Inquiry: The University of Arkansas Undergraduate Research Journal

Volume 5 Article 7

Fall 2004

Musical Copyright Infringement and Policy Implementation at Higher Education Institutions

Henry Haruaki Wendel
University of Arkansas, Fayetteville

MUSICAL COPYRIGHT INFRINGEMENT AND POLICY IMPLEMENTATION AT HIGHER EDUCATION INSTITUTIONS

By Henry Haruaki Wendel
Department of Economics

Faculty Mentor: Professor John Norwood
Department of Economics

Abstract:

Copyright infringement through campus networks has become an increasingly troubling problem for higher education institutions across the nation for two reasons. First, the network infrastructure is being abused to the extent that high percentages of the traffic to and from the university are of illegal material. Second, much of these materials are illegal, so administrators must follow procedures and implement policies, which will indemnify the university when a member of the university violates the law.

Throughout the nation, university administrators are taking different approaches to combat this new issue on campuses. In this study, the policies of the one hundred seventeen Division I Football institutions were critiqued. Some schools are taking a very relaxed approach and simply have a cursory statement in their policies mentioning students, faculty, and staff must follow all laws and policies. Others have taken a more active approach. The University of Arizona has the most comprehensive policies. They have included information on the Copyright Act, links to federal regulations, and a link to the university's policies on the use of Peer-to-Peer (P2P) programs. A great number of institutions are also complying with the Recording Industry Association of America (RIAA) and disconnecting suspected violators from the campus network. However, this seems to be contradictory to our nation's Constitution which states individuals are "innocent until proven guilty." In the current system, which is common across the nation, it would seem as if users are "guilty until proven innocent."

The availability of these P2P networks has resulted in a tremendous amount of legislation and trials to occur to protect the owners of the copyrights. New legislation or large numbers of suits are filed seemingly every week. Since last August, there have been almost 2,000 suits filed against individuals and several court cases against companies across the nation. In December, federal court of appeals ruled that service providers do not have to give copyright owners the personal information of people suspected of possessing copyrighted materials. This was a huge blow to owners as this was the primary means in which they were able to fight this growing issue.

New issues that will face administrators will be very prevalent. One such process that students are beginning to use is called stream ripping. This allows users to tune into several Internet radio stations at once and while doing so, a program converts the songs into a music file and stores it on the host computer. What is so different about this program is that it uses legal streams of music and then stores the songs. There is no sharing that takes place and network administrators cannot tell that there is anything illegal taking place.

This problem is one that will not be solved soon. The emergence of new technologies and the increasing ability of students to find ways to break protectionist measure implemented by the copyright owners will continue to grow. While this thesis has been a comprehensive study of the legal history, institutional policies, and what might be in store in the near future, there would be aspects of this issue that could not be predicted. This is a very timely issue that will surely see much more spotlight.

Introduction:

In the last few years, there have been thousands of lawsuits against people illegally downloading copyrighted music through the Internet. The recording industry has been fighting this growing trend since 1999. Artists are holding file sharing largely responsible for a 25 percent decline in sales of CD's since 1999, when Napster, the first popular file-swapping software, was released (Harmon). While the various recording labels do not attribute all this loss to illegal downloads, they do feel it is a substantial portion, with as much as $700 Million in sales lost to these downloads (Suing Music Downloaders). Today, there are various means by which college students can download illegal materials. The most prolific sources are Peer-to-Peer (P2P) programs that connect various users to each other as a means of exchanging files. There are literally hundreds of P2P networks that students can use; however, Kazaa, Limewire, and Morpheus are the predominant utilities used by college students to acquire legal and illegal materials as defined by the 1998 Digital

Millennium Copyright Act (DMCA) and subsequent legislation. With the proliferation of high-speed Internet in collegiate residence halls across the nation, students are able to spend less time downloading and are able to access much more illegal content than in previous years. At any given moment in time, there are hundreds of thousands of users on Kazaa alone who have terabytes of information shared. These factors have forced the Recording Industry Association of America (RIAA) to battle to decrease these illegal downloads to help slow the drastic drop in record sales.

In a recent CBS/New York Times poll (See Appendix B) there was a clear distinction in the ideas held by those between the age groups 18-29 years and 30 and older years. The younger group tended to pay closer attention to the latest occurrences dealing with sharing music and felt it was more acceptable to share music files. Sixty-nine percent of the younger bracket thought it was at least somewhat acceptable to share music files compared to the fifty-five percent among the older group. The staggering difference between the two groups came in the extreme answers to the question with twenty-nine percent of the younger group thinking it was always acceptable compared to nine percent of the older group. In contrast the same ratio of younger to older individuals showed only thirty percent thought it was never acceptable compared to forty percent.

In August of 2003, the RIAA initiated a plan to start a stringent campaign against individuals who were violating copyright law by downloading music. The RIAA has teamed with college administrators in determining which students were abusing the facilities, but also worked to educate all students on the law and the consequences of violating such law. Subsequently, the RIAA followed through on its plan, and on September 8, 2003, filed 261 lawsuits against people found in violation of the DMCA, promising to file thousands more soon (Harmon). Many people have been appalled at the RIAA for some of the people who have been sued. For instance, one of the defendants is a 12-year-old named Brianna Lahara (Suing Music Downloaders).

The major problem the RIAA has faced has been eliminating the file-sharing programs that are prevalent today. Unlike Napster, Kazaa and the other programs today do not store any files on their servers; instead, users connect to each other directly using Kazaa as a medium for this connection. Therefore, Kazaa is not in violation of any copyright law. Furthermore, there is a substantial amount of legal material available through these channels, which gives justification for allowing these companies to stay in existence. This has forced the recording industry to ask Internet providers such as Verizon and AOL, as well as college administrators to release information about their customers who are downloading these files. Colleges and Universities are also facing problems from these illegal downloads. This is a two-part problem: first, the colleges are providers of the means by which the students are able to download the copyrighted materials (Hamilton). Universities could be held partially liable for this action; however, the RIAA has tended to try to work with Universities as long as they are giving information on their users. Second, the universities are having hardware issues from these downloads. Due to the high demand on the university's infrastructure from downloading and streaming (the act of listening to the material without downloading it), colleges are limiting bandwidth to the residence halls in order to compensate for this problem. This allows the scholarly research in the different academic buildings to continue with as little delay as possible.

