

TOPIC:

PEER-TO-PEER FILE SHARING REQUIREMENTS OF THE HIGHER EDUCATION OPPORTUNITY ACT

INTRODUCTION:

The Higher Education Opportunity Act (HEOA), enacted on August 14, 2008, creates new requirements for colleges and universities regarding peer-to-peer (P2P) file sharing. The law and its implementing regulations require student notification of copyright law and its associated penalties, and the establishment of a coherent plan to address P2P activity on campuses. This NACUANOTE discusses the new HEOA requirements established in the statute and regulations, their relation to current legal requirements, and what colleges must do to comply.

DISCUSSION:

It's Tricky [1]: Current DMCA Requirements for Colleges

Those colleges and universities that directly provide some form of Internet access qualify as Internet Service Providers (ISPs). Like their commercial counterparts, college ISP's are eligible for the legal protections afforded by the Digital Millennium Copyright Act (DMCA), including safe harbors from liability due to their users' activities.

To qualify for all of the safe harbors enumerated in the legislation, universities must take some proactive steps. Universities must have a policy or program that terminates repeat infringers and must not prevent copyright owners' efforts to locate and protect their intellectual property [2]. The requirements distinguish between college-owned devices [3] and personal devices [4].

Send Lawyers, Guns & Money: Congress and the HEOA [5]

In 2008, Congress passed, and President Bush signed, the Higher Education Opportunity Act [6], an amendment to the Higher Education Act of 1965 [7]. Included in the hundreds of pages of the Act, within the section governing Title IV Financial Aid, are short paragraphs requiring all colleges that accept federal financial aid to take steps to stem the spread of peer-to-peer file sharing. The Department of Education (the Department) issued proposed [8] and final [9] regulations on preventing peer-to-peer file sharing in 2009. The regulations reflect compromises reached during earlier negotiated rulemaking sessions with representatives of the entertainment industry and higher education [10] and officially took effect July 1, 2010. Before then, colleges were simply required to make "best efforts" to comply with the statute.

Two Step [11] to Comply: P2P in the Higher Education Opportunity Act

HEOA includes two sections; referred to herein as a "notification" requirement [12] and a "written

plan" requirement [\[13\]](#) that affect peer-to-peer file sharing. The Congressional Record that accompanied passage of the statute provides some context to Congress' intent in crafting this language [\[14\]](#).

Regulate [\[15\]](#): The Final Regulations on P2P

The final Department P2P regulations clarify the statutory language by further detailing what constitutes actual compliance on a campus. The notification requirements were virtually unchanged [\[16\]](#). The written plan requirements, however, are far more detailed [\[17\]](#).

The Times They Are a Changin' [\[18\]](#): Complying with the New Requirements

Contrary to initial concerns, the new regulations do not require significant expenditures to comply. Colleges do not *have* to purchase technology-based deterrents and most colleges will not have to expend additional funds or acquire new hardware or software to comply. Rather, the regulations require notification to students, some organization and policy drafting by each college or university, and a decision on whether and how it will comply with the technology-based deterrents requirement, often by continuing current administrative practice.

The Department states that the final regulations only apply to colleges that provide students with "school-maintained and operated internet services," thus exempting those institutions that provide no Internet service [\[19\]](#).

Notifications

P2P notification will accompany the many other notifications printed (or digitally created) annually in a student handbook or similar document [\[20\]](#). It consists of three parts: a statement that unauthorized distribution of copyrighted material may bring civil and criminal penalties, a summary of the penalties for violating copyright law, and a description of the college's specific policies. In June 2010, the Department published a "Dear Colleague" letter summarizing the regulatory requirements, and offering sample language, developed in conjunction with the content industry and colleges, that colleges *may* use to meet the notification requirement [\[21\]](#). In the interim and in addition to that sample, other samples appear in this note [\[22\]](#). The institution need not provide such notice to faculty and staff [\[23\]](#).

Written Plan

If your college does not have a written plan to handle file sharing, the regulations require your college to draft one [\[24\]](#). The regulations state that these plans do not need to be all encompassing or interfere with your college's educational or research business practices [\[25\]](#). The Department specifies that any written plan must apply to all users of a college's network (including faculty, staff, contractors, and guests), not simply to student users [\[26\]](#).

