11-13-2006

Social learning theory as a model for illegitimate peer-to-peer use and the effects of implementing a legal music downloading service on peer-to-peer music piracy

Nathan Fisk

Running head: SOCIAL LEARNING THEORY

Social Learning Theory as a Model for Illegitimate Peer-to-Peer Use and the Effects of Implementing a Legal Music Downloading Service on Peer-to-Peer Music Piracy

A Thesis Presented to The Faculty of the Department of Communication

Rochester Institute of Technology

In Partial Fulfillment of the Master of Science Degree in

Communication & Media Technologies

by

Nathan W. Fisk

September 14, 2006

The following members of the thesis committee approve the thesis of Nathan W. Fisk on September 14, 2006

_____

Dr. Rudy Pugliese
CMT Coordinator
Department of Communication
Thesis Advisor

_____

Dr. Samuel McQuade
College of Applied Science & Technology
Center for Multidisciplinary Studies
Thesis Advisor

_____

Dr. Bruce Austin
Department of Communication
Chairman

Dedication

For the four people that made this work possible:

My parents, Stephen and Suzan

My mentor, Dr. Samuel McQuade

And most of all, my wife, Elizabeth

Table of Contents

Abstract

In an attempt to both provide added services to students and help curb the growing problem of music piracy on college campuses, many universities have implemented legal digital music services. The Rochester Institute of Technology (RIT) was one of these universities, where the Cdigix Ctrax service is provided to students. In order to evaluate the effectiveness of such a strategy, Information Technology Services (ITS) at RIT requested the services of Dr. Samuel McQuade, who administered a Web-based survey to all Ctrax users and an equal number of randomly selected non-Ctrax using students at RIT. In total, 447 students responded to the survey. This thesis represents a secondary analysis of the data gathered from that survey within the context of social learning. The findings reveal that social learning theory provides a useful framework for explaining illegitimate P2P at RIT and potentially on college campuses across the nation.

Introduction

Digital copyright violation, is a significant concern for the music, movie and software industries. While the actual impact of piracy is nearly impossible to calculate with precision, simply the threat of damage to one the world's highest-grossing industries has both government and industry leaders concerned (Peer-to-Peer Piracy, 2004). With an estimated $626.6 billion at stake (Siwek, 2004) due to millions of people blatantly violating copyright regulations combined with constant industry lobbying for stricter copyright enforcement laws, government and law enforcement have taken notice. In the United States, much of this attention has focused on college campuses which are widely viewed as piracy hotbeds due to the combination of campus-wide high bandwidth connections to the Internet, technology savvy students, and high concentrations of computers in an institutional environment where students are in constant social interaction with one another. As such, colleges have begun to take steps towards protecting themselves and their students from legal liability as the intellectual property industries and government crack down on digital copyright infringement issues.

Despite the increased attention on digital piracy issues, there has been little empirical research on the topic. Understandably, the literature that does exist tends to focus on the prevalence of digital copyright infringement, rather than on the impacts of a proposed solution. Furthermore, the extant studies are focused on software piracy more often than music piracy, due to the fairly recent emergence of music piracy via peer-to-peer networks.

One potential method of managing illegitimate music downloading and sharing on a college campus is to provide students with a legal alternative to piracy by offering a music downloading service at little or no cost. Recently, the Rochester Institute of Technology (RIT) implemented the Cdigix Ctrax music downloading service in an attempt to curb the ever-growing problem of piracy on campus and thereby avoid legal repercussions from the music industry and to repair the image of the Institute following a December, 2001 raid by the U.S. Customs Service.

This thesis builds upon a program evaluation initiated by Information Technology Services at RIT and conducted by Dr. Samuel McQuade. The evaluation was designed to determine the extent to which the implementation of the Ctrax service impacted illegitimate music downloading behavior on campus. However, in order to empirically examine the processes by which illegitimate music downloading is learned and accepted by students, additional questionnaire items were developed and added to answer the following research questions:

- Does social learning theory provides an applicable model for describing perceptions and behaviors regarding illegitimate P2P use?
- Are there significant differences between the perceptions and behavior of students who are enrolled in the legal downloading service versus those of students who are not?

Review of the Literature

History of Digital Copyright Infringement

Following the years since its creation, the Internet has proven to be a medium capable of transmitting nearly any form of content. With sufficient bandwidth, text, still images, audio and video can be quickly and efficiently transmitted over great distances. Infinite amounts of exact digital copies of text, audio and video can be made using publicly available computer hardware and a limited amount of technological skill. The ability of the Internet and computer technologies to do exactly that has struck fear in the hearts of intellectual property industries around the world. With unfettered, and more importantly, convenient methods of copying and transferring both copyrighted and public domain works, their livelihoods may be at stake (McFadden, 2004).

Piracy, or at least the unauthorized reproduction of intellectual property, is far from a new activity. Throughout history, as new media technologies have been developed, so have innovative ways to use and abuse those technologies to illicitly copy and distribute intellectual property (Lessig, 2005). As these behaviors have emerged, copyright law has traditionally expanded to accommodate the new technology while maintaining the balance between the rights of copyright holders to control their intellectual property and consumer demand for unfettered access to intellectual property. When observed as a form of social technology, this expanding of law is concurrent with the theory of technologically-enabled crime (McQuade, 1998).

According to this theory, following the radical use of technology for some form of social abuse, the incidence and complexity of that form of technologically-enabled abuse tends to increase slowly, followed by a period of rapid growth, creating a “technology crime wave” (McQuade, 1998, p11). The first stage of the crime wave is known as the “new crime phase,” in which the abuse is not recognized and generally misunderstood. During this phase the incidence of the abuse slowly increases. The new crime phase is followed by the “adaptive crime phase,” in which the abuse is recognized as crime, but not understood by the general populous. During this phase, incidence of the abuse grows rapidly as larger segments of the population become aware. These phases of abusive behavior occur in the gap that is created as policing technology and legislation lag behind the abusive behavior. During these phases, complexity increases while understanding and manageability decreases, placing law enforcement and legislators in a metaphorical arms race in an attempt to manage the crime. If and when policing technology and legislation combines to form an effective method of managing the abuse, the wave enters the “ordinary crime phase” and begins to slowly dissipate (McQuade, 1998).

In the case of digital piracy, the burden of developing new technologies to manage abuse of copyright has largely fallen upon the intellectual property industry, rather than upon government legislators and law enforcement. In desperation, copyright holders must regularly find new ways of maintaining control over the texts they own as new methods of content distribution are developed and utilized by consumers and competitors in innovative ways that surpass what is covered by law. How has this

situation of industry enforcement come about, and what are the consequences of the intellectual property industries' fight to dissipate the digital piracy crime wave?

The first known incidents of digital piracy originally occurred in 1975, with paper tape copies of Micro Soft (now Microsoft) BASIC for the MITS Altair. After acquiring one of a number of tapes stolen from a demonstration, a member of the now legendary Homebrew Computer Club made 50 copies and distributed them among the club members. Included in the manual for Micro Soft BASIC was a small warning that read "Copying or otherwise distributing MITS software outside of the terms of such an [licensing] agreement may be a violation of copyright laws" (*MITS Altair BASIC*, 1975). This tiny statement was revolutionary; up until this point software designed for personal computers was freely distributed! The club was divided on the issue of continuing to copy and use the software, yet few members refused a copy. Here was the initial innovative abuse of computer technologies to violate software copyright. To this day, the ideological debate between free software supporters and commercial developers continues (Markoff, 2000).

Similar to the original copying incident within the Homebrew Computer Club, early methods of distribution were limited to local areas, due to the lack of a high-bandwidth national network that allowed data to be quickly transmitted from one computer to another. Pirated software was not uncommon and limited to the distance that any one person was willing to move a copy via some form of physical storage medium. Few people gave any real thought to violating software copyrights, and copies were more difficult to make and distribute widely. However, throughout the 1980's the computer

underground, including hackers, phreaks and pirates, began to utilize and exploit computer networks. The software industry was growing, and so was piracy (Sterling, 1992).

The Bulletin Board System, or BBS, as a method for computer enthusiasts to communicate was becoming immensely popular after the first was developed by Ward Christensen in 1979. Many early software pirates used BBSs as a trading or storage sites, sharing new software with anyone who knew the phone number of the BBS and further increasing the complexity of digital copyright infringement. Using BBSs, software pirates organized into groups, with each member performing specific tasks. The role of many pirates, known as couriers, was simply to shuttle pirated software from BBS to BBS. With the invention of the BBS, law enforcement began to catch up with copyright violators. BBSs were such a central component of the computer underground that law enforcement routinely set up false BBSs in order to catch computer criminals bragging about their latest exploits or posting calling card codes to the site (Sterling, 1992; Mollick, 2005). The piracy "scene" at this point in time was entirely about winning respect and prestige, rather than financial gain. Pirates found thrill and excitement through software piracy, releasing cracked software and stockpiling the largest library of "warez" as possible (Goldman, 2003).

In 1982 *Time* magazine named the computer "Machine of the Year"; the first and only one of two times the "Person of the Year" award has been given to a non-human (Reimer, 2005; Person of the Year, 2006). While the true "birth" of the Internet was in 1983, it still had a long way to go before becoming the Internet as it is known today.

Internet access was still unavailable to the general public. At this time, the Internet was still restricted by a set of rules known as the Acceptable Use Policy, or AUP. The AUP only allowed the use of the Internet for academic purposes, banning all commercial use. However, private non-Internet network access was available through a number of service providers such as GEnie, CompuServe, Prodigy and later America Online. In 1989 the AUP restrictions were lifted, paving the way for the first true Internet Service Providers (ISPs) (Hannemyr, 2003).

In 1991, Tim Berners-Lee announced the details of the World Wide Web project, and shortly after in 1993 Marc Andreessen released Mosaic – the first popular Web browser (Berners-Lee, 1991). The Web was a near immediate success, bringing the power to easily publish material on the Internet to a booming Internet population. In 1994 and 1995, the major private network service providers connected their networks to the Internet, providing Internet and Web access to millions of existing customers (Hannemyr, 2003). Berners-Lee's innovations drove true widespread adoption of the Internet, setting the stage for the eventual widespread adoption of Peer-to-Peer (P2P) technologies. Average non-technical people flocked to the Internet, drawn by the World Wide Web. While truly accessible digital and audio were still a long way off, many of these new Internet users would eventually become P2P users.

Beginning in the 1990's, the software industry was beginning to take the growing digital piracy problem more seriously as well. The pirate BBS scene had peaked, and software pirates were then flocking to the commercialized Internet – abandoning BBS systems for File Transfer Protocol servers and Internet Relay Chat. In 1993, a MIT

student, David LaMacchia used several MIT systems to host a pirate BBS known as Cynosure. Noticing the unusual behavior, MIT notified the FBI. LaMacchia was later indicted on one count of violating the wire fraud statute, which prohibited the use of interstate lines for fraudulent purposes (*United States of America v. LaMacchia*, 1994). This strategy was the only one available to the prosecution, as the copyright law did not then cover acts of infringement that were not committed specifically for financial gain. After just over a month of operation, the government estimated that the Cynosure BBS system had been used to illegally copy more than $1 million worth of software (Goldman, 2003). Despite the value of the software itself, the indictment failed to cite any financial gain on the part of LaMacchia during the BBS operation. LaMacchia was charged by the government under the wire fraud statute, but LaMacchia's defense argued that the wire fraud statute did not apply to the case due to the lack of financial gain or commercial advantage. Furthermore, the defense argued, interpreting the wire fraud statute to protect copyright would render it unconstitutionally vague and previous court cases had already set the precedent that copyrights could not be infringed upon through fraud (*Dowling v. United States*, 1985). The judge accepted the defense's argument, and the case was dismissed (*United States of America v. LaMacchia*, 1994; EFF, 1994; Hoag, 1995).

The dismissal of the LaMacchia case, along with the threat that digital piracy posed to the software industry, spurred software copyright owners to seek the assistance of Congress. Congress first responded by passing the No Electronic Theft Act in 1997. Until this time, copyright law was designed to punish those who duplicated copyrighted

works for financial gain, allowing those who gained nothing financially while infringing upon copyright to slip through the legal system. In the act, the definition of financial gain was modified to include the receipt of anything of value, including copyrighted works and criminalized the duplication and distribution of works valued at over $1,000 (The No Electronic Theft ("NET") Act, 1997). While the act was specifically designed to close the “LaMacchia loophole,” it was ineffective in reducing piracy rates despite a number of convictions in the years that followed (Goldman, 2003).

The NET act marks the end of the new crime phase for digital copyright infringement. By 1997, the unauthorized duplication of software was widely recognized as a criminal act, but still generally misunderstood. Many major software developers also began attempts to combat the growing problem of piracy by requiring registration keys when installing software. Microsoft began communication efforts describing the impacts of software piracy as illegal copies of the popular Windows95 operating system became an increasing problem ("In 1997, Software," 1998).

Following the creation of the NET act, law enforcement began to push towards eliminating the problems of digital copyright violation. However, policing digital copyright infringement proved to be extremely difficult for law enforcement. As policing efforts increased, pirates quickly adopted increasingly complex technologies to avoid detection and identification. Warez traders frequently used hacked servers to “bounce” their connections to IRC servers, obscuring their true IP address and location from law enforcement. Private e-mail and chat servers were created by the traders, and many began to encrypt their communications to prevent wiretapping and sniffing efforts by the

government ("Illegal 'warez' Organizations," 2002). The adoption of new technologies by the pirates and warez traders forced law enforcement officers to undergo the more difficult task of infiltrating warez groups by posing as new recruits. While this method was largely successful, groups of warez traders proved to be extremely close-knit, and suspicious of outsiders (McCandless, 1997).

While the NET Act successfully led to the prosecution of approximately 80 software pirates, including a number of high-profile piracy group members, the rate of piracy continued to rise even during the time the cases in violation of the act were being prosecuted (Goldman, 2003). Furthermore, the seemingly more serious crime of piracy for commercial gain went largely unnoticed. However, the actions taken were initial attempts of protecting copyright in the face of changing technology, and more effective legislation was to follow.

The No Electronic Theft Act was quickly followed in 1998 by what is now one of the most criticized pieces of legislation effecting digital copyright: the Digital Millennium Copyright Act (DMCA) (Lessig, 2005). The DMCA is the direct result of what is quite literally the Berne Convention of its time – the World Intellectual Property Organization (WIPO) Treaties (Lutzker, 2005; Pember, 2006). The sections of the DMCA causing the highest impact on digital piracy are the anti-circumvention provisions and the “Safe Harbor” provisions for Internet service providers. At this time, the intellectual property industries had been developing new technologies to help protect their copyrighted materials from pirates. In order for the pirates to convert the copyrighted property into a digital format that can then be used universally, the copyright

protections must first be circumvented. The anti-circumvention provision in the DMCA prohibits the circumvention of these measures and the distribution of devices that are specifically designed to do so. For example, this would make it illegal for pirates to decrypt an encrypted DVD in order to make illegitimate copies. However, the same law makes it illegal for legitimate consumers to make a backup of the same DVD or to transfer that DVD to another medium, which is the primary reason the DMCA has drawn criticism. The “Safe Harbor” provision specifically protects Internet service providers from liability when their users illegitimately transmit or make available copyrighted data via the Internet (Digital Millennium Copyright Act, 1998; US Copyright Office, 1998).

Only one year following the introduction of the DMCA, in September 1999 19-year-old Shawn Fanning released the peer-to-peer (P2P) application that would forever change the face of the music industry – Napster. Napster was a simple application that indexed the music files on users' PCs, transferred that information to a central database, and allowed users to search that database for access to the songs that they wanted. If a user requested a file from another user, the two users' PCs would transfer the file between themselves rather than using an intermediary device to transfer the file. Theoretically, this would absolve Napster of all legal liability, as none of the copyrighted material was transmitted through the centralized Napster database.