Statutory Framework and Case History:

The authority of Congress to pass legislation protecting the works of authors is provided for in Article One, Section Eight of the Constitution. In carrying out this mission Congress has stated that:

> Copyright protection subsists, in accordance with this Title, in original works of authorship fixed in any tangible medium of expression... Works of authorship include the following categories: (1) literary works; (2) musical works, including any accompanying words; (3) dramatic works, including any accompanying music; (4) pantomimes and choreographic works; (5) pictorial, graphic, and sculptural works; (6) motion pictures; (7) sound recordings; and (8) architectural works." (17 USC 102)

Currently, the broadest legislation passed concerning this topic is the Copyright Act of 1976. Under Section 102(a) of this Act, copyright owners are required to have the following characteristics in order to gain protection: 1) the work must be original, 2) creative, and 3) fixed (able to be reproduced and sold) (Hawke, 3). Section 106 of the Act provides several rights to the owner of the copyright:

> 1) To reproduce the copyrighted work in copies or phonorecords
>
> 2) To prepare derivative works based on the copyrighted work
>
> 3) To distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending
>
> 4) In the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures, and other audiovisual works, to perform or display the copyrighted work publicly
>
> 5) In the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission. (Hawke, 4)

Extended in 1998 by the Copyright Term Extension Act of 1998, copyrights are valid on any work for the span of the creator's life plus 70 years (17 U.S.C., Section 302). The most important aspect one must remember concerning copyright is that it is a strict liability tort, which means no intent is required to be found in violation (Background ... University Networks). Under the Act, there are three forms of infringement that a user can be found to be responsible for: direct, contributory, and vicarious.

Direct: According to Title 17 of the U.S.C. Section 501(a), "anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122..., or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of a copyright..." Keeping this in mind, virtually anyone found in violation of sharing protected music can be found directly infringing copyright law.

Contributory: As defined by case law, contributory infringement could be claimed if "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another...." (Gershwin Publishing Corp v. Columbia Artists Management, Inc., 443 F. 2d 1159, 1162 (2"d Cir. 1971)). Intuitively, this would require the direct infringement of copyright law by another party, not involved in the contributory infringement. There are two parts that are important when considering liability: 1) knowledge; and 2) inducing, causation, or material contribution (Background ... University Networks). According to the Joint Committee of the Higher Education and Entertainment Communities, students who knowingly leave their computers connected to a P2P program allowing for users to download from them could be found contributing to copyright violation.

Vicarious: Vicarious liability, on the other hand, can be imposed on persons who do not "induce" or "cause" direct infringement or, for that matter are not even aware that another party is involved in infringing activity when their economic interests are intertwined with the direct infringers (Background ... University Networks). Napster has already been found liable because of contributory and vicarious infringement; however, there have not been any students who have been sued because of vicarious infringement. Theoretically, a student could be found liable if he or she was operating a P2P network and uploaded or downloaded files, deliberately enabled others the access to files, had the right to manage the activity of the networks users and gained financially from the activity (Background ... University Networks).

The most important legislation passed in regard to this issue in recent years is the Digital Millennium Copyright Act of 1998 (DMCA) that amends the aforementioned Copyright Act. This legislation is very broad and set the standard on copyright infringement through the Internet. It also makes it illegal to break an electronic encryption, or to distribute information allowing someone to break the encryption. Also, it is perpetual in nature. Thus, even if the copyright has expired, the encryption can continue, and it is illegal to break it. Educational institutions have a very important section of the DMCA to consider when instituting policies for their networks and users. As defined in the University of Houston's Acceptable Use of Computing Resources, the DMCA "is a federal statute that limits an online service provider's liability for copyright infringement claims based solely on the online service provider's automated, copying, storing and dissemination functions." The good news for college and university administrators is that the DMCA restricts liability for service providers that engage in: 1) transitory (mere conduit) digital network communications; 2) system caching; 3) information residing on systems or networks at the direction of users; and 4) information location tools. (17 U.S.C. Section 512). In order to be eligible for safe harbor (which indemnifies the university from any legal recourse), colleges and universities must implement policies that agree to disconnect egregious offenders and also designate someone to take notices from the Copyright office.

While the DMCA does provide protection for colleges and universities, students must be acutely aware that this protection is not an overarching one that covers them as well. As described later in this paper, during a recent decision in a case brought against Verizon Internet Services, Inc., there has been a subpoena process initiated under the DMCA to detect which person is in violation by tracing a specific Internet Protocol address (IP address). Id. At Section 512(h).

Copyright Infringement Act - This federal law explicitly states that Internet service providers are not responsible for monetary remission to copyright owners if the provider is complying with the copyright owner to effectively target violators seeking commercial advantage or financial gain. Complying may include but is not limited to terminating the Internet service to the user permanently or temporarily; complying could also include turning over identifying information to the copyright owner. (17 USC 512)

No Electronic Theft Act - This federal law defines financial gain as stated in the Copyright Infringement Act and sets the minimum gain at $1000 during any 180-day period, of one or more copies or phonorecords or I or more copyrighted works. Under the NET Act, fines, imprisonment (up to five years), forfeiture, destruction, or disposition of the illegal material can all be sanctions placed on violators. (17 USC 506)

Other actions courts have taken against violators include injunctions and restitution of costs and attorney's fees. Injunctions have typically been the immediate action taken against violators as prescribed by sections 502 and 503 of the Act, which allow for restraining orders, preliminary injunctions, impoundment, and disposition orders. Therefore, students found in violation of the Act could have their computers seized by authorities. In order to

comply with authorities, immediate actions taken by universities tend to lean towards disconnecting students from the campus network. While the DMCA does provide protection for colleges and universities, students must be acutely aware that this protection is not an overarching one that covers them as well.

RIAA:

The Recording Industry Association of America (RIAA) is the organization which represents a majority of the major record labels responsible for producing much of the music heard today. The stance taken by the RIAA is very obvious: the organization wholeheartedly opposes the illegal copying of copyrighted music. With the passage of the Digital Millennium Copyright Act in 1998, the RIAA realized a great shift in managing their anti-piracy campaign. In a press release on March 5, 1998, the organization is quoted as saying "anti-piracy statistics indicate that while cassette piracy has dropped 80% over the last five years and cassette street vendors are dissipating, music piracy is rapidly moving towards the Internet and CD piracy" (RIAA Press Release, March 5, 1998). At the time of this press release, the cost to the average consumer to pirate a song was much higher than today. At that time, prices for CD burners started around $400 and Internet prices hovered around $20 a month for a 56k connection; the phenomenon had not reached its full potential.

In 2000, RIAA's battle against the online providers such as MP3.com and Napster started in full force. In their first victory, a federal judge ruled in favor of RIAA against MP3.com and ordered the company to cease and desist from all their illegal practices. However, much more publicized was the case that would eventually bring Napster to its knees. On May 5, 2000, a California district judge ruled against Napster, Inc., citing violation of copyright laws. (114 F. Supp.2d 896, Cal. D.C. 2000) At the heart of these two firms being found responsible for copyright violations was the method in which they provided their music. Both supplied users with a means to download music from a central storage server, which was owned by the respective company. However, copyright laws prohibit this from taking place, because only the individuals who purchase the music have the right to possess the Mp3s. This was a huge victory for the RIAA. At the time, Napster was the largest source for free online music. However, Napster would not take this as the final word, and later that year, Napster appealed the decision of the lower court. On February 13, 2001, music producers, song writers, and artists won a major victory when the Ninth Circuit Court of Appeals upheld the decision of the District Court and ruled in favor of the respondents on all counts. (239 F.3d 1004, 9' Cir. 2001) In their decision the court stated, "Napster by its conduct knowingly encourages and assists the infringement of plaintiffs' copyrights." (239 F.3d 1004, 9th Cir. 2001) Along with the ruling that copyright laws were violated, the court ruled that the preliminary injunction against Napster was too broad and ordered the District Court to redefine their injunction in a narrower manner. After all the subsequent motions were filed by Napster and all eventually struck by the courts, Napster finally realized they had lost the battle.