- **Education**

The written plans must include an educational component. The proposed Regulations stated somewhat opaquely that educating mechanisms "could include any additional information and approaches determined by the institution to contribute to the effectiveness of the plan, such as including pertinent information in student handbooks, honor codes, and codes of conduct in addition to e-mail and/or paper disclosures [\[27\]](#)." Colleges across the country have taken different approaches to educating their students. Cornell, for example, employs an educational video using real students [\[28\]](#), and the University of Michigan has developed "BAYU" or "Be Aware You're Uploading," an educational and action system that tracks

uploading of content and notifies users that they may be uploading in violation of the law [29]. Your college may use similar or different mechanisms to notify students about appropriate and inappropriate use of copyrighted material, but your college's tactics should reflect its culture and values.

- Responding to Unauthorized Distribution of Copyrighted Material

Your written plan must include procedures for handling unauthorized distribution of material (read: illegal file sharing), including the use of your college's student disciplinary process. The regulations do not require that the institution actively monitor networks or seek out students to discipline. However, when the issue is brought to the attention of the college, typically by means of a valid DMCA notice, the college must have written procedures for handling the matter, usually, by removing the student from the network, at least temporarily, asking them to remove the offending file from their computer or stop sharing that file, and potentially using the college disciplinary process.

College disciplinary procedures for illegal file sharing are as diverse as colleges themselves. Some terminate students from the network for short amounts of time, others for longer. Some colleges refuse to terminate students from the network during final exam or study periods. Others charge students a fee to reconnect to the network; sometimes that fee escalates for repeat offenders [30]. Some colleges ask their judicial affairs department to discipline accused students while others leave the discipline to IT professionals [31]. At other institutions, first offenses are handled by IT professionals and subsequent offenses are handled by student affairs administrators. The regulations do not specify *how* a college must use its disciplinary process for illegal file sharing, just that discipline must be a potential part of the process, at least for certain cases.

- Technology-based Deterrents

The institution's written plan must include the use of one or more technology-based deterrents [32]. Institutions are offered several options for such deterrents, and the regulations state plainly that they do not favor one technology over another [33]. Some technological options are hardware and software blocking packages, aggressive manual (or automatic) processing of DMCA notices, dialing down bandwidth and packet shaping. Each of the above-referenced methods interacts at a different level with network operations. The feasibility of implementing each method will vary from institution to institution. Some examples of technology-based deterrents are:

- *Packet Shaping*: Packet shaping works to "shape" the speed of data over the institution's network. These technologies classify, analyze, and manage the bandwidth, giving priority to certain types of data, such as e-mail while de-prioritizing other types of data, such as shared files [34].
- *Content Filters*: Content filters in the form of hardware and software solutions are generally considered the most intrusive and costly of the technology-based deterrent options. These filters are placed directly on the network and scan all network traffic seeking matches to the digital "fingerprints" stored in the device. Files that are a match to these fingerprints are blocked [35].
- *Low-tech Options*: Accepting and responding to DMCA notices, as outlined in the notes to § 1 above. The Automated Copyright Notice System, developed in 2003 by NBC Universal and Universal Music Group (UMG) with support from Disney, provides a technical framework for the automated processing of DMCA notices [36]. Many schools have implemented ACNS, or built onto it, to move away from the time

and resource consuming manual processing of the notices [37]. Others handle the process manually.

- Legal Alternatives for Downloading Copyrighted Material

The regulations also require that institutions periodically review the current state of legal alternatives for downloading or otherwise acquiring copyrighted material and publish that review on a college Web site or otherwise distribute that information to students. EDUCAUSE makes a list of known legal file sharing alternatives available to the higher education community [38]. Inasmuch as few colleges have the staff to monitor the industry the way EDUCAUSE does, a link to their list may assist institutions in staying in compliance with this requirement as technology and the industry change.

In addition to publishing the list of legal alternatives, the regulations require that institutions also offer legal alternatives for downloading or otherwise acquiring copyrighted content, “to the extent practicable”. The Department has commented that simply not blocking legal alternatives does not satisfy the requirements, as it is not the same as making legal alternatives available [39]. In a “Dear Colleague” letter issued in June, 2010 the Department reaffirmed that legal alternatives need only be made available to the extent practicable, but provided no further guidance [40]. The road to offering legal downloading alternatives to college students is paved with a lot of mis-starts and failed attempts such as the re-branded Napster, Roxio, and Ruckus [41]. Companies of more recent vintage are meeting with colleges and universities seeking takers for new business models [42].