In terms of technology adoption, the timing of the Napster release could not possibly have been better. Inexpensive home PCs had become powerful enough to play digital audio and their storage capacities had grown to a point where a sizable digital audio archive could be stored easily. The MPEG Audio Layer 3 format had already

gained some popularity on the Internet, compressing what were once large and unmanageable digital audio files into smaller, easy-to-transfer ones. Most colleges and universities had implemented high bandwidth networks across their campuses to provide Internet access to a new generation of students. Internet service providers were beginning to offer high-speed access through cable modem and DSL technologies. Napster spread from college to college and home to home – the number of Napster users doubled every five to six weeks, reaching 20 million users within the first year of operation. Seeing the popularity of Napster, other P2P applications began appearing and gaining momentum. New clients and networks such as Kazaa, Morpheus, Gnutella and eDonkey all released clients for a variety of P2P networks, each quickly gathering users (Honigsberg, 2002; Green, 2002).

Napster was particularly popular on college campuses, where broadband Internet access was easily available. The issue of P2P music piracy became so prominent that both the US Senate and the US House of Representatives began holding hearings centered on music and the Internet (*Music on the Internet*, 2000; Oversight *Hearing on Music*, 2001). In 2001, what was once the Subcommittee on Courts and Intellectual Property on the Committee on the Judiciary, U.S. House of Representatives became the Subcommittee on Courts, *the Internet* and Intellectual Property. The issue of infringing P2P use on college campuses became such an issue, that the House subcommittee would later focus specifically on it (*Oversight Hearing on Peer-To-Peer*, 2003).

The music industry also saw the oncoming threat and immediately began to take legal action against Napster. The prosecution argued that Napster was liable for

contributory and vicarious copyright infringement, while Napster denied any liability by way of the Audio Home Recording Act. By July of 2001 Napster, or at least the true P2P file sharing network that had been Napster, was rendered completely inoperational by an injunction issued by the U.S. Ninth Circuit Court due to Napster's active role in indexing the illegitimate content made available on the network (*A&M Records v. Napster, Inc*, 2002). The music industry had won the battle, but what had become a war on piracy was still raging. While the Napster network was shut down, its millions of users were simply displaced to other welcoming P2P networks.

Amidst the Napster legal battles, at a hacking conference Bram Cohen announced a new open source project, known as BitTorrent (Thompson, 2005). The BitTorrent protocol was a revolutionary new method of transferring large files among a large number of users. In a process known as swarming, each file transferred via the BitTorrent protocol is split up into small parts and transferred between each user attempting to download the file. Rather than each user downloading from one host, each user trades pieces of the file with each other – distributing the bandwidth costs across the group. While Cohen originally developed the protocol simply as an attempt to make large file transfers more efficient, BitTorrent was quickly adopted by Internet users for downloading copyrighted works. More efficient file transfer speeds was not the only benefit for BitTorrent users – the new protocol also made detection and identification more difficult for law enforcement. Furthermore, the swarming method creates an interesting legal dilemma. As most BitTorrent users fail to actually share every part of a file to any other user, how many parts must a user share in order to violate copyright?

Here again a technology is developed that facilitates digital copyright infringement in a new, more complex way while increasing the incidence of the abuse by making it more convenient.

The potential seriousness of the growing piracy problem had not entirely escaped law enforcement agencies, as they began making their own attempts at managing the new criminal behavior. Three simultaneous, but separate, law enforcement actions were conducted around the world on December 11, 2001, targeting major digital piracy and warez groups. These actions were known as Operation Buccaneer, Operation Bandwidth and Operation Digital Piratez. A broad range of enforcement agencies took part in the operations, including the US Customs Service and Federal Bureau of Investigation. A number of apartments on college campuses were raided, Rochester Institute of Technology being one of the colleges. The operations were successful, resulting in dozens of indictments against key individuals in the piracy distribution chain (*Federal Law Enforcement*, 2001). Unfortunately, these actions only served to send piracy group members into hiding, rather than actually preventing any illegal P2P sharing by the wide majority of average users.

Faced with an overwhelming amount of music piracy, and a general reluctance by the government to make an attempt at prosecuting millions of illegal file-sharers under federal statutes, the music industry was forced to take further action. In September of 2003, the RIAA announced its intentions to begin individually suing P2P users engaged in infringing behavior. The RIAA was widely criticized for the move to suing individual users, further adding to the already poor perception of the music industry. The RIAA

settled the wide majority of these cases out of court, typically for a sum of $3,750, despite the fact that the RIAA would normally receive an average of only $0.70 per song (Beckerman, 2006). Further fueling the criticism were specific cases that seemed particularly unfair or ridiculous, including suits against disabled single mothers (Beckerman, 2005), non-computer owners (I. Thompson, 2005) and one dead woman (Orlowski, 2005). In the month that the RIAA began suing individual file-sharers, the average number of simultaneous users on P2P networks had risen to nearly 4.5 million (Mennecke, 2006; Resnikoff, 2006).

As mentioned previously, it was during this time that university administrators were being asked to begin taking steps to manage the rampant piracy issues on nearly every campus network (*Oversight Hearing on Peer-To-Peer*, 2003). The administrators found themselves in a difficult position; cracking down on illegitimate P2P file sharing through technological or regulatory means would make their organization seem less attractive to both current and prospective students. However, university administrators were feeling pressure from both the intellectual property industries and the federal government to do so. In this situation, many colleges began to consider providing access to legal music downloading alternatives to P2P. Penn State became the first in 2003 to collaborate with the newly reformed Napster to provide such a service ("Penn State and Napster," 2003). Following Penn State, many other universities began subscribing to legal music downloading services (*Oversight Hearing on Reducing*, 2005). In 2004, RIT contracted with Cdigix, Inc. to provide the Ctrax digital music service to their students (Daneman, 2004).

As the RIAA continued suing individual P2P users, the average PC became more and more powerful, and average bandwidth to the home was on the rise. Digital music files were no longer the only type of content being shared via P2P networks; digital video was being shared as well. Full length movies and television shows could be encoded and distributed in hours. The issue of illegal P2P file sharing was no longer a problem faced only by the music and software industries. As such, in 2003 the Motion Picture Association of America (MPAA) began their own lawsuit against a company profiting from digital audio and video piracy: Grokster (*MGM v. Grokster*, 2005).

The major difference between Napster and Grokster (which used the FastTrack network) was the topology of the file sharing network each used to index and transfer shared files. While Napster had a central indexing server, and could be accused of actively facilitating illegal copyright infringement, Grokster was entirely decentralized – a true P2P network. However, Grokster was a for-profit company and generated advertising revenue from advertisements displayed on the software client. Before arriving at the Supreme Court, Grokster had won against MGM twice in the lesser courts – with each case being dismissed on the grounds of the *Sony Corp v. Universal City Studios* case in 1984. The Sony case protected VCR manufacturers from liability when VCR owners used VCRs to violate copyright (*Sony Corp v. Universal City Studios*, 1984*;* Oppenheimer, 2005). However, the Supreme Court ruled that Grokster did hold secondary liability for encouraging and facilitating direct infringement by its users, and then profiting by doing so (*MGM v. Grokster*, 2005). This decision prevents file sharing services from profiting off wide scale infringement of copyright, while at the same time

maintaining the ability for non-profit P2P networks to operate regardless of the content being distributed.

The Supreme Court decision against Grokster, while drawing attention among some of the more technically savvy groups on the Internet, failed to make an impact upon the larger segment of average P2P users. As Grokster was forced to cease distribution of their client, P2P users simply migrated to another freely available client or network. Judging by the incredible growth in P2P use, neither had the ongoing lawsuits by the RIAA (McQuade, 2006). In the month that the Grokster case was decided, the average number of simultaneous P2P users had reached nearly 9 million - over twice the number of users than when the RIAA began the civil suits (Mennecke, 2006; Resnikoff, 2006).

With legal efforts on behalf of the intellectual property industries largely failing to have an impact on digital copyright infringement, there has been a slow movement towards modifying communication technologies in order to restrict the use of digital content. Concepts such as Digital Rights Management (DRM) and trusted computing have become extremely popular among communication device manufacturers and the intellectual property industries. DRM and trusted computing technologies restrict the methods by which legally obtained digital content may be accessed, copied or transferred from person to person.

Circumvention of DRM protections is a criminal act under the DMCA (Digital Millennium Copyright Act, 1998). This potentially places many acts that would normally fall under the category of fair use, such as creating backup copies of DVDs or converting content from one media format to another (“*Unintended Consequences: Seven”*, 2006).

Merely the act of examining copyright protection systems for academic purposes can result in swift legal retaliation by the industry (Slater, 2006). Furthermore, some of the DRM systems in use by the intellectual property industries have been found to actually circumvent computer security, creating vulnerabilities that may be exploited by attackers. When such a system is utilized for popular music releases, as in the case of Sony's DRM kit, the security flaws could easily poke holes in corporate computer security efforts worldwide (Russinovitch, 2005).

Even today, technologies that make the job of policing digital copyright infringement increasingly difficult are being developed. Methods of encrypting BitTorrent traffic are being developed, making it more difficult for ISPs to detect and filter BitTorrent traffic ("BitTorrent Protocol Encryption," 2006). Rather than using global, public P2P networks, many users are turning instead to local, private P2P networks. Within these networks, files may be shared with reduced risk of discovery by the intellectual property industries ("Music, Movie Industries," 2006). Furthermore, software is being developed with the specific purpose of “muddying the waters of the digital copyright debate” (Rohrer, n.d.). This software, known as Monolith, accepts two binary files (e.g. digital video, digital audio, software) as input and outputs a file that contains none of the information found in the two input files. Theoretically, this new file constitutes an original work. However, by combining the output file with one of the original input files, the second input file may be recovered. By combining a copyrighted work with a work freely available within the public domain, an original work may be

created that can be legally distributed. In order to retrieve the copyrighted work, a user simply needs the public domain text that it was originally combined with.

The history of digital copyright violation is marked by increasingly rapid incremental innovations in content distribution technology. These technologies are facilitating a wave of intellectual property crime, one that has been rising for over two decades with no end in sight. The speed at which the collaborative efforts of the Internet can adapt and change remains too much for the legislative and enforcement abilities of government to effectively manage the abuse of digital distribution systems. As such, the intellectual property industries are being forced to manage the abuse of their copyrighted works through legal action and slow changes to the ways in which content may be accessed through technology.

Impacts of Digital Copyright Infringement

Computer crime and abuse has been ongoing nearly as long as the development of computers themselves, with the first recorded case of computer abuse occurring in 1958 (Parker, 1984). As is the case with many new forms of crime, it is believed that many cases of computer crime and abuse initially went unnoticed or not prosecuted due to a lack of understanding about computer crime and abuse (Parker, 1984; McQuade 1998). Since then, computer crime and abuse have taken on a variety of different forms. The complex nature of computer crime makes categorization and definition extremely difficult; however, many forms of computer crime and abuse are simply traditional crimes performed with updated technology.

Digital music copyright violation is a fairly recent phenomenon, not truly becoming apparent until the infamous Napster peer-to-peer file-sharing network was developed in the fall of 1999. From the popularity of Napster sprung dozens of similar peer-to-peer networks, both commercial and open-source. At approximately the same time, music sales began to drop drastically, with total number of units sold falling by 10% in 2001 (Liebowitz, 2003).

While at first glance, the immediate drop in sales may appear to be the result of file-sharing, the studies done on the topic are divided. On one end of the spectrum, an analysis performed by Liebowitz (2003) has concluded that illegal file-sharing was essentially the main force behind the sales drop. Liebowitz came to this conclusion without attempting to measure on actual illegal music downloading activity or analyzing existing data on the subject. For this reason, his results have often been criticized. In opposition to the Liebowitz analysis, another study by Oberholzer-Gee and Strumpf (2004) conclude that illegal file-sharing has no impact on the music industry whatsoever. Zentner (2003) however, concluded that file-sharing has some smaller impact on the industry, while failing to explain the entire observed decline in sales (Hui, 2002; Boorstin, 2004; Petiz, 2004; Rob, 2004). Private studies performed by the recording industry have been largely unreleased, but it has been reported that a study requisitioned by one of the four major music labels reached the same conclusions as Oberholzer and Strumpf (2004) (“Music’s Brighter Future”, 2004).

Theoretical Explanations for Digital Piracy Behavior

It has been just over five years since the rise and fall of Napster and downloading music continues to be a popular activity among Internet users, with 32% of Internet users participating in 2002 (Madden, 2003)[1]. Despite the continued popularity, media attention and legal threats, empirical research involving digital music piracy via peer-to-peer networks is scarce. However, researchers have been studying computer crime and abuse since the late 1960s, many of whom in some way measured software piracy and copyright violation. In particular, of the few studies that have been performed on computer abuse, social learning theory has been tested as a model for explaining computer crime.

In the disciplines of psychology and communication, social learning theory is most commonly associated with the studies of Albert Bandura (Littlejohn, 1983). Bandura's social learning theory states that both deviant and normative human behavior is learned through a combination of observed behavior, communication with others, encounters with disciplinary action and cognitive modeling (Bandura, 2001; Siegel, 2001). Essentially, people gather information about the potential outcomes of any given behavior from a variety of sources, including both other people and media, and use that information to make assumptions about the outcome before engaging in that behavior themselves. Without this capacity for learning by example, Bandura argues that human development would have been severely retarded, tedious and hazardous. Without social

[1] Unfortunately, Madden's study fails to mention if the music downloading is legal or illegal, only that 32% of Internet Users had reported doing so as of October 2002.

learning, humans would have no method for learning beyond simple trial and error (Bandura, 2001; Grusec, 1992).

Bandura was primarily interested in applying social learning theory to deviant behavior, violent behavior in particular. He hypothesized that when exposed to a model engaged in violent behavior with no observable consequence, people would be more likely to engage in violent behavior themselves. In order to test this hypothesis, Bandura devised the study that for which he would later become most well known for – the bobo doll study. In this study, Bandura first exposed children to a model engaged in violent behavior against a “bobo” doll, either in person or through film or television recordings (Bandura, Ross & Ross, 1961). The study found that after being exposed to a violent model, either through face-to-face interaction or by viewing the model on film or television, they were more likely to engage in violent behavior against the bobo doll themselves when left in a room without supervision (Bandura, Ross & Ross, 1961; Griffin, 1991; Reiner, 2002).

In the field of criminology, scholars have taken the concepts provided by Bandura and further refined them to more clearly explain the processes by which deviant behavior is modeled and imitated. Combined with Sutherland's (1947) differential association theory, Akers has developed an extremely well received theory, which has proven useful for empirically explaining many different types of criminal and deviant behavior. (Akers & Jensen, 2005). In particular, Akers' version of social learning theory has become one of the most commonly used theories for explaining computer crime and abuse, which may

be of interest to both communication and criminology scholars alike (Hollinger, 1993; Skinner & Fream, 1997; Rogers, 2001).

Like Bandura, Akers assumes that the same process of learning leads to both conforming and deviant behavior. However, Akers further operationalizes Bandura's concepts of observed behavior, communication with others, encounters with disciplinary action and cognitive modeling. Akers version of social learning theory specifies four separate theoretical constructs: differential association, differential reinforcement, definitions and imitation. Differential association is the amount of exposure to deviant attitudes and behavior an individual gains by associating with someone who regularly participates in the aforementioned deviant behavior. Again, this may include the mediated observation of others engaged in deviant behavior, such as television watching or Internet use (Hollinger & Lanza-Kaduce, 1988, Skinner & Fream, 1997). Differential reinforcement refers to rewards that an individual perceives will be gained through participating in the deviant behavior. Definitions are attitudes towards a deviant behavior, either positive - where the behavior is deemed entirely acceptable or neutralizing - where the behavior is excused or justified. Finally, imitation refers to the recreation of deviant behavior based on observed behavior by others (Akers, 1998).

While having no true theoretical testing component, the first empirical study on computer crime and abuse was performed in 1989 by Richard C. Hollinger. Hollinger’s study focused on only two dimensions of computer abuse, unauthorized access and software piracy, and only covered a period of four months. Even then, before personal computers had truly become ubiquitous, it was found that 10% of the 1,672 student

sample reported being in some way involved with software piracy. Extrapolated out against the entire student population, Hollinger calculated that there were 3,500 incidents of felony piracy on the campus every four months (Hollinger, 1993).

Following Hollinger's lead, Skinner and Fream (1997) performed a second statistical study of computer crime. This study not only expanded upon Hollinger's original questionnaire by measuring more than two forms of self-reported computer abuse, but also by introducing a theoretical explanation for computer abuse. Specifically, Skinner and Fream explored the use of social learning theory as a tool for explaining computer abuse. Once again, a high prevalence of self-reported software piracy was found, with 41.3% of respondents admitting to using, copying or giving away pirated software. When used as a model for computer abuse, social learning theory was found to explain 37% of the variance in software piracy with all of the variables entered into the regression model. As a whole, when gender was entered into the regression model first, followed by the social learning constructs, social learning theory explained 90% of the variance in the combined reported computer abuse when gender did not have a significant effect (Skinner & Fream, 1997).