Since the Napster ruling, many other companies have been shut down as well. However, the RIAA has lost several battles to other online content "providers." These other providers are called Peer-to-Peer networks, which serve as a medium that allows users to connect to other users to download material on the user's hard drive. In several cases since 2001, courts have consistently ruled that these providers are not in violation of copyright laws because they do not actually ever possess the illegal materials. This has caused a lot of turmoil for the music industry, and in October of 2002, the "creative content industries" asked thousands of higher education institutions to monitor, educate, and reprimand students on violations of copyright laws in relation to the DMCA. Subsequently, six leading higher education associations representing virtually every college and university in the United States also sent letters to support the RIAA's request. Knowing that this could reduce liability on the part of the institution and also helps in diminishing the demand strain on the campus networking, colleges and universities have been complying with this request. (Press Room, Content Community, College Groups Outline Threat of P2P, Ask for Action)

The last major case, which has set a major precedent in the file-sharing controversy, was the lawsuit between the RIAA and Verizon. The issue of this case was whether or not the RIAA could sue Internet service providers to force them to provide information pertaining to suspect copyright infringers. The argument Verizon made was that this information was private and that corporations cannot sue for this information, even if it is against Verizon's Acceptable Use Policy (AUP). According to Verizon's AUP, rule 4 states, "You may not store material on, or disseminate material over, Verizon Online's systems or servers in any manner that constitutes an infringement of third party intellectual property rights, including rights granted under the US Copyright laws." However, even though Verizon knew they had users in violation of the DMCA, they did not feel they could be compelled to turn over this private information. In their decision, the trial court sided with the RIAA which stated that with sufficient proof, Internet service providers were required to provide the identity of the person accused of infringement (In re Verizon Internet Services, Inc. 240 F. Supp.2d 24, D.D.C., 2003). "It is also clear that the First Amendment does not protect copyright infringement ... Nor is this an instance where the anonymity of an Internet user merits free speech and privacy protections (31-32, District Court Opinion.)" This statement from the District Court's Opinion was one of the fundamental reasons it came to its decision. Furthermore, the court also said the following, "Verizon has provided no sound reason why Congress would enable a copyright owner to obtain identifying information from a service provider storing the infringing material

on its system, but would not enable a copyright owner to obtain identifying information from a service provider transmitting the material over its system." (18, District Court Opinion). In effect, this decision would force service providers to turn over the names of their users who have repeatedly downloaded copyrighted material. The process to identify an individual offender is quite extensive. First, the copyright owner or designee detects which IP address is receiving or sending illegal material. Once this happens, the owner would file a John Doe suit using the IP address to identify the person. Once there is a preponderance of evidence, service providers are required to turn over the identifying information to the copyright owner. This decision was later overturned in December of 2003, when the U.S. Court of Appeals issued a decision which said Verizon and other service providers could not be compelled to turn over private information of their users (351 F.3d 1229, D.C. Cir. 2003). This was a tremendous setback for copyright since now they would have to depend on firms to do so voluntarily.

The RIAA has also brought thousands of suits against individuals for their violation of copyright laws. Hundreds of these suits were brought against college students at institutions around the country. Among the first to be subpoenaed were two students at Rensselaer Polytechnic Institute, one at Michigan Technological University, and one at Princeton University. The RIAA brought these suits against the students threatening penalties up to $150,000 per song that was illegally stored on their computers (Goldstein, The Dartmouth). These students were all accused of not only sharing their music, but also publicizing their collections to the public with libraries containing anywhere from 27,000 to I million music files (Goldstein, The Dartmouth). Each of these suits was settled out of court, and even though each of the four students denied the allegations, the students settled by agreeing to pay between $12,000 and $17,500 and disabling their file-sharing services (Carlson, Record Companies). About a month after this first round of suits, the RIAA sent warning letters (See Appendix Q to approximately 2 million users of file-sharing services to educate them about copyright law (Carlson, Record Industry). To date, approximately 2,000 suits have been brought against individuals with hundreds of those people being college students across the nation.

Today, the RIAA spends millions upon millions of dollars attempting to catch intellectual property right violators. One might ask why the RIAA does not share files on programs like Kazaa to catch these individuals; however, due to U.S. law, this could be considered entrapment and could tarnish their reputation in the eyes of the consumer. Therefore, independent firms are hired to find individuals who are sharing these copyrighted materials. Of course, once these sharers found out that the RIAA and other copyright owners were doing this, they began changing file names to make it increasingly difficult for these firms to find the illegal materials. Now, these firms have to run comparisons to find the likelihood that the songs downloaded are copies of those that are trademarked.

Colleges and Universities:

Colleges and universities across the nation have been forced to deal with this epidemic that is plaguing networks. There is a very important message that needs to be conveyed to all users of the campus network infrastructure, which is that access to the network is a privilege, not a right. Those found in violation of any policies set forth by the institution shall be punished accordingly. This establishes a standard to all users that lets them know that this type of behavior will not tolerated and the institution is very serious in these terms. The excessive downloading by students in residence halls across the country has caused tremendous strain for the infrastructure in place, and limits the amount of web traffic that can be used for the primary purpose of academics. Since 2001, network administrators have been struggling with providing enough bandwidth to everyone who is in "need" of it. For example, Mr. Dewitt Latimer of the University of Tennessee said that downloads from Kazaa alone constituted more than 50 percent of the traffic on residential networks; moreover, about 75 percent of the outgoing traffic was directly attributable to outside users downloading materials from students within the residence halls at the University (Chronicle, September 28, 2001). Also in 2001, Justin Sipher, Director of Computing and Technology Services at the State University of New York at Potsdam, said that SUNY-Potsdam had doubled bandwidth capacity in the last year and would double again within a month. To inhibit students from abusing their network accessibility, administrators are taking a few different approaches. The most prevalent form of restricting access is to purchase hardware that allows administrators to perform "Bandwidth-shaping." Managers can tell these devices to restrict the speed at which certain types of downloads are allowed to be transferred (Carlson, Napster was Just the Start). Some hardware controllers are also able to prioritize certain Internet ports that could have higher priority and actually disconnect others if the network becomes too crowded.

One may ask why administrators do not just monitor the files being transmitted through their networks in order to identify the users who are sharing the illegal files. First of all, the cost to hire people to monitor the network traffic would be exorbitant and more than likely unfeasible. However more importantly, under the regulations set forth by the DMCA, if network administrators were to monitor file traffic, they could be held responsible for not sanctioning their users if transmitting the files. While many institutions do write into their policies that they maintain the right to search through the files on the network, the hypothesis of the actual implementation of this policy would be to monitor the transmittal of viruses and not whether a file is legal or not.