- Periodic Review of Written Plan

Finally, the written plan must include language that requires periodic review of said plan to determine its continuing effectiveness. The proposed regulation stated that “[i]t would be left to each institution to determine what relevant assessment criteria are, [43]” although nothing in the language of the proposed or final regulations defines how long “periodic” is. An annual review of the college’s plan, prior to the annual publication, and in consideration of changes in the technologies and student habits and behaviors, would seem to be reasonable. Some institutions may use a “process-based review” while others find an “outcome-based review” more satisfactory [44].

The Next Episode [45]

While it is unlikely that the regulation’s requirements will be amended in the near term, the entertainment industry continues to seek federal protection from digital content sharing in order to maintain its market share [46]. Concurrently, the industry is using a state-by-state campaign to enact statutes that may require even more effort by colleges and universities [47]. Such state laws may create different requirements for public and private colleges in certain states. Finally, several private and industry groups look to work with colleges to provide legal downloading alternatives.

CONCLUSION:

Closing Time [48]: Final Thoughts on Compliance

College and university attorneys, and the policy makers with whom they work, should consider the unique environment at each institution and craft their compliance with an eye toward that environment and the lessons the institution wishes to impart to its students, while not demonizing any specific technology [49]. While it is perfectly acceptable for a college to use the sample notices provided here or in the Federal Financial Aid Handbook, or to draft a notice that reads like the first screen on a DVD [50], the broad regulations also provide an opportunity to share the college's values on intellectual property and to educate your students on the distinctions between legal and illegal uses of other's creative works. Remember that your institution is likely a major creator and user of intellectual property, and may even occasionally avail itself of the protections provided by the law. Further, the written plan requirements provide opportunities to educate students on fair use, property rights, and some of the thorny ethical issues that arise in the digital era. While compliance with the laws and regulations will not be onerously difficult for most colleges, a little creativity will go a long way toward preparing your students for a digital world peppered with questions of creation, ownership and sharing of data and content.

FOOTNOTES:

FN1. Run-DMC, *It's Tricky*, on RAISING HELL (Profile Records 1987). We imagine that the first thing a copyright-sensitive attorney will ask when they see the titles and headings in this paper and accompanying links to You Tube sites is whether we are violating copyright or whether it is fair use. In fact, it is not fair use; it isn't even use at all. Rather, we are simply referencing a use that may or may not be a proper use of work on a third-party site. The authors happen to like the songs that we chose as headings in this paper and encourage readers to legally obtain that content after sampling the songs on the You Tube links.

FN2. See 17 U.S.C. § 512(i)(1); see also Steven J. McDonald, *Face the Music: The Law and Policy of File Sharing* (Feb. 21-24, 2009) (PDF).

FN3. Two additional requirements must be met to satisfy the safe harbor under § 512(c) of the legislation. That section addresses "[i]nformation residing on systems or networks at direction of users" (17 USC § 512[c]) and applies to "a system or network controlled or operated by or for the service provider" (*Id.*). This section is interpreted to govern university-owned resources, such as faculty, staff, and computer lab computers. Universities must register a designated agent with the Copyright Office to receive notices of violations (See 17 USC § 512 [c] [2]). The Copyright Office maintains a directory of such agents (See 17 USC § 512 [c] [2]). In order to maintain the "safe harbor" under the law and not be liable for monetary damages for infringing material on an ISP's server, the ISP must not have "actual knowledge" of the infringing material, not receive a direct financial benefit from the infringement, and, when notified, must "respond expeditiously" to remove the infringing material or disable access to such material (See 17 USC § 512 [c] [1]). The statute sets out the elements required in a "takedown" notification (See 17 USC § 512 [c] [3]). Inasmuch as these are computers that the college or university actually *owns*, the institution *must* take action when it receives a DMCA takedown notice or risk its safe harbor.