Skinner and Fream were not the only researchers to explore the use of social learning theory to explain computer abuse. In a doctoral thesis for the University of Manitoba, Marcus K. Rogers compared self-report survey results from known computer criminals and non-criminal Internet users. In his surveys, Rogers included questions that tested for differential association and differential reinforcement, along with a number of different deviant computer behaviors. Again, piracy was found to be the most prevalent

crime out of the eight listed on the surveys. Rogers also found that past criminals did have higher levels of differential association and differential reinforcement than non-criminals (Rogers, 2001).

A subsequent study (Higgins & Makin, 2004) also found components of social learning theory to be integral to understanding software piracy. Using a convenience sample of 318 respondents from two classes open to all undergraduate students on a university campus, Higgins and Makin tested both social learning theory and components of control theory as a model for software piracy. Based on the data gathered from the surveys, it was concluded that differential association was extremely important in determining software piracy behavior. Positive definitions of software piracy were also found to have a significant influence over an individual's reported involvement in software piracy (Higgins, 2004).

Another study on computer use and ethics that included a social learning theory component was performed in April of 2004 on the Rochester Institute of Technology campus. Questions on attitudes and behaviors regarding multiple types of computer abuse and crime, including digital software piracy, digital movie piracy and digital music piracy were answered by 873 randomly selected students. In accordance with previous studies performed by Hollinger (1993), Skinner & Fream (1997) and Rogers (2001), items that tested the applicability of social learning theory to computer abuse behavior were included in the questionnaire (McQuade, 2004).

Definitions (as defined by social learning theory) were gathered through questions that asked respondents to rate their agreement with statements such as "It is OK for me to

pirate commercial software because it costs too much for me to buy" on a five-point Likert-like scale, which was followed by questions asking the respondent to rate certain kinds of computer behavior on a five-point Likert-like ethical scale. Differential association was measured by asking respondents to list what percentages of their friends were performing certain types of computer abuse, along with questions asking respondents to rate how acceptable their friends, family and other adults would find their participation in the same types of computer abuse on a five-point approval scale. Imitation was measured through questions requiring respondents to write in the number of times they had performed a given computer activity within the past year. Differential reinforcement was measured through questions asking how likely it was that respondents would be caught engaging in different types of activities, and how severe the punishment for engaging in those activities would be if they were caught (McQuade, 2004).

The data generated for this particular study have yet to be fully analyzed, but initial findings again show an extremely high prevalence of intellectual property crime. Digital music piracy was the most prevalent of all crimes and abuses listed on the survey, with over 50% of the respondents reporting that they had shared music over 30 times in the past year. The survey also asked how much students would be willing to pay for a music downloading service, to which over 40% of the students responded zero dollars (McQuade 2004).

Method

This study asks the following research questions:

- Does social learning theory provides an applicable model for describing perceptions and behaviors regarding illegitimate P2P use?
- Are there significant differences between the perceptions and behavior of students who are enrolled in the legal downloading service versus those of students who are not?

In order to answer these questions, a survey instrument was developed. As part of an ongoing effort to measure computer use, abuse and victimization on the RIT campus. As such, the survey largely mirrored that of the original RIT Computer Use and Ethics survey (McQuade, 2004). Some of the questions from the original measure certain constructs specifically applicable to this study, while others extend on earlier questions. In addition to the items taken from the original RIT Computer Use and Ethics survey, the author designed items specifically to measure the four constructs of social learning theory. The format of these questions were taken largely from studies conducted by Skinner & Fream (1997) and by Rogers (2001). For the complete survey instrument and more specific information on response sets and scales, please see *Appendix A – Survey Instrument.*

The first set of questions relevant to this study measure the four constructs in the social learning model - Differential association, imitation, definitions, and differential reinforcement. Items 12 and 97 measured differential association. Item 12 measured the

approximate proportion of friends of the participant who engaged in music sharing via P2P networks. The responses choices were none, about 25%, about 50%, about 75% and nearly all. Item 97 measured the approximate percentage of friends of the participant who engaged in unauthorized music sharing. The responses were placed on a 7-point Likert-like scale ranging from 0% to 76+%. Item 13 measured imitation by requiring participants to describe how frequently they observe unauthorized music file sharing via P2P networks. The possible responses ranged from more than once per day, once per day, once per week, 2-3 times per week, once per month, less than once per month, to never. Definitions were measured through item 77 by asking respondents to indicate how ethically wrong they perceived engaging in unauthorized music file sharing to be. Responses were placed on a 5 point Likert-like scale ranging from not wrong to very wrong. Differential reinforcement was measured through items 140a and 140b. Item 140a asked for the participant's perception of the likelihood of being discovered by authorities for sharing files. Responses were placed on a 5 point Likert-like scale ranging from not likely to very likely. Item 140b asked for the participant's perception of the severity of punishment they would expect to receive of discovered by authorities. Responses were again placed on a 5 point Likert-like scale ranging from no punishment to severe punishment.

The second set of questions relevant to this study measured the extent to which respondents engaged in illegal music file sharing behaviors following the implementation of Ctrax at RIT. Item 11 asks participants if they generally understand what P2P file sharing is, with yes and no as response options. Items 14, 16, and 17 attempt to measure

self-reported P2P music downloading behavior. Item 14 asks participants if they currently use a P2P application to download music, with yes and no as response options. If participants chose “no,” they were asked to skip to question 19. Item 16 measures how frequently respondents report using file sharing applications to share music, with seven responses ranging from more than once per day to never. Item 17 attempts to measure the number of songs that participants report having downloaded through a P2P network within the previous year. Response options range from 1-20 songs to more than 100 songs.

The final set of questions relevant to this study measured the extent to which respondents utilized the Ctrax music service. Item 19 asked respondents if they had even heard of the Ctrax service, with yes and no as the response set. Respondents who answered “no” were asked to skip past the remaining questions involving the Ctrax service. Items 21 and 22 were similar questions, asking users if they had ever logged on to the service, and if they had ever downloaded music through the service, respectively. Items 39 and 40 measured the number of songs that respondents reported having downloaded from the Ctrax music service. Ctrax users have the option of downloading a DRM protected song that may be played on a computer for no additional charge, or paying an additional fee to download the song in MP3 format, allowing them to play the song on other devices (*Ctrax Service Overview,* n.d.). As such, item 39 addressed the number of DRM protected songs a respondent had downloaded, while item 40 addressed the number of paid MP3 songs that had been downloaded. Each item had seven response options, ranging from none to more than 100 songs.

The sample set of students asked to participate in the survey was comprised of the full population of 744 Ctrax users along with an equal number of randomly selected non-Ctrax using RIT students. Both the identification of Ctrax users and the random sample of non-Ctrax users from the RIT student population was performed with the assistance of the RIT Information Technology Services (ITS) department. ITS is largely responsible for the administration of both the RIT e-mail system and components of the Ctrax service. As such, ITS was able to provide a list of the e-mail addresses of all Ctrax users, along with an equal number of randomly selected non-Ctrax users. Non-Ctrax users were selected from a list of student e-mail addresses that did not include the Ctrax population.

For distribution and administration, the RIT developed Web-based survey tool "Clipboard" was used. Previous studies on the RIT campus had previously made use of the same tool, and had shown that Clipboard was adequate for a similar study (McQuade & Fisk, 2005). An invitation e-mail was prepared by the principal investigator, Dr. Samuel McQuade, which was then sent under the name of the RIT Chief Information Officer, Diane Barbour. The full text of this e-mail may be found in Appendix B. Requests to participate in the survey were sent via e-mail to the entire sample of students, which included instructions and a direct hyperlink to the survey itself. The use of the Clipboard tool required each respondent to log in via their RIT DCE account user name and password. Upon completion, that user would no longer be provided with access to the survey, preventing duplicate results. The survey remained open for student access from April 12, 2005 until April 26, 2005.

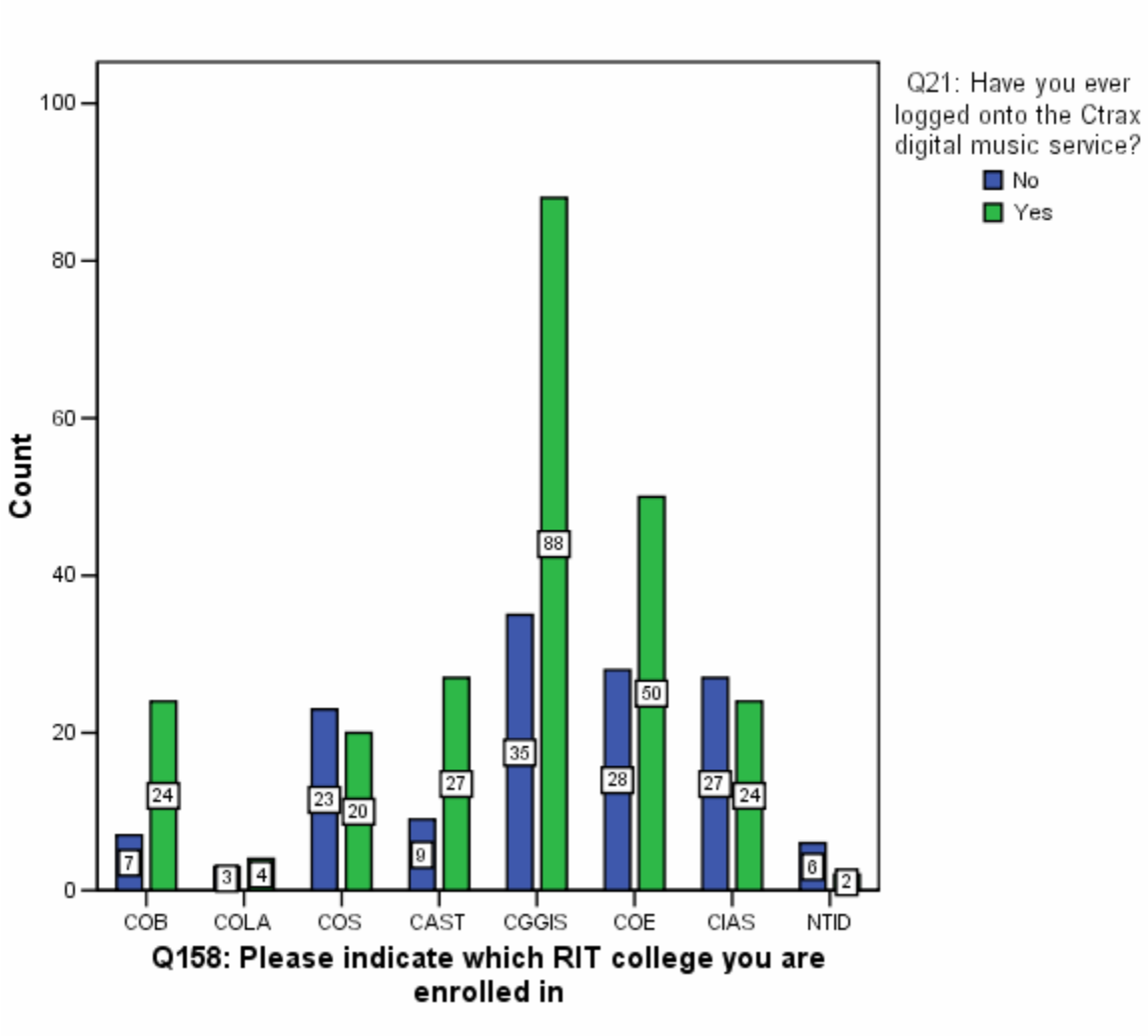
This method of administration was particularly appropriate for the RIT campus. The study is focused solely on RIT students, all of whom have Internet access in some way. More specifically, the study focuses on RIT students who are either actively pirating music, using the legal downloading service, or both. The behaviors being measured inherently require Internet access, so sampling problems resulting from non-Internet users failing to gain access to the survey are no longer an issue.

Analysis

Following the two week survey period, 447 students responded to the survey. Analysis of the demographical data indicated that a representative sample of the RIT population was obtained. The survey sample is approximately 70% male and 30% female, with a distribution across college enrollment and matriculation status that closely matches that of the entire RIT population (McQuade & Fisk, 2005).

The sample also has a near-equal distribution of both Ctrax subscribers and non-Ctrax subscribers, where 55% of respondents had actually downloaded music through Ctrax and 45% had not. All told, 33% of all Ctrax subscribers at RIT responded to the survey. Consistent with the distribution of student demographics at RIT, the highest concentration of Ctrax users came from the Golisano College of Computing and Information Sciences (GCCIS), with 20% (n=447) of the total number of participants enrolled there.

Figure 1. Sample Demographics



Prevalence of P2P & Ctrax Use

Nearly 96% (n=442) of the respondents responded that they had a basic understanding of P2P file sharing, and half (n=439) admitted to currently using a P2P file sharing application to share music. Of those who admit to currently using a P2P application to share music, half (n=254) do so at least once per week. Of those who share

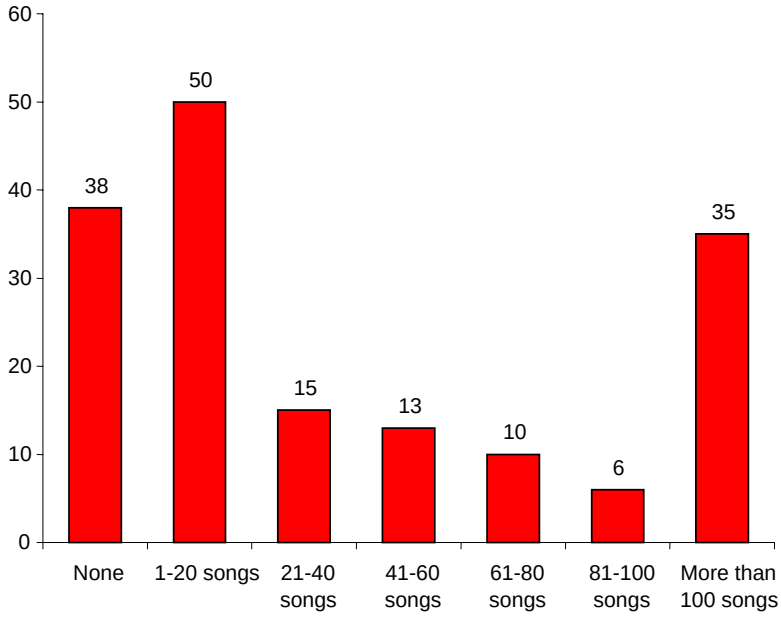
music via a P2P network, 8% responded that they share music via a P2P network more frequently than once per day.

When asked to indicate the number of songs that they had downloaded within the past year, 48% (n=225) of the P2P users responded that they had downloaded more than 100 songs. By multiplying the number of users who responded within each response choice by the highest and lowest numbers of songs downloaded listed for that response choice, it can be estimated that within this sample alone between 14,265 and 18,540 songs have been downloaded through a P2P service within the past year. When extrapolated out across 15,000 students at RIT, there are between 470,745 and 611,820 songs are downloaded through a P2P service per year. Considering that 120 songs was assumed to be the upper range for the "more than 100 songs" response, and that nearly half of the participants answered in that category, these estimates are highly conservative.

After one year of Ctrax availability to students, the wide majority of respondents knew of the service with 84% (n=442) reporting that they had heard of the service through some means. However, over half (63%) of the respondents to the survey were originally invited to participate specifically because they had logged on to Ctrax at some point. After controlling for Ctrax users, 88% (n=143) of the non-Ctrax users had at least heard of the service. Of the registered Ctrax users, only 56% (n=246) reported having downloaded a song through the service.

Similar to the distribution of data measuring the number of songs downloaded through P2P within the last year, the distribution of the data measuring the number of songs downloaded through Ctrax was bimodal.