Furthermore, administrators are pushing for educational programs to inform students of their legal and ethical restrictions in downloading material from legal and illegal sources. For instance, the University of Delaware has required students to

become educated on these issues and subsequently pass a test before gaining access to the campus network (Chronicle, Sept. 28). Then, if these students violate the policy, their network connections are disabled and students are instructed on the legal issues (Chronicle, Sept. 28). Other institutions require egregious offenders to write educational papers or create educational programs before being allowed to reconnect to the network. One other form of protection at least one institution has tried was to actually seize the computers suspected of containing illegal materials. In November 2002, the US Naval Academy confiscated approximately 100 computers (Baker, Knight Rider Tribune Business News). In other cases, some network administrators are banning the use of file-sharing programs on the campus network. For instance, in April 2003, the New Jersey Institute of Technology decided to prohibit the use of any file-sharing programs through the network (Carlson, New Jersey Institute).

Campus network administrators are also affected by any new legislation or judgment handed down in regards to file sharing. In 2000, Metallica sued Yale University, Indiana University and the University of Southern California along with Napster for allowing their users to use Napster to download their songs. Metallica felt these institutions had done nothing to positively enforce the DMCA and, therefore, used these three universities as examples for the rest of the country. These three suits were later dropped when the institutions agreed to ban the use of Napster on their networks (Chronicle, Appeals Court Rules). Administrators in several departments at all residential campuses have been faced with the issue of how to enforce these policies and to what extent they would be working in conjunction with the RIAA to fully comply with the law.

One aspect that bypasses P2P networks completely is using other file transfer options for sharing music within an intranet on the campus. This allows friends within an institution to send files to each other without ever connecting to a P2P network. Users could then copy CDs to their computers or download MP3 files and then transmit these illegal copies to their friends. To add to the complex issue, students can also now send files through instant messaging clients such as MSN Messenger and AOL Instant Messenger. These present grave challenges to administrators because unlike the P2P networks, they cannot just block a certain IP address to disallow access. Essentially, network administrators would have to monitor the files being transferred to determine if they were legal files. This however poses the aforementioned problem of having network administrators monitoring files; it opens the university up for liability.

The latest technique that students across the nation are using is a process called Stream Ripping. Applications use an Internet radio source to provide the songs, which are then converted into MP3 files and stored on the local computer's hard drive. This brings two very problematic issues to administrators. First, with the current infrastructure in place, it will be difficult to distinguish whether a student is listening to the Internet radio stations or if they are using these stations to provide music. Also, since the firms are using shared directories to catch copyright violators, there is no surveillance technique that can be used within the program. With these conditions in place, it is almost impossible to determine whether students are violating federal copyright laws.

Preventative Measures Taken:

Administrators have taken several steps to prevent the possibility of having to comply with any lawsuits filed by the RIAA against their students. Colleges and universities from around the nation have taken proactive stances to alleviate this problem. One of the most interesting methods which administrators are using to prevent lawsuits is to actually create a blanket subscription that students can take part in to legally download music from online sources. In November 2003, Penn State University became the first to sign such an agreement with Napster. Napster was of course the first file-trading software company that was sued for their part in violating intellectual property rights. After Napster was found liable, the company was bought out and started a pay service that is now what is being used by Penn State. Normally, users would pay $9.95 per person per month for this service (which only applies to Windows 2000 and XP users), but Penn State has been provided a discounted rate for the service (Chronicle, Young). Right now, a mandatory information technology fee (Chronicle, Read) is paying for this service. Following in their footsteps was the University of Rochester who signed a similar deal four months later. Both institutions use the service, which allows the students at both universities the opportunity to download the songs to their computers, listen to streaming music, and find out information about the artists they are listening to. However, if students wish to bum these songs to a CD or upload them to portable MP3 players, students will have to pay an additional $0.99 per song transferred. Charles Phelps who serves as Provost at Rochester said colleges have a "responsibility to help students understand the law and what is proper legal and moral behavior." With this in mind, Rochester has also started to create public forums updating students on the laws revolving around copyrights. Furthermore, Phelps said the university is planning to offer a course on "the legality of file sharing (Chronicle, Young)." Officials at Penn State have said that if this service is successful, there is a possibility that the service could extend to off-campus students, Macintosh users, faculty, staff, and even alumni in the future (Chronicle, Read). In response to these deals, Mike Bebel, President and COO of Napster said, "We want to encourage a new generation to try using legitimate services. (Chronicle, Read)."

There has been some opposition to this new trend in offering these services to students. Fred von Lohmann, an attorney with Electronic Frontier Foundation said, "This is a classic example of trying to force students to take what the record labels are willing to give. Consider what Napster offers compared

to what you can get with peer-to-peer file sharing. Napster mostly excludes independent artists." Many students will agree with Mr. von Lohmann. What incentive do students have to pay per song if they are still able to download the songs for free from these P2P sources? For many students, it is not only in their rooms that they listen to the music. A vast majority of the students bum these songs to CDs and take them to their car to listen to during their travels to work, home, or play. The only motivation students would have to follow these avenues would be to stay legal in all their actions. However, this is assuming every student knows that downloading music from other users is illegal and unethical.

Another form of prevention that the RIAA has is a program called Audible Magic, which can identify copyrighted songs in the midst of their transfer from computer to computer (Schwartz, NY Times.com). Once these transfers are detected, they are blocked. According to the article, Audible Magic executives say that the program can be installed on network devices as well as integrated into P2P programs like Kazaa. Legally, this provides even more assistance to administrators who can use this sort of program to decrease their liability. Already, Charles Phelps, Provost at the University of Rochester has said he was impressed with the new program. If all expectations hold true, this may be the best solution in solving this extremely complex situation.

Another form of preventative policy is to limit the amount of content a user can download during a specified time period. For instance, the University of Vermont has added a limit of one gigabyte per student per day, which would still allow for a tremendous amount of information to be downloaded (Chronicle, September 28, 2001). Other institutions have similar policies in place that might allow for a set amount each week. Moreover, some schools use programs that will require some users to logon to the network in order to have full access to the Internet. For instance, the University of Arkansas uses a program called ResNet, which forces students to logon for certain time sessions (within the residence halls it is a 24-hour session and in the general access areas, it is a 3-hour session). This allows for two critical issues to be controlled while users have access. First and foremost it tracks which person is actually assigned to the IP address that may be in violation. For instance, if a student goes to a public access port and connects, the user must login; therefore, being able to monitor which user is connected at what time. Also valuable, since the sessions expire at most every twenty-four hours, users are not able to download the extremely large files that take several days to acquire.

