.

Taylor, S. A., Ishida, C., & Wallace, D. W. (2009). Intention to engage in digital piracy: A conceptual model and empirical test. *Journal of Service Research, 11*, 246-262. Retrieved October 3, 2009 from SAGE.

Taylor, S. L. (2004). Music piracy--Differences in the ethical perceptions of business majors and music business majors. *Journal of Education for Business, 79*, 306-310.

Thong, J. Y. L., & Yap, C. –S. (1998). Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems, 15*, 213-237. Retrieved September 28, 2009 from Business Source Premier.

Thurstone, L. (1931). Comparison of validity and reliability concepts. *The reliability and validity of tests: Derivation and interpretation of fundamental formulae concerned with reliability and validity of test and illustrative problems* (pp. 97-104).

University of Central Florida Website (2009). Retrieved May 11, 2009, from http://www.osc.sdes.ucf.edu/?id=computer_misuse

U.S. Copyright Office (2008). Copyright Basics. Retrieved Retrieved September 25, 2009 from http://www.copyright.gov/circs/circ1.pdf

van Eechoud, M., & van der Wal, B. (2008). Creative commons licensing for public sector information opportunities and pitfalls. Retrieved September 25, 2009 from http://www.ivir.nl/publications/eechoud/CC_PublicSectorInformation_report_v3.pdf

VoIP terms – What does VoIP mean? (n.d.). Retrieved November 11, 2009 from http://www.discover-voip.info/voip-basics/voip-terms.html

Wagner, S. C., & Sanders, G. L. (2001). Considerations in ethical decision-making and software piracy. *Journal of Business Ethics, 29*, 161-167. Retrieved September 29, 2009 from SpringerLink.

Wallach, W., Allen, C., & Smit, I. (2008). Machine morality: Bottom-up and top-down approaches for modeling human moral faculties. *AI & Society, 22*, 565-582.

Wallace, J., & Erickson, J. (1992). *Hard drive: Bill Gates and the making of the Microsoft Empire*. New York: (Jon Wiley & Sons).

Waterman, D., Ji, S. W., & Rochet, L. R. (2007). Enforcing and control of piracy, copying, and sharing in the movie industry. *Review of Industrial Organization, 30*, 255-289. Retrieved October 4, 2009 from SpringerLink.

Werth, L. H. (1997). Getting started with computer ethics. *ACM SIGCSE Bulletin, 29,* 1-5.

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review, 26*, 317-333. Retrieved October 3, 2009 from SAGE.

Worona, S. (2008). On making sausage. *EDUCAUSE Review, 43*(6) Retrieved May 12, 2009 from http://www.educause.edu/library/erm08615

Wu, S. –Y., & Chen, P. –Y. (2008). Versioning and piracy control for digital information goods. *Operations Research, 56*, 157-172. Retrieved October 3, 2009 from Extenza.

Zentner, A. (2008) Online sales, Internet use, file sharing, and the decline of retail music specialty stores. *Information Economics and Policy, 20*, 288-300. Retrieved September 27, 2009 from ScienceDirect.