Figure 2. Number of songs downloaded via Ctrax



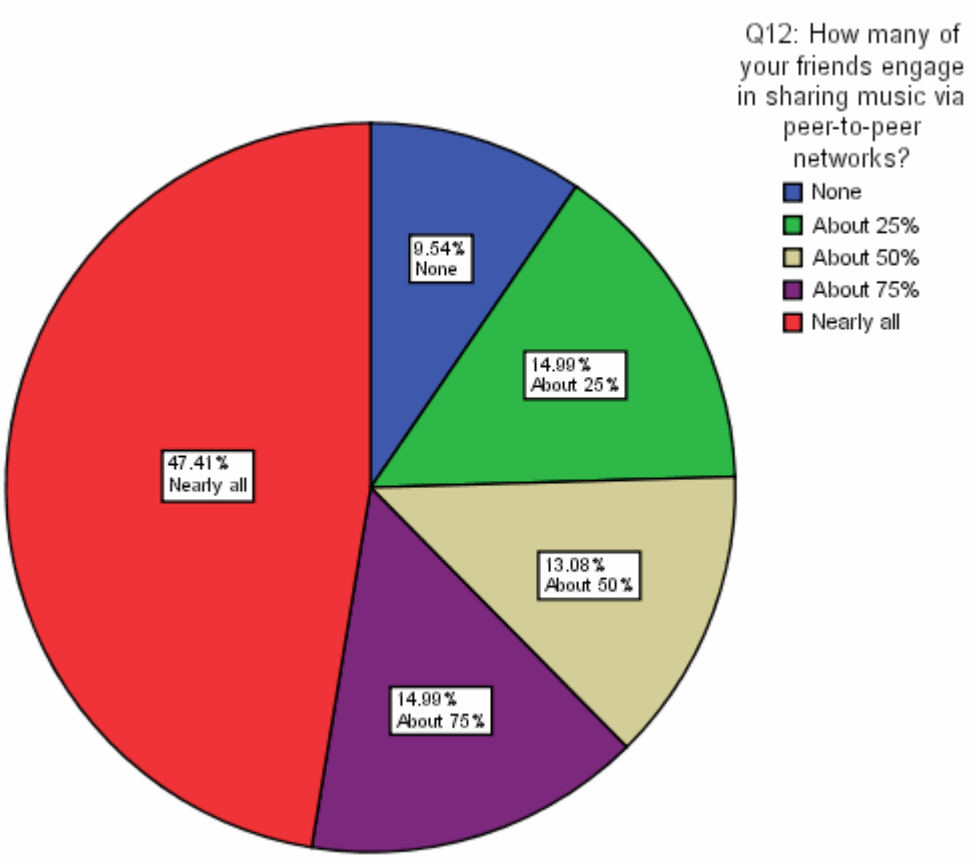
With a significant number of Ctrax users responding that they downloaded smaller or larger amounts of songs at each end of the scale this would seem to indicate that there are groups of relatively casual and core users. However, the group of Ctrax users at the high end of the legal downloading scale is still far smaller than users at the high end of the P2P downloading scale.

When Ctrax users were asked to indicate the number of songs they had actually purchased in MP3 format from the service, only a very small minority reported doing so. 89% (n=165) indicated that they had never purchased a song in MP3 format from the Ctrax service. Only three respondents indicated that they had downloaded more than 20 songs.

A Test of Social Learning Theory – Descriptive Statistics

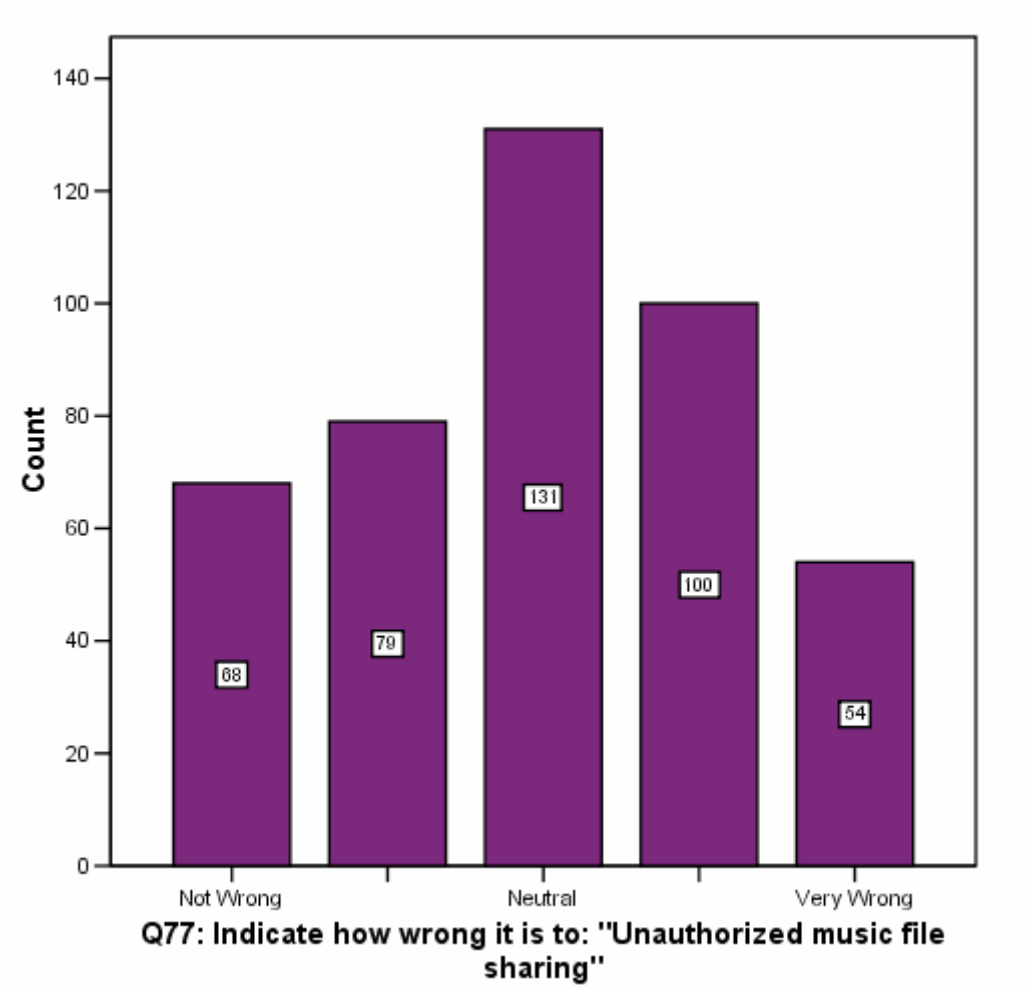
As described in the method section, items gathering data on each construct in the social learning model were included in the survey instrument. The first of these constructs is differential association. The data gathered from items 12 and 97 indicates that the social environment is largely supportive of unauthorized music sharing via P2P networks. When asked to approximate the percentage of their friends that engage in unauthorized music sharing via P2P networks, 47% (n=367) of respondents indicated "Nearly all" on survey item 12 (see Figure 1) and 46% (n=363) of respondents indicated "76+ percent" on survey item 97.

Figure 3. Differential association as measured by Q12



Definitions setting was measured through survey item 77, and again indicates a social environment supportive of unauthorized music sharing via P2P networks. The majority of participants found unauthorized music sharing to be generally acceptable or neutral, with responses (see Figure 2) falling in a normal distribution. 29% (n=432) found unauthorized music file sharing to be a “neutral” activity, while 16% found the activity to be entirely “not wrong.”

Figure 4. Definition setting as measured by Q77



Differential reinforcement was measured through items 140a and 140b. The data collected from these items indicates that respondents were generally unafraid of discovery or punishment for engaging in unauthorized file sharing behavior. The responses for item 140a (see Figure 3) were negatively skewed, with 58% (n=421) responding 2 or below on a 5 point likelihood of discovery scale, with 0 being “Not Likely.” The responses for 140b (see Figure 4) were more normally distributed, however

27% (n=417) indicated a 1, and 23% indicated a 2 on a 5 point severity of punishment scale with 0 being “No Punishment.”

Figure 5. Differential reinforcement as measured by Q140a

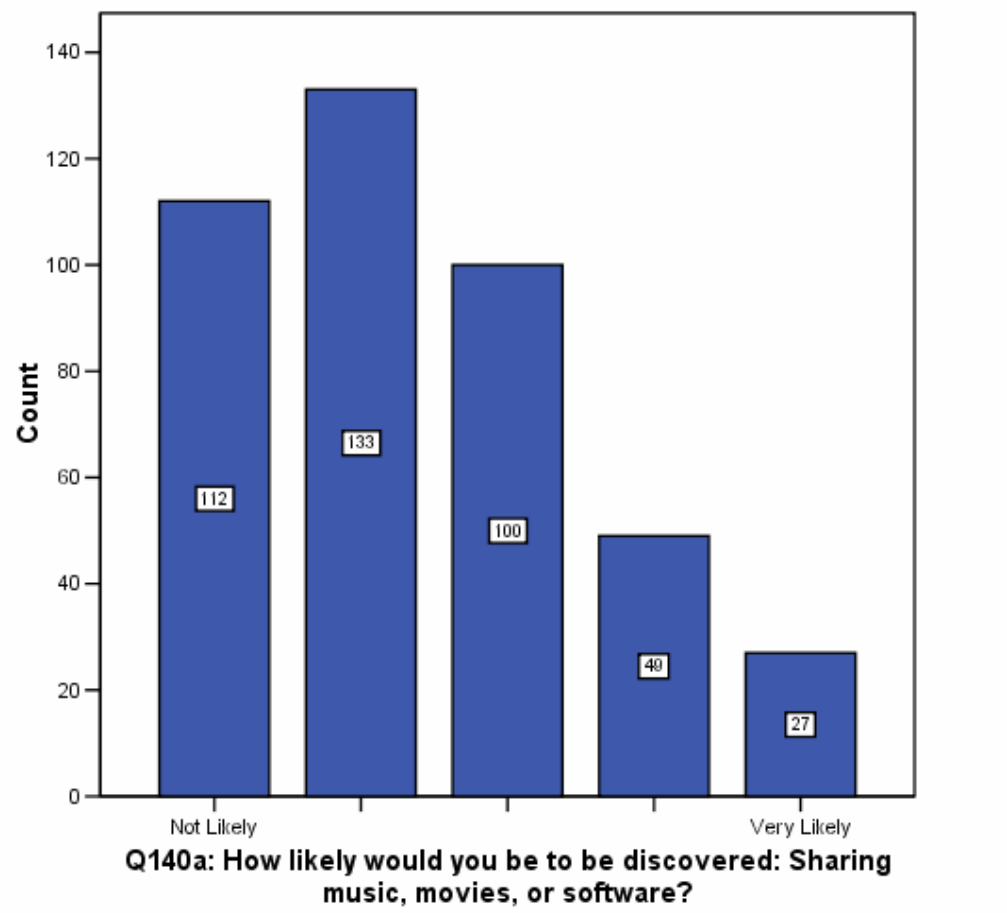
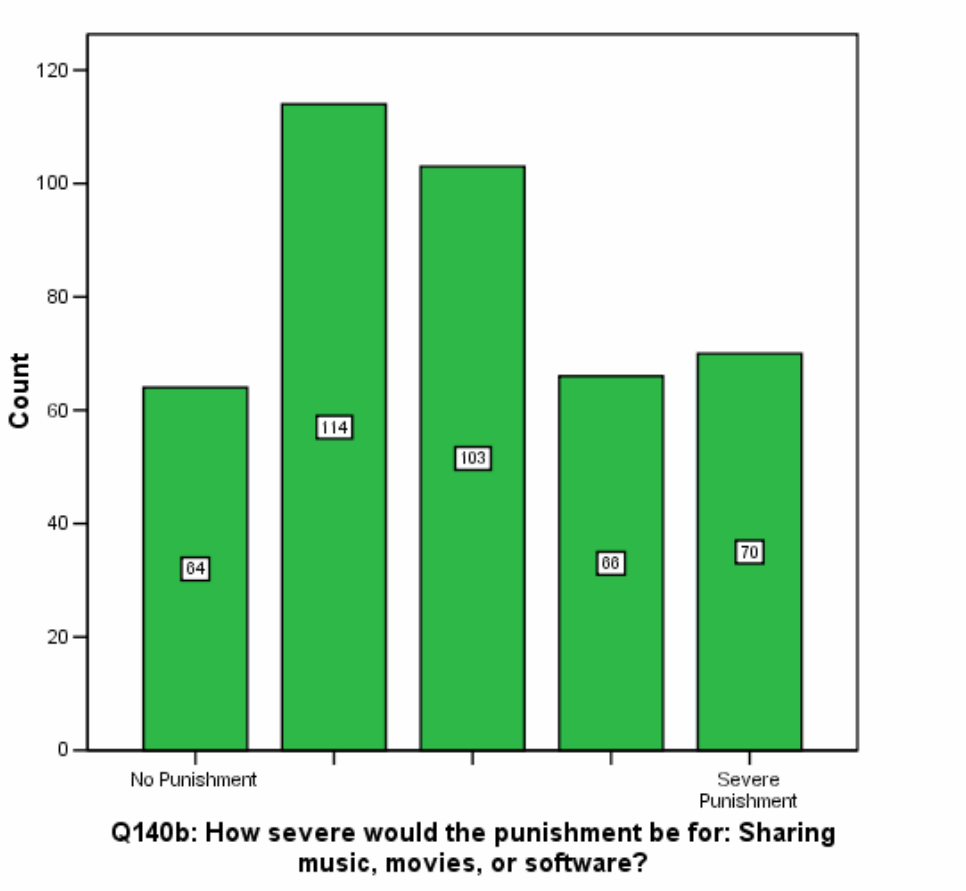
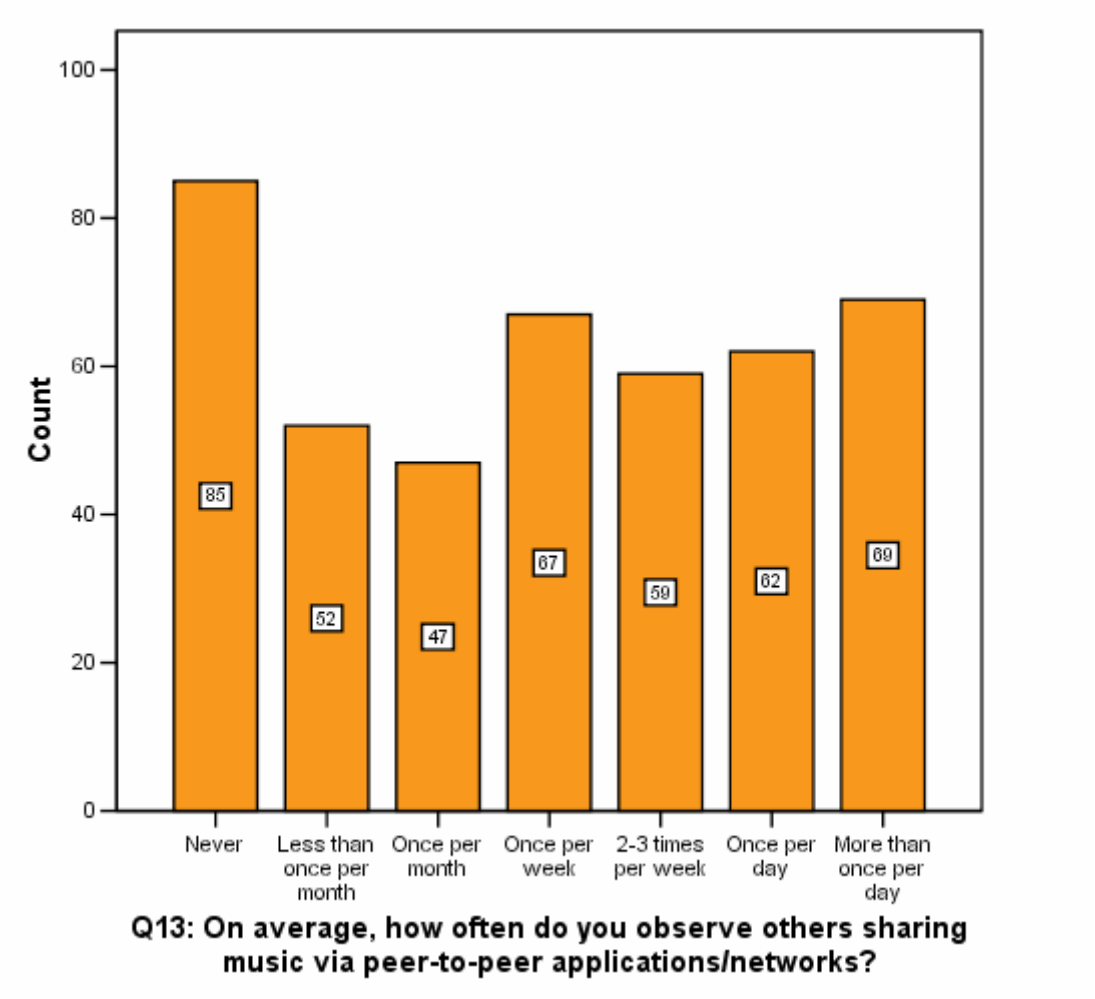


Figure 6. Differential reinforcement as measured by Q140b



Finally, imitation is measured through item 13. Here again the responses are normally distributed, which indicates that a significant number of the respondents are regularly exposed to P2P music sharing behavior. Only 19% (n=441) report never observing P2P music sharing behavior, while 58% observe P2P music sharing behavior at least once per week. This level of exposure would leave many opportunities for respondents to gain an understanding of the use of P2P clients and networks.