Methodology of Researching University Policies:

The Acceptable Use Policies of all the Division I institutions (See Appendix D) were collected by searching each of the 117 schools' websites and printing a hard copy of their policies concerning acceptable use. The hopes were that using the websites of each institution would provide the most current version of the policies. This however may not be the case if the newest version had not been uploaded for viewing at the time of the search. Also to be considered is the type of schools that are part of the NCAA's Division I for football. A vast majority of these institutions are very large public schools that may hold different standards as compared to their smaller counterparts. The reason this manner of selection was chosen is because of an already well-established grouping of institutions that tend to be institutions at the heart of most new occurrences. For a listing of all the institutions studied, please follow the link:

http://web1.ncaa.org/ssLists/sportByInst.do?sport=MFB&division= 1.

Policy Critique:

During the research for this thesis, the computing policies of each Division I institution were collected to compare and contrast how effective these regulations are in both insulating the institution from legal recourse by the RIAA and in informing students, faculty, and staff of their responsibilities in ethical behaviors while using the campus computer infrastructure. The challenge in gathering each of these policies was that there was no one name that was consistently used by every school in naming their policies. Among the names found were: Acceptable Use Policies, Code of Computing Ethics, and Computing Policies (for the purpose of this paper, the term Acceptable Use Policy is used). A vast majority of the institutions studied had policies in place as required by the DMCA. Many state laws (such as Arkansas's Act 1287 of 2001) require state agencies to create acceptable use policies.

There are two primary means by which universities have enabled themselves to limit the amount of illegal downloading that occurs at their respective campuses. First and foremost is that almost every school includes a sentence in their policies that requires all users to follow all university policies, as well as local, state, and federal regulations. Obviously, this requires any users on the campus networks to abide by the aforementioned laws. Many institutions have started to include some additional resources in their Acceptable Use Policies. Copies of the DMCA, state and local laws, and special notices about copyright violations have become increasingly prevalent in policies. The second restriction that schools place on their users is that they may not partake in activities, which tie up the resources of the infrastructure and hinder the academic pursuits of the faculty and students. With the increased number of files being downloaded or streamed, the students in the residence halls have monopolized much of the bandwidth. However, if this problem becomes excessive, schools would then be able to sanction them based on this rule without knowing if they had illegal materials.

Through the research conducted, there was one university that stood out as having excellent policies in contrast with their peers in regards to their inclusion of copyright information. The

University of Arizona has policies that were very comprehensive without being excessive. Section 7 of the Acceptable Use of Computers and Networks at the University of Arizona is extremely inclusive of what constitutes infringement and also includes links to internal and external sources. The reason this is so beneficial is because students may not be aware of all the legal aspects of possessing or trading these illegal materials. While a majority of the schools studied only state that students must follow all appropriate laws, Arizona has included a specific link to a page devoted to the use of P2P programs and links to the U.S. Copyright Office as well. Also important is the use of being somewhat broad in the policies. Some institutions mention copyright infringement, but only as it relates to the software piracy that is common today. If institutions make this reference, they should be careful and also include references to how users can get into trouble by illegally copying other forms of data files. Otherwise, the users may claim that they "thought only software was illegal because that is all that is mentioned in the policies."

Some institutions have chosen to include examples of violations of the policies which have been set forth. While this is very beneficial to readers, policy makers must be careful and should include a phrase to the extent of, "these example are provided for practical knowledge; however, they are not all inclusive."

A number of schools also take the liberty to add in the punitive sanctions that can be brought against those found in violation of the school's policies. The sanctions are fairly common among the institutions:

1) After a charge has been brought against the student, an administrator will meet with or e-mail the student and discuss the violation with the individual.

2) The offender's Internet access will be disabled (sometimes immediately) either temporarily, or for repeat offenders, permanently.

3) Seizure of equipment that contains the illegal content.

4) Censorship of the material if posted on a website within the university's domain.

5) Referral to the proper legal authorities.

The trend with institutions today is to limit the violator's access immediately. At the University of Arkansas, a typical educational sanction requires a student found in violation to write a five-page paper concerning the topic of copyright infringement or intellectual property ownership.

Recommendations:

When creating or revising Acceptable Use Policies, institutions must be acutely aware that students are not fully knowledgeable in the most current legal proceedings. Children have never had the accessibility to computers and the Internet as they do now, and many start downloading music when they are in elementary or junior high school. Since this is almost a part of everyday life now, the challenge for collegiate institutions will be to educate their students and staff about the legal ramifications of this activity. Therefore, the inclusion of a section specifically dedicated to intellectual property rights is crucial. Also, much like some of the institutions currently have in place, computing policies should include links to the more crucial information that is outside of the university's policy which students may not have direct interaction with. Information such as the DMCA, NET Act, the Educase website, and any local or state regulations would be very advantageous in the education of students. Also, the consolidation of all relevant documents into one comprehensive policy would be very beneficial. Lastly, inclusion of a code of ethics can be greatly helpful. One such code is the EDUCOM Code of Software and Intellectual Rights (See Appendix E). This Code can be easily adapted to any institution and could also be part of a document that each user signs in agreement to abide by all relevant policies and laws. Once this policy is created, students, faculty, and staff should have easy access to this document. The ultimate link would be off of the homepage of each institution's website. If each institution could include the link at the bottom of the homepage with their privacy policies and other disclaimers, users would not be able to use that as an excuse for being ignorant of the policies.

In evaluating the sanctions handed out by the institutions, the vast majority of the sanctions are understandable. However, the troubling one is the immediate restriction on the use of the network's services. For instance, at the University of Arkansas, when Computing Services is notified that one of their users has been caught downloading or sharing illegal materials, the department immediately disables the Internet port in question (since copyright owners are able to identify the alleged IP address identified as infringing, this allows the department to identify the user). However, this seems to be contradictory to our nation's Constitution which states individuals are "innocent until proven guilty." In the current system, which is common across the nation, it would seem as if users are "guilty until proven innocent."

The Future:

Napster's service seems to be in direct contradiction to what some network administrators are trying to curtail. It is well known that streaming music and video requires much more bandwidth than a simple download of each of these songs that Napster would be providing. This seems to be the opposite of what many administrators have stated is one of their primary goals, which is to reduce the amount of network traffic from these downloads. The campus administrators of institutions which are contracting with Napster may see problems with having students stream so much multimedia content that

bandwidth will be monopolized by these files without any sort of hardware controls. Furthermore, with the proliferation of legal online music sources, Napster has not been as successful. For instance, one of the newest sources for online music downloads is Wal-Mart's website (www.walmart.com). Here shoppers can purchase individual songs without having to have a monthly subscription and each song costs only $0.88. With approximately the same size library of songs available to download, Wal-Mart also has exclusive rights to certain hit songs. The only problem with Wal-Mart's service is they only offer edited songs, which could eliminate a possible source of sales for the company. With this new entrant, one would predict that other vendors would have to lower costs and/or eliminate any monthly service charge. With almost every other music vendor offering songs at $0.99, they will have to compete with Wal-Mart's new prices. However, Wal-Mart has an advantage in being able to sustain losses for their initial period while trying to drive out their competitors. This being said, the stamina that programs like Napster show will be quite intriguing. Also, it would seem like that the agreements between Napster and institutions like Penn State will become less prevalent as students who wish to follow legal methods turn to the new low price alternatives.