Figure 7. Imitation as measured by Q13



A Test of Social Learning Theory – Correlations

In order to test the applicability of the social learning model to unauthorized music downloading through a P2P network, a Spearman's Rho correlation was used to test for relationships between the four constructs. Significant positive correlations were found between:

- Differential Association as measured by item 12 and both frequency of P2P use to share music (r[230]=.337, p<.01) and number of songs downloaded via P2P (r[230]=.299, p<.01)
- Differential Association as measured by item 97 and both frequency of P2P use to share music (r[211]=.393, p<.01) and number of songs downloaded via P2P (r[230]=.409, p<.01)
- Imitation as measured by item 13 and both frequency of P2P use to share music (r[211]=.533, p<.01) and number of songs downloaded via P2P (r[230]=.395, p<.01)

Significant negative correlations were found between:

- Definitions setting as measured by item 77 and both frequency of P2P use to share music (r[211]=-.467, p<.01) and number of songs downloaded via P2P (r[230]=-.366, p<.01)
- Differential Reinforcement as measured by item 140a (likelihood of discovery) and frequency of P2P use to share music (r[211]=-.143, p<.05)
- Differential Reinforcement as measured by item 140b (severity of punishment) and frequency of P2P use to share music (r[211]=-.150, p<.05)

Beyond the relationships with P2P music sharing behavior, there exist significant relationships between each of the social learning constructs, with the exception of differential reinforcement. See Appendix C: Social Learning Theory Correlation Table for the full correlation table.

While the relationship between differential reinforcement and illegitimate music downloading behavior is weak, social learning theory provides and appropriate framework for explaining at least some illegitimate music sharing and downloading behavior. Overall, as students observe music downloading, socially interact with others engaged in music downloading, form neutralizing definitions of music downloading and fail to observe punishment for music downloading, the more likely they are to engage in music downloading themselves.

Perceptional and Behavioral Differences between Ctrax Users and Non-Users

In order to determine if significant perceptual or behavioral differences exist between Ctrax users and non-users regarding P2P music downloading and sharing, Mann-Whitney U tests were performed.

- No significant difference ($U=6111.5$, $p>.05$) was found between Ctrax users (Mean Rank=114.66) and non-users (Mean Rank=114.25) in terms of frequency of P2P music sharing
- No significant difference ($U=4965.0$, $p>.05$) was found between Ctrax users (Mean Rank=110.89) and non-users (Mean Rank=102.05) in terms of number of songs downloaded via P2P

- No significant difference (U=15798.0, p>.05) was found between Ctrax users (Mean Rank=195.67) and non-users (Mean Rank=183.05) in terms of how ethical engaging in unauthorized music file sharing is perceived to be

Summary of Findings

Significant correlative relationships were found between each of the four social learning constructs and illegitimate music downloading, supporting the applicability of the social learning model to illegitimate music downloading behavior. Of the four constructs, the strongest correlative relationship to illegitimate P2P behavior was with definitions setting, indicating that the less ethically acceptable students find illegitimate music downloading, the less likely they are to engage in that behavior. The weakest correlative relationship to illegitimate music downloading behavior was with differential reinforcement, indicating that likelihood of discovery and severity of punishment have little to no significant impact on illegitimate music downloading behavior.

No significant differences in unauthorized music downloading behavior or ethical perceptions were found between Ctrax users and non-users, suggesting that Ctrax use has limited or no impact on the perceptions or behaviors of RIT students regarding P2P use for unauthorized music sharing.

Limitations

This study does have a number of limitations. Most obvious of these limitations is that as a survey, the data collected were entirely self-reported. As with any survey attempting to gather data on deviant or criminal behaviors, there are issues with bias due to the potential reluctance of respondents to admit to engaging in the behaviors being mentioned. Furthermore, definitions of crime vary from respondent to respondent, particularly with newer forms of crime such as digital copyright infringement (Pepper & Petrie, 2003).

Further questions should have been included in the survey to more accurately measure the impacts of differential reinforcement on P2P behavior. Upon further examination of Akers' conceptualization of social learning theory, it seems that differential reinforcement cannot simply be measured by questions targeting fear of discovery. Rather, questions measuring respondent exposure to the repercussions of others being discovered while engaging in the deviant behavior should have been added.

The social learning construct of imitation could also have been better measured. While Skinner & Fream (1997) measured imitation in a similar manner, the item measuring imitation on the questionnaire merely measured exposure to a model, where imitation as defined by social learning theory is the mirroring of behavior that a model was observed engaging in. Measurement of imitation may prove difficult via a self-response questionnaire, as respondents may be unaware that they are actually modeling

behavior observed in others. It is assumed that increased exposure to a model leads to imitation of that model.

Coincidentally, only one day following the initial release of survey invitations to students, the Recording Industry Association of America (RIAA) announced its intentions to take legal action against 25 students enrolled at RIT citing copyright infringement issues. Following the announcement, there was a flurry of media activity surrounding RIT. Multiple reporters came to RIT questioning students about piracy behavior, their impressions of the actions taken by the RIAA and the Ctrax digital music service. This dissemination of information regarding legal actions towards copyright infringers is likely the true purpose of the RIAA legal actions. As such, the breaking news of impending legal action against P2P users at RIT may have influenced the survey results in some way.

Finally, the survey data are currently over a year old. The Ctrax service continues to be provided on the RIT campus, and the current state of illegitimate P2P use at RIT is largely unknown. In such a time, Ctrax may very well have started to make a significant impact on continued P2P use at RIT.

Implications for Policy and Program Services

The successful implementation of a digital content distribution system of this size and scope requires the collaboration of numerous organizational entities. Cdigix and RIT have both encountered obstacles through the process of bringing Ctrax to campus, such as early marketing issues and interface problems. Despite these earlier problems, Cdigix and RIT have done an exemplary job in providing RIT students with a useful and inexpensive alternative to unauthorized digital music sharing. Furthermore, the survey data indicate that while illegal P2P use is still a problem on campus, there are a number of students who are heavily using Ctrax as an alternative.

The survey data makes it immediately apparent that in order for Ctrax to make an impact upon digital music copyright violation on college campuses nationwide, it must itself gain acceptance via the same channels as P2P technologies – through a process of widespread social learning. A technological solution without a social foundation will have only limited success or it will simply fail outright. Just as P2P technologies have gained acceptance through socio-cultural means, so must the legal alternatives - a task easier said than done.

The survey data suggest that perceptions of likelihood and severity of punishment for illegal file sharing (differential reinforcement) are only weakly correlated with illegal file sharing behavior. However, perceptions of how ethically wrong illegal file sharing is had the strongest relationship with illegal file sharing behavior. As such, in the short term RIT ethics training and education designed to reduce illegal file sharing on campus should focus more strongly on portraying illegal file sharing as ethically wrong, rather

than highlighting the likelihood and severity of punishment for engaging in illegal file sharing. Unfortunately, the defensive legal tactics of the RIAA have placed a strong emphasis on punishment through thousands of expensive law suits, rather than modifying the definitions of illegal file sharing. One recent, if unintended, step towards changing ethical perceptions of illegal file sharing on the RIT campus was a lecture by notable copyright scholar, Lawrence Lessig. Lessig seemed to be extremely well received by students and faculty alike, while he condemned the legal actions of the RIAA and simultaneously maintained an underlying respect for copyright.

In the long term, further research should be performed to identify the patterns of technology diffusion and adoption by students on campus. Initial anecdotal evidence gathered from RIT ITS, Residential Computing (ResNet) and various RIT students indicates that the more technologically adept students tend to use their knowledge as a means to gain acceptance into social groups. As such, technically adept students become makeshift technical support representatives and resident trainers who may install, configure and explain P2P clients for entire groups of students. By taking this role, they not only gain acceptance among peers, but also potentially increase the amount of content available on each network. If this anecdotal evidence is supported by empirical data, then it may be possible to take advantage of the existing social structure. Groups of students that are most likely to be providing technical support to other students could be targeted with specialized ethics education, and provided with minor incentives to encourage ethical computer use.

Conclusion

Overall, social learning theory seems to be an adequate model for explaining P2P music downloading and sharing behavior. Each of the four social learning constructs were all found to have a statistically significant relationship with illegal P2P behavior. Essentially, the more often students observe illegal P2P behavior, the more likely they are to engage in it themselves. The less they perceive illegal P2P behavior to be wrong, the more likely they are to engage in it themselves. The less they perceive that they will be caught, the more likely they are to engage in illegal P2P behavior.

With all of the elements combined, this has created a self-perpetuating culture of illegal P2P use on the RIT campus. The technologically oriented students use their knowledge of P2P networking to gain social acceptance among their peers. As more people observe the non-technical students using the technology and the cycle repeats, and increase the acceptability and prevalence of illegal P2P use on campus.

The spread of P2P technology use cannot simply be attributed to the novelty of new technology. There are cultural influences that push acceptance of P2P technologies beyond just small groups of computer “nerds” and into mainstream social circles. This becomes especially true on college campuses, where students of all levels of social and technological skill study, interact and live together on a daily basis. Such an environment lends itself perfectly to social learning (Hollinger, 1993; Skinner, 1997; Rogers, 2001; Higgins, 2004).

Implementing a subscription based digital music service in an environment supportive of illegal P2P use, and gaining any acceptance at all is truly an

accomplishment. The struggle to hold illegal P2P use in check is a difficult one, particularly with such a large user base and strong cultural grounding. However, with a combined effort to facilitate community growth around an already useful service, it may become significantly easier. That said, adoption of Ctrax in the first year was slow at best. At the time of the survey, of 15,338 students enrolled at RIT, only 744 had registered for Ctrax. However, with the proper push, this could be exactly the starting user base Ctrax needs to gain acceptance with the remainder of the RIT community.

Unfortunately, the initial unveiling of the service was extremely quiet, with only posters inviting students to join the service. Furthermore, initial perceptions of Ctrax were potentially damaged by early problems with billing: students were told that the service was free, but only after they had paid for it and reimbursed in RIT "Tiger Bucks." These initial problems combined with initial skepticism by students, faculty and staff have created a negative image that may be difficult to overcome.

Furthermore, the Ctrax service has had no significant impact upon the perceptions and behaviors of RIT students regarding P2P music downloading and sharing. There is no significant difference between the perceptions and behaviors regarding music downloading and sharing between Ctrax users and non-users. Furthermore, the percentage of users shown by this study to be observing and engaging in P2P music downloading and sharing are nearly identical to studies performed before Ctrax was available to RIT students (McQuade, 2006).

On the basis of this study, many new future opportunities for research become apparent. For example, a similar study could be administered in the same manner as the

original paper computer use and ethics survey. Beyond music piracy, movie and software piracy are also large problems on the RIT campus (McQuade, 2004). While there may be no upcoming services planned to help curb these problems, a similar study could be performed to determine the usefulness of social learning theory as a model for other forms of intellectual property crime. Finally, if the Ctrax service does eventually change music piracy behavior over peer-to-peer networks, will the reduced music piracy behavior influence the other two major forms of piracy behavior on campus?

References

A&M Records v. Napster, Inc (9th Cir. Mar. 25, 2002), http://www.ce9.uscourts.gov/web/newopinions.nsf/0/c4f204f69c2538f6882569f100616b06?OpenDocument.

Akers, R. (1998). *Social learning and social structure: a general theory of crime and deviance*. Boston: North Eastern University Press.

Akers, R. L., & Jensen, G. F. (2005). Social learning theory and crime: a progress report. *Advances in Criminological Theory*, *15*, 1-61.

Bandura, A. (2001). Social cognitive theory of mass communications. In J. Bryant, & D. Zillman (Eds.). *Media effects: Advances in theory and research* (2nd ed., 121-153). Hillsdale, NJ: Lawrence Erlbaum.

Bandura, A., Ross, D., & Ross S. A. (1961). Transmission of aggression through imitation of aggressive models. *Journal of Abnormal and Social Psychology*, *63*, 575-582.

Beckerman, R. (2006, May 8). How the RIAA Litigation Process Works. In *Recording Industry vs the people*. Retrieved May 12, 2006, from http://recordingindustryvspeople.blogspot.com/

Beckerman, R. (2005, Oct 3). Oregon RIAA Victim Fights Back; Sues RIAA for Electronic Trespass, Violations of Computer Fraud & Abuse, Invasion of Privacy, RICO, Fraud. Retrieved August 22, 2006, from Recording Industry vs The People Web site: http://recordingindustryvspeople.blogspot.com/2005/10/oregon-riaa-victim-fights-back-sues.html

Berners-Lee, T. (1991, Aug 06). Worldwideweb: summary. Message posted to alt.hypertext, archived at http://groups.google.com/group/alt.hypertext/msg/395f282a67a1916c

BitTorrent protocol encryption. (2006, May 11). *Wikipedia*. Retrieved May 11, 2006, from http://en.wikipedia.org/wiki/BitTorrent_protocol_encryption

Business Software Alliance, (2003). Eighth annual bsa global software piracy study. Retrieved Feb. 08, 2005, from http://www.bsa.org/globalstudy/2003_GSPS.pdf.

Boorstin, E. (2004), "Music Sales in the Age of File Sharing", Senior thesis, Princeton University.

Ctrax Service Overview. (n.d.). Retrieved May 16, 2006, from Cdigix Web site: http://cdigix.com/website/ctrax/ctraxOverview.asp

Daneman, M. (2004, July 20). Cornell, RIT add downloading. *Democrat and Chronicle*. Retrieved May 18, 2006, from http://www.democratandchronicle.com/news/0720754V6L1_news.shtml

Digital Millennium Copyright Act, H.R. Con. Res. H.R.2281, 105th Cong. (1998) (enacted), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf.

Dowling v. United States, No. 84-589 (9th Cir. June 28, 1985), http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=search&court=US&case=/us/473/207.html.

EFF. (1994, Apr 10). Student indicted on piracy charges. *Computer Underground Digest*, 6(31). Retrieved Feb 26, 2006, from http://www.eff.org/legal/cases/LaMacchia/lamacchia_case.docs.

Federal law enforcement targets international Internet piracy syndicates. (2001, December 11). Retrieved May 12, 2006, from US Department of Justice Web site: http://www.cybercrime.gov/warezoperations.htm

Goldman, E. (2003). A road to no warez: the no electronic theft act and criminal copyright infringement. *Oregon Law Review, 82*, 369-432.

Griffin, E. (1991). *A first look at communication theory*. 1st ed. Colombus, OH: McGraw-Hill.

Green, M. (2002). Napster opens pandora's box: examining how file-sharing services threaten the enforcement of copyright on the internet. *Ohio State Law Journal, 63*, 1-20.

Grusec, J. E. (1992). Social learning theory and developmental psychology: the legacies of robert sears and albert bandura. *Developmental Psychology*, *28*(6), 776-786.

Hannemyr , G. (2003). The internet as hyperbole: a critical examination of adoption rates. *The Information Society*, *19*(2), 111-121.

Higgins, G. E., & Makin, D. A. (2004). Does social learning theory condition the effects of low self-control on college students' software piracy?. *Journal of Economic*

Crime Management, 2. Retrieved Feb 12, 2005, from http://www.jecm.org/docs/higgins_v2_i2.pdf.

Hoag, A. D. (1995). Defrauding the wire fraud statute: united states v. lamacchia. *Harvard Journal of Law & Technology*, *8*(2), 509-520.

Hollinger, R. C. (1993). Crime by computer: correlates of software piracy and unauthorized account access. Security Journal, 4(1), 02-12.

Hollinger, R. C., & Lanza-Kaduce, L (1988). The process of criminalization: The case of computer crime laws. *Criminology*. *26*, 101-126.

Honigsberg, P. J. (2002). The evolution and revolution of napster. *University of San Francisco Law Review*, *36*, 473-508.

Hui, K. & Png, I.P.L. (2002). *Piracy and the Legitimate Demand for Recorded Music*. National U. of Singapore, School of Computing. http://ssrn.com/abstract=262651

Illegal "warez" organizations and Internet piracy . (2002, July 19). *Operation buccaneer: Organization & process*. Retrieved May 10, 2006, from US Department of Justice Web site: http://www.cybercrime.gov/ob/OBorg&pr.htm

In 1997, software piracy caused the loss of an estimated 1,947 jobs and more than $185 million in combined lost wages, tax revenues and retail sales, according to International Planning & Research Corp. (IPR) of Redmond. (1998, November 2). *Microsoft press pass*. Retrieved May 11, 2006, from Microsoft Web site: http://www.microsoft.com/presspass/press/1998/nov98/portlandpr.mspx

Kaye, B. K., & Johnson, T. J. (1999). Research methodology: taming the cyber frontier-techniques for improving online surveys. *Social Science Computer Review*, *17*(3), 323-337.

Kominski, R. (1999). Access denied: changes in computer ownership and use: 1984-1997. Retrieved Feb. 07, 2005, from http://www.census.gov/population/socdemo/computer/confpap99.pdf.

Lessig, L. (2005). *Free culture: the nature and future of creativity*. New York: Penguin.

Liebowitz, S. J. (2003) Will MP3 downloads Annihilate the Record Industry? The Evidence so Far. http://ssrn.com/abstract=414162

Littlejohn, S. (1983). *Theories of human communication*. 2nd ed. Belmont, CA: Wadsworth.

Lutzker, A. P. (2005). Primer on the digital millennium. Retrieved Feb. 25, 2006, from http://www.arl.org/info/frn/copy/primer.html#part1.

Madden, M. (2003). America's online pursuits - the changing picture of who's online and what they do. Retrieved Feb. 01, 2005, from http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.PDF.

Markoff, J. (2000, September 18). A tale of the tape from the days when Microsoft was still Micro Soft. *New York Times*. Retrieved May 11, 2006, from http://raven.utc.edu/cgi-bin/WA.EXE?A2=ind0009c&L=hp3000-l&P=12762

McCandless, D. (1997, April). Warez wars. *Wired*, *5*(4), 44-55.

McFadden, E. S. (Ed.). (2004, October). *Report of the department of justice's task force on intellectual property*. US Department of Justice. Retrieved May 11, 2006, from US Department of Justice Web site: http://www.usdoj.gov/criminal/cybercrime/IPTaskForceReport.pdf

McQuade, S. (1998). *Towards a Theory of Technology-enabled Crime* Unpublished Manuscript, Institute of Public Policy - George Mason University, Fairfax, VA.

McQuade, S. (2004). *RIT Computer Use and Ethics Survey – Preliminary Findings Briefing* Presentation, Rochester Institute of Technology. Grace Watson Hall, Rochester, NY. 13 May.

McQuade, S., & Fisk, N. W. (2005, December 2). *Preventing and Controlling Digital Piracy*. Address presented at the meeting of the Recording Industry Association of America, Washington, D.C.

McQuade, S. (2006). *Understanding and managing cybercrime*. Boston: Allyn & Bacon.

Mennecke, T. (2005). Riaa's grand total: 10,037 - what are your odds?. *Slyck News*. Retrieved Feb 26, 2006, from http://www.slyck.com/news.php?story=769

Mennecke, T. (2006, February 7). P2P population reaches record high. *Slyck News*. Retrieved May 11, 2006, from http://www.slyck.com/news.php?story=1085

Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster, Ltd., et al. 04 U.S. 480 (2005)

MITS Altair BASIC reference maual. (1975). Albuquerque: MITS. Retrieved May 11, 2006, from AICS Research, Inc Web site: http://aics-research.com/nostalgia.html

Mollick, E. (2005). The engine of the underground: the elite-kiddie divide. *ACM SIGGROUP Bulletin*, *25*(2), 23-27.

MPAA | anti-piracy. (n.d.). Retrieved Feb. 10, 2005, from Anti-Piracy Web site: http://www.mpaa.org/anti-piracy/content.htm.

Music's brighter future. (2004). *The Economist*, *373*(8399), 71-74.

Music, Movie Industries Target Theft On Internal Campus Networks. (2006, April 27). *RIAA press room*. Retrieved May 11, 2006, from RIAA Web site: http://www.riaa.com/news/newsletter/042706.asp

Music on the Internet: Is There an Upside to Downloading? Hearing before the Senate Committee on the Judiciary, 106th Cong. (2000), http://judiciary.senate.gov/hearing.cfm?id=195.

No Electronic Theft ("NET") Act, 17 U.S.C. § 101 (1997), http://www.usdoj.gov/criminal/cybercrime/17-18red.htm.

Oberholzer, F. & Strumpf, K. (2004). *The Effect of File Sharing on Record Sales: An Empirical Analysis* Unpublished Manuscript, Harvard Business School, Cambridge, MA.

Oppenheimer, M. S. (2005). Yours for keeps: mgm v. grokster. *John Marshall Journal of Computer & Information Law*, *23*, 1-57.

Orlowski, Andrew (2005, Feb 5). RIAA sues the dead. *The Register*, Retrieved Aug 3, 2006, from http://www.theregister.co.uk/2005/02/05/riaa_sues_the_dead/

Oversight Hearing on Music and the Internet before the Subcomm. on Courts, the Internet, and Intellectual Property , 107th Cong. (2001), http://judiciary.house.gov/media/pdfs/printers/107th/72613.pdf.

Oversight Hearing on Peer-To-Peer Piracy on University Campuses before the Subcomm. on Courts, the Internet, and Intellectual Property, 108th Cong. (2003), http://judiciary.house.gov/media/pdfs/printers/108th/85286.pdf.

Oversight Hearing on Reducing Peer-To-Peer (P2P) Piracy on University Campuses: A Progress Update before the Subcomm. on Courts, the Internet, and Intellectual Property, 109th Cong. (2005), http://judiciary.house.gov/media/pdfs/printers/109th/23572.pdf.

Parker, D. B., & Nycum, S. H. (1984). Computer crime. *Communications of the ACM*, *27*(4), 313-315.

Peer-to-Peer Piracy on University Campuses: An Update Hearing Before The Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary House of Representatives 108th Cong. (2004) http://judiciary.house.gov/media/pdfs/printers/108th/96286.PDF

Peitz, M. & Waelbroeck, P. (2004). *The Effect of Internet Piracy on CD Sales: Cross-Section Evidence.* CESifo Working Paper Series No. 1122. http://ssrn.com/abstract=511763

Pember, D. R., & Calvert, C. (2005). Copyright. In *Mass Media Law* (14th ed., pp. 495-545). Boston: McGraw-Hill.

Penn State and Napster team up to make legal tunes available to students. (2003, November 6). *Penn State Live*. Retrieved May 18, 2006, from Penn State University Web site: http://live.psu.edu/story/4586

Pepper, J. V., & Petrie, C. V. (Eds.). (2003). *Measurement Problems in Criminal Justice Research:*. Washington, D.C.: National Academies Press. Retrieved May 18, 2006, from http://fermat.nap.edu/books/0309086353/html/10.html

Person of the Year. (2006, February 25). In *Wikipedia: The free encyclopedia*. Retrieved February 25, 2006, from http://en.wikipedia.org/wiki/Time_Magazine's_Person_of_the_Year

Piracy of Intellectual Property on Peer-to-Peer Networks Hearing Before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee of the Judiciary House of Representatives 107th Cong. (2002) http://commdocs.house.gov/committees/judiciary/hju81896.000/hju81896_0.HTM

Rainie, L. (2004). retrieved Jan. 26, 2005, from Pew Internet Project and Comscore Media Metrix Data Memo Web site: http://www.pewinternet.org/pdfs/PIP_File_Swapping_Memo_0104.pdf.

Reimer, J. (2005, Dec 14). Total share: 30 years of personal computer market share figures. *Ars Technica*, Retrieved Feb 25, 2006, from http://arstechnica.com/articles/culture/total-share.ars/4.

Reiner, R. (2002). Media Made Criminality: The Representation of Crime in the Mass Media. In Maguire, M., Morgan, R., and Reiner, R. (Eds.), *The Oxford Handbook of Criminology* (pp. 376-416). Oxford, NY: Oxford University Press.

Resnikoff, P. (2006, February 8). File-Sharing levels remain strong in January. *Digital Music News*. Retrieved May 11, 2006, from http://www.digitalmusicnews.com/results?title=BigChampagne

Rob, R. & Waldfogel, J. (2004). *Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students*. NBER Working Paper No. W10874. http://ssrn.com/abstract=612076

Rogers, M. K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study* Unpublished PhD Thesis, University of Manitoba, Winnipeg, Manitoba.

Rohrer, J. (n.d.). *Monolith*. Retrieved May 11, 2006, from http://monolith.sourceforge.net/

Siegel, L. (2001). *Criminology: theories, patterns and typologies*. 7th ed. Belmont, CA: Wadsworth.

Siwek, S. (2004). Copyright industries in the u.s. economy: the 2004 report. Retrieved Feb. 01, 2005, from http://www.iipa.com/pdf/2004_SIWEK_FULL.pdf.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-519.

Slater, D. (2006, April 28). DRM. In *EFF Deep Links*. Retrieved May 10, 2006, from http://www.eff.org/deeplinks/archives/cat_drm.php

Sony Corp. v. Universal City Studios, No. 81-1687 (U.S. Jan. 17, 1984), http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=464&invol=417.

Sterling, B. (1992). *The hacker crackdown*. New York: Bantam.

Sutherland, E. H. (1947). *Principles of Criminology*. Philadelphia: J. B. Lippincott.

Thompson, C. (2005, January). The bittorrent effect. *Wired, 13*(1), 1-5. Retrieved May 11, 2006, from http://www.wired.com/wired/archive/13.01/bittorrent.html

Thompson, I (2005, Feb 3). RIAA defendant 'has never used a computer'. Retrieved August 22, 2006, from vnunet.com Web site: http://www.vnunet.com/vnunet/news/2149712/riaa-sues-pirate-without

Unintended Consequences: Seven Years under the DMCA. (2006, April). Retrieved May 12, 2006, from EFF Web site: http://www.eff.org/IP/DMCA/?f=unintended_consequences.html

United States of America v. LaMacchia, No. 9410092-RGS (United States District Court District of Massachusetts Dec. 28, 1994), http://www.isc.meiji.ac.jp/~sumwel_h/doc/cases/LaMacchia_1994_SD_Massachusetts.htm.

U.S. Census Bureau, (2004). Table 4b. use of the internet at home for people 18 years and over with an internet connection at home, by selected characteristics september 2001. Retrieved Feb. 07, 2005, from http://www.census.gov/population/socdemo/computer/ppl-175/tab04B.pdf.

U.S. Copyright Office, (1998). The digital millenium copyright act of 1998. Retrieved Mar. 01, 2006, from US Copyright Office Summary Web site: http://www.copyright.gov/legislation/dmca.pdf.

Yost, J. (2002). Operation: buccaneer - six students detained for computer piracy. Retrieved Feb. 13, 2005, from Reporter Magazine Online - Operation: Buccaneer Web site: http://www.reportermag.com/vnews/display.v/ART/2002/01/11/3c3e98cb0cb99?in_archive=1.

Zentner, A. (2003). *Measuring the Effect of Music Downloads on Music Purchases* Unpublished Masters Thesis, University of Chicago, Chicago, IL.

Appendix A – Survey Instrument

Survey Listing :: **Preview Survey**

RIT Computer Use Survey

Printer-Friendly Version

Instructions:

RIT COMPUTER USE SURVEY CONSENT FORM
You are requested to participate in the RIT Computer Use Survey. This research project has the endorsement of the University. You are encouraged to read this form carefully before deciding *whether or not to complete* the survey.

Purpose of Study:

This survey is being conducted by RIT's Department of Criminal Justice, as part of an ongoing research initiative at RIT to measure the amount and variety of computer use among RIT students, we well as attitudes and other factors that affect how and why students use computers at RIT and other locations.

Costs and Benefits of Participation:

There is no cost to you for participating in this study, nor will you be compensated in any way for participating. Benefits of participating include contributing to knowledge and understanding about how and why college students use computers. This information could influence the type and level of computer services available to RIT students, faculty and staff. It will also inform computer-related education as well as policies, laws, and regulations relating to information security education, and to computer crime prevention and control.

Confidentiality of Records and Data:

Even though you are requested to take the survey online using RIT's Clipboard survey tool, no personally identifying information will be recorded. In addition, all the information you provide will remain completely confidential and will not be attributable to you personally. All of the survey data will remain secure throughout the study accessible only to approved members of the research team.

Risks of Participation:

The survey instrument and data analysis procedures used in this research have been carefully developed to ensure complete confidentiality of your answers. However, there is a very small risk that by participating in this study other people may become aware of sensitive information related to your use of computers. There is also a very small risk that, in the process of taking the survey, you would remember harmful experiences involving the use of computers by yourself or others that would cause you to experience emotional or psychological trauma. However, both of these possibilities are extremely unlikely to occur.

Voluntary Participation:

This survey is completely voluntary and will take approximately 15 minutes to complete. Merely by taking the survey you may become aware of certain computer services offered by RIT, and other issues related to computer use and ethics and thereby be better able to discuss such topics with your fellow students and instructor(s). You are free not to participate in the study, or you may stop taking the survey after you begin but if you do none of your survey answers can be

"submitted". Thanks you for your willingness to participate in the survey.

Contact Persons:

For more information concerning this study, or if for any reason you are concerned about the research, please contact:

Samuel McQuade, PhD
Assistant Professor of Criminal Justice
Phone number (585) 475-4368

If you have any questions about your rights as a research subject, you may contact the Human Subjects Protection Specialist of the:

Research Subjects Review Board
Office of Sponsored Research Services
Rochester Institute of Technology
141 Lomb Memorial Drive;
Rochester, NY 14623-5604
Phone number (585) 475-7525

Acceptance and Approval
By clicking on the "Click here to submit survey" button at the end of the survey I acknowledge that I am at least 18 years of age, have read the contents of this consent form, have been encouraged to ask questions before participating, and give my consent to participate in this study.

Section A: Computer Use While Growing Up

1. **When you were growing up, did you have a computer in your house?**

- Yes
- No

2. **If you answered "Yes" to the above question, were you the primary user of the computer in your house?**

- Yes
- No
- Not applicable

3. **At approximately what age did you start using computers?**

4. **How much supervision of your computer activities did your parents provide as you were growing up?**

- ○ No supervision
- ○ Little supervision
- ○ Some supervision
- ○ A lot of supervision
- ○ Extensive supervision
- ○ not applicable

5. **From whom have you learned the most about computers?**

- ○ Parent
- ○ Other family member
- ○ Teacher
- ○ Employer
- ○ Other person 24 years old or less
- ○ Other person 25 years old or more

6. **If you chose "other family member" in the above question, please specify who:**

7. **To what extent did this person also teach, require or inspire you to use computers responsibly?**

- ○ Not at all
- ○ A little
- ○ Somewhat
- ○ A lot
- ○ Extensive
- ○ Not applicable

8. **While you were learning about computers, what types of activities were you doing? (choose all that apply)**

- ☐ Playing computer games
- ☐ Using email
- ☐ Web browsing

- [ ] Downloading music or other types of files
- [ ] Word processing
- [ ] Programming
- [ ] Other

9. **Did you receive formal computer ethics education or training before coming to RIT?**

- ( ) Yes
- ( ) No

10. **If you answered "Yes" to the above question, who mainly provided the education or training? (Choose all that apply)**

- [ ] Grade school teachers
- [ ] Junior high / middle school teachers
- [ ] High school teachers
- [ ] Non-RIT college professors
- [ ] Parents
- [ ] Employers
- [ ] Not applicable
- [ ] Other...