One interesting combination of the previous two policy recommendations could facilitate legal transfers. That is, if an institution were to block all P2P file-sharing programs except one, the one that the school contracts with, then they could still allow the transfer of these legal files. These files would all be legitimate copies of each file. However, many of the legal sites that offer files available for purchase would not even require a second fee in order to copy to a different media. Therefore, the students' fees that are paid each year could then be applied to these contracts with providers.

There are hundreds of ways in which students at universities violate copyright laws. While downloading material is one manner in which students acquire files, universities must realize that there is no way they can eliminate the exchange of these files. College administrators and the RIAA will continue to face the entrepreneurial spirit of college students. For instance, record labels have started to encrypt CDs that have intermittent sounds that destroy the quality of any copies; however, this encryption problem was short lived as users found ways to bypass this issue. Having this situation at college campuses is quite a unique situation. In one way, administrators hope the encryption is not broken in order to reduce the amount of traffic. On the other hand, our classrooms are the setting where students are learning how to break these encryption codes which allow them to continue in this problem. Once users broke this "problem", it was only a matter of time until the content on the P2P networks again became illegitimate copies. Therefore, our incubators of knowledge are helping to promote the problem at hand.

The future also contains means by which very creative individuals will bypass the entire process of having to worry about being caught for sending MP3 files. In an interview with Eric Roberts, Associate Director for Technology for University Housing at the University of Arkansas, Mr. Roberts said that a fear is that one day converting MP3 files into a HyperText Transfer Protocol (herein referred to as http) file could become commonplace. This is the same protocol used for creating common web pages. Essentially, this conversion would create an enormous http file that is indistinguishable from other http pages (Roberts). Once this conversion takes place, users could download these files and convert them back into MP3 files. The problem then posed to administrators is being able to discern a standard webpage from the converted music file because the only distinguishing difference would be size that cannot solely be a determinant. As of now, the technology to create these http files is not available, nor is the technology to detect it. Essentially, it seems to be a race to find out if this may one day become a prevalent issue.

Music is not the only source of problems that face campus administrators. Software, video, and academic plagiarism through the campus networks are also issues that are very prevalent today. In fact, this has become such a significant problem that the RIAA has collaborated with the Motion Picture Association of America (MPAA), the Software and Information Industry Association (SIIA), and the Entertainment Software Association (ESA). The video, software, and music industries are all taking a very strong stance on securing their rights in regard to copyrights. As seen in the research, thousands of individuals have been sued, laws have been created, and policies have been set. Most recently, on March 31, 2004 the U.S. House of Representatives passed legislation entitled the "Piracy Deterrence and Education Act of 2004." Within this legislation, Congress recognizes the issue that P2P networks bring to copyright owners and attempt to institute policies that will eliminate this issue by expanding upon the sanctions that are available through the NET Act. The new sanctions for a first violation include up to three years imprisonment for violators with a possible five years available if the user has commercial intentions in violating the copyrights. These sanctions can double for a second or subsequent offense. This Act did not only create criminal penalties for each of these offenses. Also included were programs developed to educate different organizations on the most up-to-date information in regards to enforcing copyrights, as well as a program called the Internet Use Education Program that would try to educate the public on current issues. These programs allow the federal government to reduce the likelihood of a person claiming ignorance

Also, the Federal Bureau of Investigation (FBI) is working with the RIAA, MPAA, SIAA, and the ESA on a new program to create an "Anti-Piracy Warning Initiative." Announced on February 19, 2004 the FBI and the various organizations will spend billions of dollars in this effort. With this program, a new seal will be displayed on future copyrighted materials

(www.fbi.gov). In addition, an "Education Letter" (See Appendix F) has been created for informational purposes.

The aforementioned industries have not been completely successful in their attempts to deter copyright infringement globally. In late March 2004, a Canadian Federal Court Judge ruled that service providers cannot be forced to identify their users to the Canadian Recording Industry Association or other copyright owners (CTA.ca). More than likely to be appealed, this decision is similar to the Verizon case mentioned previously in regard to U.S. law. Citing a lack of evidence to turn over the private information, Judge Konrad von Finckenstein compared the transfer of music to a photocopy machine. Von Finckenstein said, "I cannot see a real difference between a library that places a photocopy machine in a room full of copyrighted material and a computer user that places a personal copy on a shared directory linked to a P2P service."

Conclusion:

It is obvious that the measures taken by the Recording Industry of America have made a tremendous impact on the number of illegal files transmitted from user to user. In fact, after the announcement on June 29, 2003 that they would be targeting individual violators, there was a decrease of approximately two million users of Kazaa in the subsequent three months. Some of the files available to the public on these file-sharing networks expose customers to legal liability. Thousands of users have had to curtail their downloads in fear of having legal action taken against them. Furthermore, administrators of collegiate networks across the world have had to take strict action in order to limit the liability for the universities in which they work. However, the end of this problem is still years away. New technology, creative minds, and the ever-threatening specter of illegal manifestation on collegiate networks are impending, and network administrators must remain vigilant in protecting their infrastructure. Another key aspect is the continued battle of the legal music providers to entice the key market of college students to buy their products. More than likely, the trend to enter into contracts with music providers like Napster is over; however, new ideas are imminent and only time will tell what the future holds for not only the United States, but the global community as a whole.

Works Cited:

Baker, Chris. "U.S. Naval Academy Seizes Students' Computers. *Knight Ridder Tribune Business News*.Harm Washington: pg. 1, 26 November 2002.

Carlson, Scott. "Appeals Court Rules that Napster Violates Copyright Law." "The Chronicle of Higher Education." *Information Technology*, pg. 44. 23 Feb 2001.

—. "Napster Was Just the Start of the Bandwidth Invasion." "The Chronicle of Higher Education." *Information Technology*, pg. 43. 27 April 2001.

—. "New Jersey Institute of Technology Prohibits File Sharing on Its Campus." "The Chronicle of Higher Education." 1 May 2003. http://chronicle.com/free/2003/05/2003050101t.htm

—."Record Companies Settle Lawsuits Against 4 Students." "The Chronicle of Higher Education." 2 May 2003. http:/chronicle.com/free/2003/05/2003050201t.htm

—. "Record Industry Will Send Warnings to Millions of Users of 2 File-Sharing Services." "The Chronicle of Higher Education." 30 April 2003. http://chronicle.com/free/2003/04/2003043001t.htm.

"Content Community, College Groups Outline Threat of P2P, Ask for Action." Press Release. Recording Industry Association of America. 10 October 2002. http://www.riaa.com/news/newsletter/101002.asp.