Section B: Peer-to-Peer File sharing

11. **Do you basically understand what peer-to-peer file sharing is?**

- ( ) Yes
- ( ) No

12. **How many of your firends engage in sharing music via peer-to-peer networks (such as Kazaa, Bit Torrent or DirectConnect)?**

- ( ) None

- About 25%
- About 50%
- About 75%
- Nearly all
- Don't know

13. On average, how often do you observe others sharing music via peer-to-peer applicaitons/networks?

- More than once per day
- Once per day
- Once per week
- 2-3 times per week
- Once per month
- Less than once per month
- Never

14. Do you currently use a peer-to-peer file sharing applicaiton (such as Kazaa, BitTorrent and DirectConnect) to download music?

- Yes (If YES, answer next question.)
- No (If NO, skip to Section C, question #19.)

15. If you share music via peer-to-peer file sharing, from whom did you learn about the application(s) you currently use to download music? Please choose all that apply.

- Self-taught
- Friends (while attending RIT)
- Friends (before attending RIT)
- World Wide Web/Search engine
- Magazine or newspaper article
- Television program
- Family members
- Other...

16. **How often do you use peer-to-peer file sharing applications to share music?**

- ☐ More than once per day
- ☐ Once per day
- ☐ Once per week
- ☐ 2-3 times per week
- ☐ Once per month
- ☐ Less than once per month
- ☐ Never

17. **Within the previous year, approximately how many songs have you downloaded using a peer-to-peer file sharing application?**

- ☐ 1-20 songs
- ☐ 21-40 songs
- ☐ 41-60 songs
- ☐ 61-80 songs
- ☐ 81-100 songs
- ☐ More than 100 songs

18. **In your opinion what is the biggest advantage of using peer-to-peer applications to download music?**

- ☐ Doesn't cost anything
- ☐ Large selection of music
- ☐ Fast download speeds
- ☐ I can download songs that I cannot buy in stores
- ☐ Other...

Section C: Music and Movie Services

19. **Have you heard of RIT's Ctrax digital music service?**

- Yes (If YES, answer next question.)
- No (If NO, skip to question #23.)

20. **If you have heard of Ctrax, indicate how you heard about it. Choose all that apply.**

- RIT announcement email
- RIT web page
- Other RIT Ctrax announcement
- Professor
- Friend or other RIT student
- Other...

21. **Have you ever logged onto the Ctrax digital music service?**

- Yes (If YES, answer next question.)
- No (If NO, skip to question #23.)

22. **Have you ever downloaded music using the Ctrax music service?**

- Yes
- No

23. **If you do currently subscribe to Ctrax, how did you learn to use the service?**

- Self-taught
- Online instructions
- RIT Helpdesk / ITS
- Friends or other students
- RIT professor
- Other...

24. **Do you use an online music service other than or in addition to RIT's Ctrax music service?**

- Yes (If YES, answer next question.)
- No (If NO, skip to question #32.)

25. **If you do subscribe to other music service(s), please indicate which one(s):**

- ☐ iTunes
- ☐ Napster
- ☐ Other...

26. **Which of the following do you regard as your primary music service?**

- ☐ Ctrax
- ☐ iTunes
- ☐ Napster
- ☐ Other...

27. **On average, how often do you use your primary online music service?**

- ☐ More than once per day
- ☐ Once per day
- ☐ Once per week
- ☐ 2-3 times per week
- ☐ Once per month
- ☐ Less than once per month
- ☐ Never

Please rate your overall satisfaction with your primary online music service in each of the following ways:

	Very Satisfied		Neutral		Very Dissatisfied
28. Number of songs offered	☐	☐	☐	☐	☐
29. Cost of service	☐	☐	☐	☐	☐
30. Quality of music	☐	☐	☐	☐	☐
31. Quality of the line listening/purchasing website	☐	☐	☐	☐	☐

32. **If you have not subscribed to Ctrax, why not? (Indicate the most important reason.)**

- ☐ Music selection not wide enough
- ☐ I heard bad things about the service
- ☐ I already subscribe to / prefer another paid music service
- ☐ Too expensive
- ☐ I do not know how to subscribe / use the software
- ☐ The service is incompatible with my computer / digital music hardware.
- ☐ I can download the same music elsewhere for free (i.e. peer-to-peer file sharing)
- ☐ Did not hear about the service
- ☐ Not a music fan
- ☐ Do not download music
- ☐ Too busy to use a music service
- ☐ Other... [ ]

33. **How much would you be willing to pay per month to subscribe to an online music service that offers unlimited downloading on up to five separate computers or portable listening devices?**

- ☐ $0
- ☐ $.01-.99
- ☐ $1-2.99
- ☐ $3-4.99
- ☐ $5-6.99
- ☐ $7-8.99
- ☐ $9-10.99
- ☐ $11-12.99
- ☐ $13-14.99
- ☐ $15-16.99
- ☐ $17+

34. **How much would you be willing to pay per song with an online music service?**

- [ ] $0
- [ ] $.01-.10
- [ ] $.11-.30
- [ ] $.31-.50
- [ ] $.51-.70
- [ ] $.71-.90
- [ ] $.91-1.10
- [ ] $1.11+

35. Please indicate all the ways in which you access music:

- [ ] I do not listen to music
- [ ] Peer-to-peer file sharing
- [ ] Online music service
- [ ] Purchase CDs / tapes
- [ ] Borrow from friends, family, library
- [ ] Listen to radio
- [ ] Listen to / watch music TV
- [ ] Listen to / watch via internet (such as Spinner or others)
- [ ] Other...

36. How much would you be willing to pay per month to subscribe to an online movie service that offers unlimited downloading on up to five separate computers or portable viewing devices?

- [ ] $0
- [ ] $.01-.3.99
- [ ] $4-7.99
- [ ] $8-11.99
- [ ] $12-15.99
- [ ] $16-19.99
- [ ] $20-23.99

- $24-27.99
- $28-31.99
- $32+

37. How much would you be willing to pay per movie with an online movie service?

- $0
- $.01-1.99
- $2-3.99
- $4-5.99
- $6-7.99
- $8-9.99
- $10-11.99
- $12-13.99
- $14-15.99
- $16-17.99
- $18+

38. Please indicate all the ways in which you access movies: (Check all that apply.)

- I do not watch movies
- Go to the movies
- Watch on TV
- Peer-to-peer file sharing
- Online movie service
- Purchase DVDs / video tapes
- Borrow from friends, family, library
- Rent movies
- Other...

Section D: For Ctrax customers only. All others go to Section E, question #44.

39. **How many songs have you *downloaded (without purchasing the MP3)* through the Ctrax digital music service since becoming a subscriber?**

- ☐ None
- ☐ 1-20 songs
- ☐ 21-40 songs
- ☐ 41-60 songs
- ☐ 61-80 songs
- ☐ 81-100 songs
- ☐ More than 100 songs

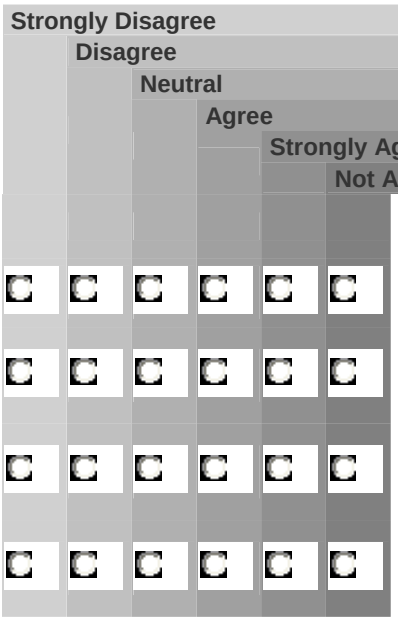
40. **How many songs have you *purchased (in MP3 format)* through the Ctrax digital music service since becoming a subscriber?**

- ☐ None
- ☐ 1-20 songs
- ☐ 21-40 songs
- ☐ 41-60 songs
- ☐ 61-80 songs
- ☐ 81-100 songs
- ☐ More than 100 songs

41. **What, if anything, is the biggest advantage of using the Ctrax service to download music?**

- ☐ Inexpensive
- ☐ Large selection
- ☐ Fast download speed
- ☐ Ability to download songs legally
- ☐ Ability to share the music purchased through Ctrax through peer-to-peer applications
- ☐ Other... [ ]

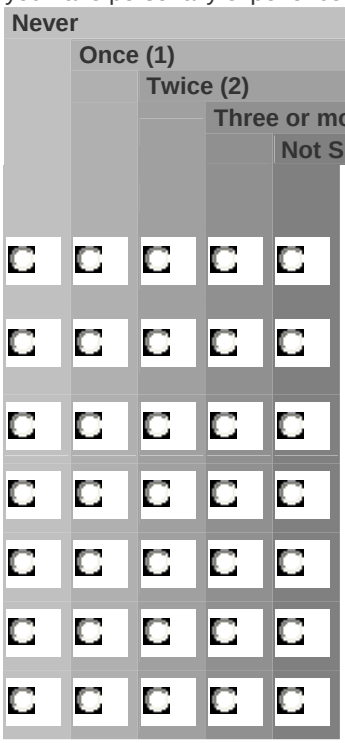
Indicate the extent to which you agree with each of the following statements:



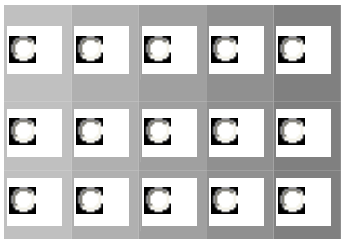
42. **"My friends who use the Ctrax digital music service enjoy using it."**
43. **"Fewer of my friends use peer-to-peer applications to share music now that Ctrax is available."**
44. **"The Ctrax digital music service will reduce the amount of illegal music file-sharing and downloading at RIT."**
45. **"Now that Ctrax has provided a legal alternative to illegal music file-sharing, I prefer to download my music legally."**

Section E: Last Year's Computer Use

Please indicate how many times, if at all, during the last year you have personally experienced EACH of the following:



46. **You accidentally downloaded a virus or worm.**
47. **You were denied computer access or service because of someone's malicious computer conduct.**
48. **Someone used a computer to harass or embarrass you.**
49. **Someone used a computer to threaten you.**
50. **Someone "hacked" into your computer.**
51. **Someone used a computer to stalk you.**
52. **Someone stole your computer or other electronic device.**



53. **Someone used personal information about you in order to pretend they were you.**

54. **Someone used a computer to defraud or cause you financial loss.**

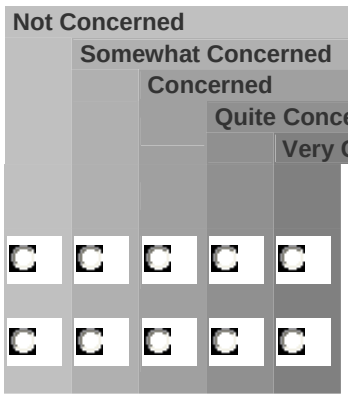
55. **Other victimization**

56. **If you were victimized, do you know who victimized you?**

- Yes
- No
- Not applicable

57. **If you answered "Yes" to the above question, was the offender a:**

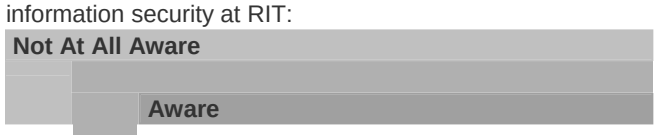
- Stranger
- Aquaintance
- Friend
- Family member
- Other...

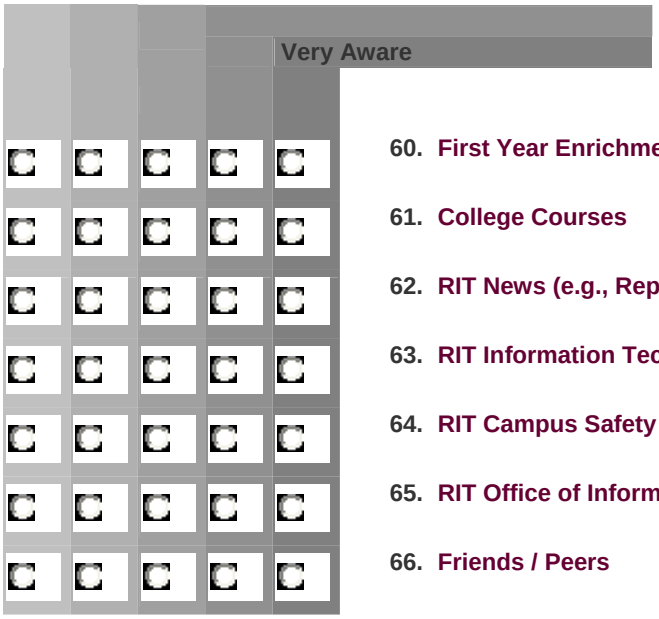


58. **How concerned are you about becoming a victim by way of a computer?**

59. **How concerned are most people you know about becoming a victim via a computer?**

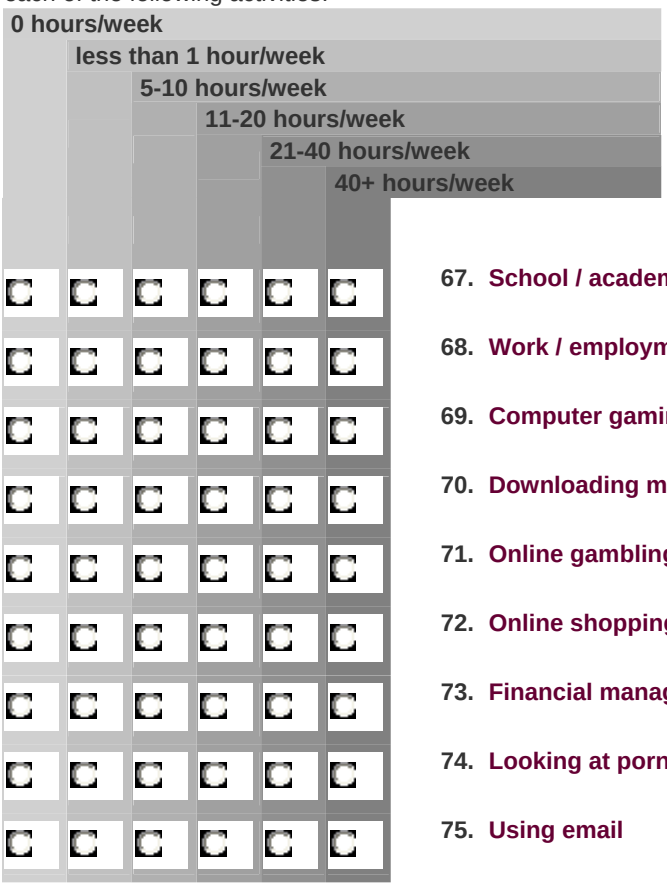
Indicate the extent to which each of the following have contributed to your awareness of computer ethics and / or information security at RIT:





60. **First Year Enrichment Program (FYE)**
61. **College Courses**
62. **RIT News (e.g., Reporter, RIT Magazine)**
63. **RIT Information Technology Services (ITS)**
64. **RIT Campus Safety (e.g., Respect Program)**
65. **RIT Office of Information Security**
66. **Friends / Peers**

With regards to the past year, please estimate the average number of hours you spent per week using computers for each of the following activities:



67. **School / academics**
68. **Work / employment**
69. **Computer gaming**
70. **Downloading music files**
71. **Online gambling**
72. **Online shopping**
73. **Financial management**
74. **Looking at pornography**
75. **Using email**

76. **Chatting online**

Section F: Attitudes About Specific Use of Computers

Please indicate how wrong it is for someone to do each of the following activities:

Not Wrong		Neutral		Very Wrong

77. **Unauthorized music file sharing.**

78. **Unauthorized movie file sharing.**

79. **Unauthorized software file sharing.**

80. **Obtain or possess someone's credit card number without their knowledge or permission.**

81. **Use someone's credit card number without their knowledge or permission.**

82. **Commit plagiarism (present someone else's thought, research or writing as your own).**

83. **Copy computer programming code to use as your own in school assignments.**

84. **Buy papers to use as your own in school assignments.**

85. **Use a computer or other electronic device to cheat on school assignments.**

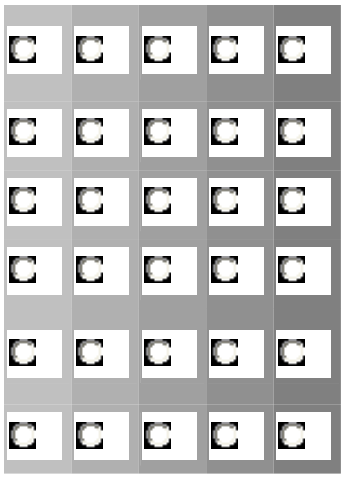
86. **Use a computer or other electronic device to cheat on exams.**

87. **Email spamming (i.e., sending out large volumes of unsolicited email).**

88. **Publicly disclose computer security flaws / vulnerabilities.**

89. **Disrupt / deny computer services.**

90. **Write and release computer viruses.**



91. **Guess password to gain unauthorized access to a computer or computer system.**

92. **Give out someone else's password without their knowledge or permission.**

93. **Gain unauthorized access solely for the purpose of looking at data / files.**

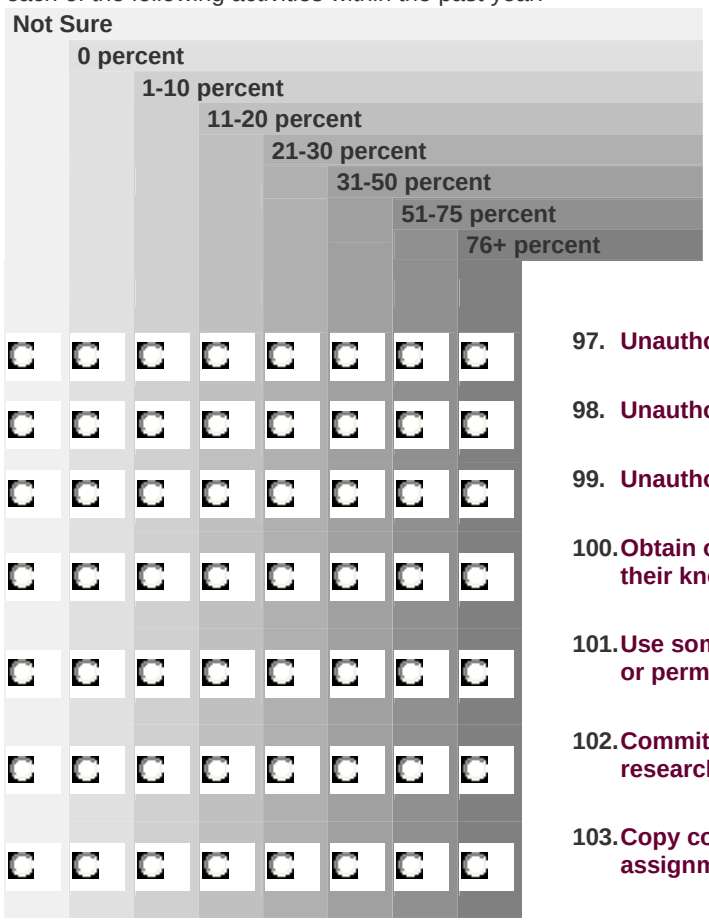
94. **Gain unauthorized access solely for the purpose of changing information.**

95. **Online harassment (e.g., use computers to embarrass, harass or pick-on people).**

96. **Online threats (i.e., using a computer to threaten someone).**

Section G: Perceptions of Computer Use by Your Friends

Please indicate the percent of your friends who have engaged in each of the following activities within the past year:



97. **Unauthorized music file sharing.**

98. **Unauthorized movie file sharing.**

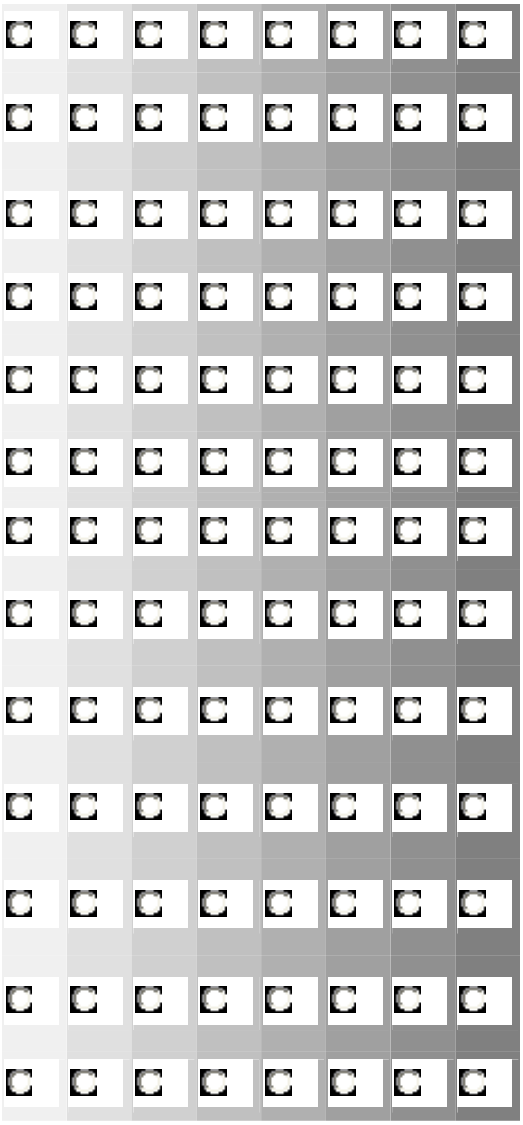
99. **Unauthorized software file sharing.**

100. **Obtain or possess someone's credit card number without their knowledge or permission.**

101. **Use someone's credit card number without their knowledge or permission.**

102. **Commit plagiarism (present someone else's thoughts, research or writing as their own).**

103. **Copy computer code to use as their own in school assignments.**



104. **Buy papers to use as their own in school assignments.**

105. **Use a computer or other electronic device to cheat on school assignments.**

106. **Use a computer or other electronic device to cheat on exams.**

107. **Publicly disclose computer security flaws / vulnerabilities.**

108. **Engage in email spamming (sending out large volumes of unsolicited email).**

109. **Disrupt / deny computer services.**

110. **Write and release computer viruses.**

111. **Guess password to gain unauthorized access to a computer or computer system.**

112. **Give out someone else's password without their knowledge or permission.**

113. **Gain unautorized access solely for the purpose of looking at data / files.**

114. **Gain unauthorized access solely for the purpose of changing information.**

115. **Online harassment (use computers to embarrass, harass or pick-on people).**

116. **Online threats (using a computer to threaten someone).**

Section H: Self-reported Computer Behavior

Please indicate the number of occasions within the last year you engaged in each of the following activities:

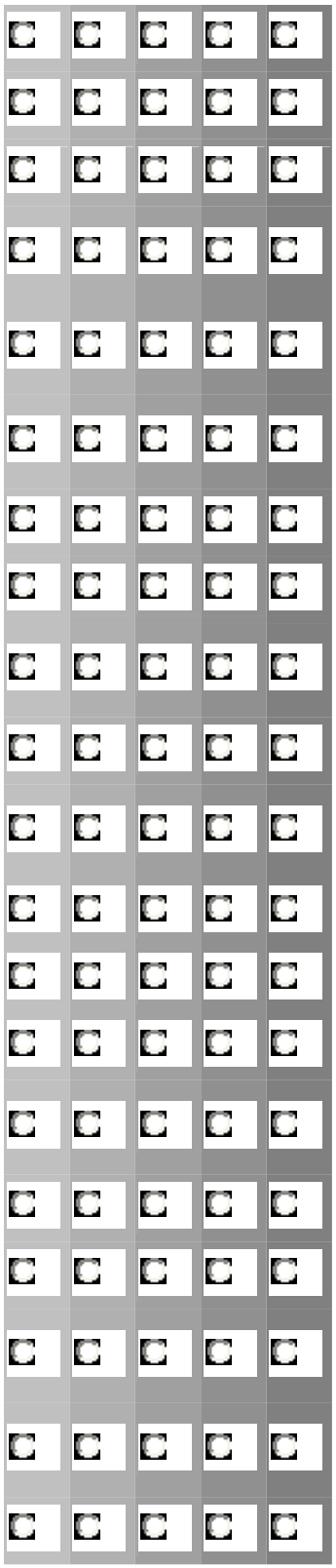
Never

1-5 times

6-10 times

11-50 times

51+ times



117. Unauthorized music file sharing.

118. Unauthorized movie file sharing.

119. Unauthorized software file sharing.

120. Obtained or possessed someone's credit card number without their knowledge or permission.

121. Used someone's credit card number without their knowledge or permission.

122. Plagiarism (presenting someone else's thought, reseach or writing as your own).

123. Copied computer code to use as your own in school assignments.

124. Purchased papers to use as your own in school assignments.

125. Used a computer or other electronic device to cheat on school assignments.

126. Used a computer or other electronic device to cheat on exams.

127. Email spamming (i.e., sending out large volumes of email that was not solicited).

128. Publicly disclosed computer security flaws / vulnerabilities.

129. Disrupted or denied computer services.

130. Wrote and released computer viruses.

131. Guessed a password to gain unauthorized access to a computer or computer system.

132. Gained unauthorized access solely for the purpose of looking at data / files.

133. Gave out someone else's password without their knowledge or permission.

134. Gained unauthorized access solely for the purpose of changing information.

135. Online harassment (e.g., use computers to embarrass, harass or pick-on people).

136. Online threats (i.e., used a computer to threaten someone).

Section I: Likelihood of being discovered and punished

Indicate how likely it is that you would be discovered by authorities (e.g., police/law enforcement or college /university officials, etc.) for the activities listed:

Indicate the level of punishment or sanction that you would expect to receive if you were discovered doing each of the following activities:

	Likelihood of being discovered 0- Not Likely … 4- Very Likely	Level of punishment 0- No Punishment … 4- Severe Punishment
137.	Sending spam email.	
138.	Guessing passwords, giving out passwords, or gaining unauthorized access in order to look at or change data / files.	
139.	Disclosing computer security flaws or vulnerabilities.	
140.	Sharing music files, movie files, or software files.	
141.	Committing plagiarism, copying computer code, purchasing assignments, or cheating on assignments or exams.	
142.	Possessing or using someone's credit card number without their permission.	
143.	Disrupting computer services or write / spread viruses.	
144.	Harassing or threatening someone online.	

Section J: Other Feelings and Attitudes Regarding Use of Computers

Please indicate the extent to which you agree or disagree with each of the following statements:

Strongly Disagree … Neutral

				Strongly Agree
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐

145. **Being ethical means always telling the truth.**

146. **Being ethical means always obeying rules.**

147. **Being ethical means never causing harm.**

148. **It is OK to lie for a good cause.**

149. **It is OK to violate rules for a good cause.**

150. **It is OK to cause some harm if in the end lesser overall harm is caused.**

151. **I would rather chat online than in-person.**

152. **Computers help me to feel in control.**

153. **I enjoy experimenting with others on computers.**

154. **I enjoy exploring with others on computers.**

155. **I enjoy competing with others on computers.**

Section K: Additional Information

156. **Of the following groups, which do you most identify with?**

- ☐ White / Caucasian
- ☐ African American / Black
- ☐ Hispanic / Latino
- ☐ Asian / Pacific Islander
- ☐ Native American
- ☐ Other... ____

157. **Please indicate your gender**

- Male
- Female

158. **Please indicate which RIT college you are enrolled in:**

- College of Business (COB)
- College of Liberal Arts (COLA)
- College of Science (COS)
- College of Applied Science and Technology (CAST)
- B. Thomas Golisano College of Computing and Information Sciences (GCCIS)
- College of Engineering (COE)
- College of Imaging Arts & Sciences (CIAS)
- National Technical Institute for the Deaf (NTID)

159. **What is your matriculation status?**

- First year student
- Second year student
- Third year student
- Fourth year student
- Fifth year student
- Other

160. **How familiar are you with RIT's Code of Conduct for Computer and Network Use?**

- Not Familiar
- Somewhat Familiar
- Familiar
- Quite Familiar
- Very Familiar

161. **Indicate your level of compliance with RIT's Code of Conduct for Computer and Network Use:**

- Not Sure
- Not Compliant
- Somewhat Compliant
- Compliant
- Quite Compliant
- Very Compliant

Thank you for completing RIT's Computer Use Survey!

Click here to submit survey

Appendix B – Invitation E-mail

Dear RIT Student

You are one of approximately 2,000 RIT students who are being asked to participate in an important online survey pertaining to how you prefer to access the music you listen to, and your attitudes towards, perceptions and use of computers for several other purposes.

Please note that although the survey appears quite long, it should take you less than fifteen minutes to complete. None of your answers to any questions will be attributed to you personally, nor will your DCE account number, username or any other personally identifying information be asked about or tracked.

Results of the survey will be made known to all of RIT during the second week of May, and the information provided will greatly help to improve computer services here at RIT.

You may access the survey online at:

http://clipboard.rit.edu/takeSurvey.cfm?id=2J92ID

_Please make every effort to respond to this survey by __noon__ on Thursday, April 14_ so that data analysis may begin within the next few days. Thank you in advance for taking time to completely answer this important survey. I know you will be interested in seeing the results within the month.

Sincerely yours,

Diane Barbour

Appendix C – Social Learning Theory Correlation Table

Intercorrelations Between Social Learning Theory Constructs & Unauthorized P2P Use

	Frequency of P2P Use (Q16)	Songs Downloaded (Q17)	Differential Association (Q12)	Differential Association (Q97)	Definitions (Q77)	Differential Reinforcement (Q140a)	Differential Reinforcement (Q140b)	Imitation (Q13)
Frequency of P2P Use (Q16)	—	.540**	.337**	.393**	-.467**	-.143*	-.150*	.533**
Songs Downloaded (Q17)		—	.299**	.409**	-.366**	-.110	-.121	.395**
Differential Association (Q12)			—	.743**	-.376**	-.128*	-.086	.618**
Differential Association (Q97)				—	-.351**	-.240**	-.173**	.576**
Definitions (Q77)					—	.175**	.294**	-.377**
Differential Reinforcement (Q140a)						—	.192**	-.139**
Differential Reinforcement (Q140b)							—	-.096*
Imitation (Q13)								—

**$p < 0.01$ 2-tailed.
*$p < 0.05$ 2-tailed.

Appendix D – Biographical Sketch

My academic and professional background and goals can largely be simplified into one broad statement: I am an information technologist striving to become a social scientist. I aim to develop stronger theoretical perspectives on the growing phenomenon of deviance and crime on the Internet. My technological background provides me with a unique perspective when approaching these issues.

My interest in computers began at a young age, and I worked in multiple technical support positions throughout high school. This interest followed naturally into an Information Technology undergraduate degree at the Rochester Institute of Technology. My primary focus throughout this degree program was on computer security and system administration. Unfortunately, the program focused primarily on the technical aspects of information technology and computer security, largely overlooking the role of computer users and impacts on society.

In the summer of 2003 I began work with then Criminal Justice professor Dr. Samuel McQuade after taking his course on computer crime. At this time, we began development on what is now the RIT Computer Use and Ethics survey with a number of other graduate students and faculty members. This survey focused on the applicability of criminological theory to computer crime on the RIT campus, and is to date the most comprehensive survey ever performed on the topic of computer crime. My experiences with Dr. McQuade lead me to begin work on a masters' degree in Communication & Media Technologies both to provide me with a solid theoretical grounding and to continue my research at RIT. I later helped to replicate the Computer Use and Ethics

survey as part of the first analysis of a legal music downloading service (Ctrax) on a college campus. The results of this research were recently presented to the Recording Industry Association of America. My participation in these research efforts lead into becoming the primary research assistant for the first textbook on computer crime, which was completed in November of 2005.

Currently, I am interested in continuing my research on deviance and crime on the Internet. In particular, I am interested in the emergence and development of online communities, the nature of legitimate and illegitimate behaviors within those communities, and the mechanisms of social control that can occur organically or artificially within those communities.