CTV.ca News Staff. "Music industry loses in downloading case." 31 March 2004. http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1080754657038_76163857.

Harmon, Amy. "261 Lawsuits Filed on Internet Music Sharing." *New York Times Online*. 10 September 2003. http://www.nytimes.com/2003/09/09/technology/09MUSI.html?ex=1064389056&ei=1&en=3b2Q1.

Harmon, Amy. "New Parent-to-Child Chat: Do You Download Music?" *New York Times Online*. 9 September 2003. http://www.nytimes.com/2003/09/10/technology/10MUSI.html?ex=1064389152&ei=1&en=2b23b.

Harmilton, Marci. "Why Suing College Students for Illegal Music Downloading Is The Right Thing to Do." 05 August 2003. http://writ.news.findlaw.com/hamilton/20030805.html.

Hawke, Constance S. *Computer and Internet Use on Campus*. San Francisco: Josey-Bass, Inc, 2001.

Napster Was Nothing Compared with This Year's Bandwidth Problems. "The Chronicle of Higher Education." Information Technology, pg. 44. 28 September 2001.

Read, Brock. "Penn State Offers Students a Legal Way to Download Music." "The Chronicle of Higher Education." *Information Technology*, pg. 29. 21 November 2003.

Remington, Michael J. "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks." Drinker Biddle & Reath LLP, Washington D.C. 7 August 2003

"RIAA Releases Yearend Anti-Piracy Statistics." Press Release. Recording Industry Association of America. 5 March 1998. http://www.riaa.com/news/newsletter/press1998/030598.asp.

Roberts, Eric. Personal Interview. 8 April 2004.

Schwartz, John. "A Software Program Aimed at Taming File-Sharing." *New York Times Online*. 8 March 2004. http://www.nytimes.com/2004/03/08/technology/08_music.html?ex=107979751.2&ei=1&en=8151758c27f20ff4.

"Suing Music Downloaders." Editorial. *New York Times Online*. 12 September 2003, http://www.nytimes.com/2003/09/12/opinion/12FRI2.html?ex=1064389008&ei=1&en=fc0ff28c.

United States. Federal Bureau of Investigation. *FBI, In Partnership with Entertainment and Software Industries, Announce Anti-Piracy Warning Initiative*. 19 February 2004. http://www.fbi.gov/pressrel/pressrel04/piracy021904.htm.

Appendices:

Appendix A:

Timeline of Important Events:

May 1999 - Napster Inc. file-sharing service is founded by Shawn Fanning and Sean Parker and explodes in popularity.

Dec. 7, 1999 - Recording Industry Association of America (RIAA) sues Napster in federal court in San Francisco alleging copyright infringement.

April 13, 2000 - Heavy metal rock group Metallica sues Napster for copyright infringement and racketeering. Rapper Dr. Dre files suit two weeks later.

July 2000 - Patel grants the RIAA's request for a preliminary injunction and orders Napster shut down. Soon after, the 9th U.S. Circuit Court of Appeals stays the lower court injunction, ruling that "substantial questions" were raised about the merits and form of Patel's injunction.

Oct. 2001 - The recording and film industries sue the companies behind the Grokster and Morpheus file-swapping services. The company behind the Kazaa file-swapping service is added to the suit later.

Jan. 21, 2003 - U.S. District Judge John D. Bates rules that Internet providers must agree to music industry requests to identify users who illegally download music. The case arose when Verizon Communications Inc. resisted a subpoena from the RIAA to track down several file-swappers.

April 3, 2003 - Hoping to "send a message," the RIAA files lawsuits against four college students who operate computer networks the RIAA says distribute copyrighted songs. One network reportedly distributed over 1 million files; the suit seeks $150,000 for each copyrighted work that was downloaded.

April 24, 2003 - In a win for the RIAA, Judge Bates rules that Verizon must hand over the names of two customers suspected of illegal file swapping. Verizon appeals the ruling.

April 25, 2003 - Judge Stephen Wilson of U.S. District Court in Los Angeles rules that Grokster and Morpheus do not have direct control over files swapped on their networks and cannot be held liable for copyright infringement committed by their users. The entertainment companies appeal.

April 29, 2003 - As part of its anti-piracy "education initiative" the RIAA, along with other music industry groups, begins sending out instant messages to a planned one million file-swappers using peer-to-peer networks Kazaa and Grokster warning them that exchanging copyrighted songs is illegal.

May 2, 2003 - The RIAA reaches settlements with the four college students it sued for trading copyrighted music files over college campus computer networks. The payouts range from $12,000 to $17,500 - substantially less than the initial lawsuits sought.

June 5, 2003 - After losing a court battle, Verizon Communications Inc. surrenders the names of four of its Internet customers to the RIAA, which had accused them of illegally offering song downloads.

June 25, 2003 - Continuing their aggressive strategy, the RIAA announces plans to sue hundreds of individual file-swappers who offer "substantial" collections of mp3s for downloading. Critics accuse the RIAA of resorting to heavy-handed tactics likely to alienate millions of music lovers.

July 14, 2003 - An Internet tracking firm reports the number of people using several Internet file-sharing services has declined by several thousand a week after the music industry's threat to sue online music swappers.

Sept. 8, 2003 - The RIAA files 261 lawsuits against individual music lovers, accusing them of illegally downloading and sharing songs over the Internet. The action, which had been expected, follows subpoenas sent to Internet service providers and others seeking to identify roughly 1,600 users.

October 2003 - Napster comes back online as a pay service with the blessing of all five major music labels. It launches with more than a half-million songs and retains some of the community features that made the old version so popular, such as allowing subscribers to trade songs and play lists.

Jan. 21, 2004 - The RIAA sues 532 "John Doe" defendants identified only by their numeric Internet protocol addresses. It's the industry's first action since an appeals court ruled that subpoenas couldn't be used to force Internet providers to identify music downloaders without filing a lawsuit first.

March 23, 2004 - The recording industry sues 532 people for allegedly sharing digital music files over the Internet. For the first time, individuals using computer networks at universities are among the targets.

Credits: CBS News, Associated Press, Wired Magazine

Appendix B:

CBS NEWSMEW YORK TIMES POLL: ONLINE MUSIC SHARING

September 15-16, 2003

q42 How closely have you followed the issue of people sharing music for free through the Internet? Would you say you've followed it very closely, somewhat closely, not very closely, or not at all?

TOTAL RESPONDENTS

		***** Age*****	
	Total%	18-29%	30 and older%
Very closely	8	13	7
Somewhat closely	31	39	29
Not very closely	23	19	24
Not at all	37	28	40
DK/NA	1	1	0

q43 When it comes to sharing music over the Internet for free, which comes closest to your view:

1. Sharing music files over the Internet is ALWAYS acceptable, no matter how many copies are made, or by whom, OR

2. Sharing music files over the Internet is SOMETIMES acceptable, if a person shares music from a CD he or she owns with a limited number of friends or acquaintances, OR

3. Sharing music files over the Internet is NEVER acceptable because it deprives musicians and music companies of their income?

THOSE WHO FOLLOW THE ISSUE

	***** Age*****		
	Total%	18-29%	30 and older%
ALWAYS acceptable	14	29	9
SOMETIMES acceptable	44	40	46
NEVER a cceptable	37	30	40
DK/NA	5	1	5

q44 Several companies are now letting people purchase individual songs over the Internet for a small price. What do you think would be a fair price to pay for an individual song that you could get on the Internet, listen to, and burn onto your own CD?

Up to 50 cents	15	27	12
51 cents to $1.00	29	33	28
$1.01 - $2.00	13	17	12
$2.01 - $5.00	17	15	18
over $ 5.00	2	0	3
Nothing	1	2	0
DK/NA	23	6	27

	UNWEIGHTED	WEIGHTED
Total Respondents	675	
Total ages 18-29	101	149
Total ages 30 and over	571	524

The poll was conducted among a nationwide random sample of 675 adults interviewed by telephone September 15-16, 2003. The error due to sampling could be plus or minus four percentage points based on the entire sample. Sampling errors for subgroups may be higher. The error due to sampling on Americans age 18-29 could be plus or minus ten percentage points.

Appendix C:

The text of the warning letter from Napster:

"It appears that you are offering copyrighted music to others from your computer. Distributing or downloading copyrighted music on the Internet without permission from the copyright owner is ILLEGAL. It hurts songwriters who create and musicians who perform the music you love, and all the other people who bring you music.

When you break the law, you risk legal penalties. There is a simple way to avoid that risk: DON'T STEAL MUSIC, either by offering it to others to copy or downloading it on a "file-sharing" system like this.

When you offer music on these systems, you are not anonymous and you can easily be identified. You also may have unlocked and exposed your computer and your private files to anyone on the Internet. Don't take these chances. Disable the share feature or uninstall your "file-sharing" software. For more information on how, go to http://www.musicunited.net/5_takeoff.html.

This warning comes from artists, songwriters, musicians, music publishers, record labels and hundreds of thousands of people who work at creating and distributing the music you enjoy. We are unable to receive direct replies to this message. For more information about this Copyright Warning, go to http://www.musicunited.net."

Appendix D:

Definition of Division I Institution by the NCAA (www.ncaa.org)

Division I member institutions have to sponsor at least seven sports for men and seven for women (or six for men and eight for women) with two team sports for each gender. Each playing season has to be represented by each gender as well. There are contest and participant minimums for each sport, as well as scheduling criteria. For sports other than football and basketball, Div. I schools must play 100% of the minimum number of contests against Div. I opponents —anything over the minimum number of games has to be 50% Div. 1. Men's and women's basketball teams have to play all but two games against Div. 1 teams, for men, they must play 1/3 of all their contests in the home arena. Schools that have football are classified as Div. I-A or I-AA. I-A football schools are usually fairly elaborate programs. Div. I-A teams have to meet minimum attendance requirements (17,000 people in attendance per home game, OR 20,000 average of all football games in the last four years or, 30,000 permanent seats in their stadium and average 17,000 per home game, or 20,000 average of all football games in the last four years, OR be in a member conference in which at least six conference members sponsor football or more than half of football schools meet attendance criterion. Div. I-AA teams do not need to meet minimum attendance requirements. Div. I schools must meet minimum financial aid awards for their athletics program, and there are maximum financial aid awards for each sport that a Div. I school cannot exceed.

Appendix E:

EDUCOM Code - Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, authorized access, and trade secret copyright violations, may be grounds for sanctions against members of the academic community.

Appendix F:

Letter from the FBI in their new Anti-piracy Initiative:

To Users of Peer-to-Peer Systems:

The FBI has undertaken a new initiative to educate and warn citizens about certain risks and dangers associated with the use of Peer-to-Peer systems on the Internet. While the FBI supports and encourages the development of new technologies, we also recognize that technology can be misused for illicit and, in some cases, criminal purposes. In an effort to help citizens learn how to protect themselves, this letter is being distributed and is posted on the FBI's web site at www.fbi.gov/cyberinvest/cyberedietter.htm.

Peer-to-Peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files. Typically, users of Peer-to-Peer networks install free software on their computers which allows them (1) to find and download files located on another Peer-to-Peer user's hard drive, and (2) to share with those other users files located on their own computer. Unfortunately sometimes these information-sharing systems have been used to engage in illegal activity. Some of the most common crimes associated with Peer-to-Peer networks are the following:

Copyright Infringement: It is a violation of Federal law to distribute copyrighted music, movies, software, games, and other works without authorization. There are important national economic consequences associated with such theft. The FBI has asked industry associations and companies that are particularly concerned with intellectual property theft to report to the FBI — for possible criminal investigation and prosecution—anyone that they have reason to believe is violating Federal copyright law.

Child Exploitation and Obscenity: The receipt or distribution of child pornography and unlawful obscenity over the Internet also is a serious Federal crime. The FBI cautions parents and guardians that, because there is no age restriction for the use of Peer-to-Peer services, pornography of all types is easily accessible by the many young children whose parents mistakenly believe they are only accessing music or movies. In fact, children may be exposed to pornography — and subsequently lured by sexual predators — even though they were not searching for pornography, as some network users deliberately mislabel the names of files for this purpose.

Computer Hacking: Peer-to-Peer networks also have been abused by hackers. Because these systems potentially expose your computer and files to millions of other users on the network, they also expose your computer to worms and viruses. In fact, some worms have been specifically written to spread by popular Peer-to-Peer networks. Also, if Peer-to-Peer software is not properly configured, you may be unknowingly opening up the contents of your entire hard drive for others to see and download your private information.

The FBI urges you to learn about the risks and dangers of Peer-to-Peer networks, as well as the legal consequences of copyright infringement, illegal pornography, and computer hacking. For more information about the law, visit www.usdoj.gov/criminal. The FBI takes seriously its mission to enforce the laws against those who use the Internet to commit crime. To report cyber crime, please contact your local FBI Field Office, www.fbi.gov/contact/fo/fo.htm or file a complaint through the Internet Crime Complaint Center at www.IC3.gov.

Faculty Comments:

Professor John Norwood, Director of the Walton College Honors Program, made the following remarks about Mr. Wendel's research:

This paper deals with a current and important topic: the policies of institutions of higher education toward copyright infringement by students. This proposal was accepted by SURF for an undergraduate research grant: clearly they believed that the topic was timely and important. Now that the project has been completed, I can say that their confidence was well founded.

Henry has done a tremendous amount of background work on this topic. He was in contact with more than 110 universities from across the country, and examined each of their copyright policies. He then assembled this information into a coherent whole that is both interesting and informative.

I believe that Henry's work will be used as a guide by a number of universities, including the University of Arkansas. He has been very thorough and diligent in his work, and the result is a piece of work that is truly outstanding.

In summary, I believe that this project has resulted in an outstanding research paper.