FN4. Section 512(a) also applies to university networks and governs "[t]ransitory digital network communications." This section of the legislation provides immunity to the ISP for information that

simply transits the ISP's networks, with no direction, input, or interference from the ISP itself, and is not stored anywhere on the ISP's network. Notably, no proactive steps are required for an ISP to avail itself of this immunity (See 17 USC § 512 [a]). This section applies to most student and guest activity on university networks as they are primarily connecting on their own machines. Therefore, the statute does not *technically* establish any legal requirement that institutions respond to, or forward, DMCA notices that correspond to such activity (See Steven J. McDonald, [Face the Music: The Law and Policy of File Sharing](#) (Feb. 21-24, 2009) (PDF), 14). However, for a variety of reasons, including the inability to determine whether a device is personal or university owned when a DMCA notice is received as well as the ability to impart a lesson to students, some colleges have chosen to treat these notices as if they were § 512 (c) notices, terminating users from the network unless and until the infringing content is removed. Many colleges, as a matter of policy, address this kind of activity through a student affairs process, rather than a legal one so as to seize upon a "teachable moment" for students.

FN5. Warren Zevon, [Send Lawyers Guns & Money](#), on *EXCITABLE BOY* (Asylum 1978).

FN6. [Public Law 110-315](#) (2008) (PDF).

FN7. Public Law 89-329 (1965).

FN8. See <http://edocket.access.gpo.gov/2009/pdf/E9-18550.pdf> (PDF).

FN9. See <http://edocket.access.gpo.gov/2009/pdf/E9-25373.pdf> (PDF).

FN10. See Department of Education [General and Non-Loan Programmatic Issues; Proposed Rule](#), 74 Fed. Reg. 42380, 42392 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN11. Dave Matthews Band, [Two Step](#), on *CRASH* (RCA 1996).

FN12. "Section 485(a) (20 U.S.C. 1092 (a)) is amended--

(E) by adding at the end the following:

"(P) institutional policies and sanctions related to copyright infringement, including--

"(i) an annual disclosure that explicitly informs students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the students to civil and criminal liabilities;

"(ii) a summary of the penalties for violation of Federal copyright laws; and

"(iii) a description of the institution's policies with respect to unauthorized peer-to-peer file sharing, including disciplinary actions that are taken against students who engage in unauthorized distribution of copyrighted materials using the institution's information technology system."

FN13. "(29) The institution certifies that the institution--

"(A) has developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents; and

"(B) will, to the extent practicable, offer alternatives to illegal downloading or peer-to-peer distribution of intellectual property, as determined by the institution in consultation with the

chief technology officer or other designated officer of the institution."

FN14. Most notably, the Manager's Report provided some context on the requirement that colleges utilize "technology based deterrents." Further, the statute is intended to be "technology neutral" allowing for a "broad range" of compliance methods. The Report closed by referencing several technological methods including hardware and software packages, automatic processing of DMCA notices, dialing-down bandwidth and packet shaping.

We are reprinting the peer-to-peer section of the Manager's Report in its entirety here:

Section 488. Institutional and Financial Assistance Information for Students.

The Senate amendment and the House bill require institutions to make available to current and prospective students the institution of higher education's policies and sanctions related to copyright infringement, including a description of actions taken by the institution of higher education to detect and prevent the unauthorized distribution of copyrighted materials on the institution of higher education's technology system.

Both the Senate and the House recede with an amendment to replace language in (iv) with language requiring institutions to make available the development of plans to detect and prevent unauthorized distribution of copyrighted material on the institution of higher education's information technology system which shall, to the extent practicable, include offering alternatives to illegal-downloading or peer-to-peer distribution of intellectual property, as determined by the institution of higher education in consultation with the Chief Technology Officer or other designated officer of the institution.

The Conferees have combined elements from both bills to require institutions to advise students about this issue and to certify that all institutions have plans to combat and reduce illegal peer to peer file sharing.

Experience shows that a technology-based deterrent can be an effective element of an overall solution to combat copyright infringement, when used in combination with other internal and external solutions to educate users and enforce institutional policies.

Effective technology-based deterrents are currently available to institutions of higher education through a number of vendors. These approaches may provide an institution with the ability to choose which one best meets its needs, depending on that institution's own unique characteristics, such as cost and scale. These include bandwidth shaping, traffic monitoring to identify the largest bandwidth users, a vigorous program of accepting and responding to Digital Millennium Copyright Act (DMCA) notices, and a variety of commercial products designed to reduce or block illegal file sharing.

Rapid advances in information technology mean that new products and techniques are continually emerging. Technologies that are promising today may be obsolete a year from now and new products that are not even on the drawing board may, at some point in the not too distant future, prove highly effective. The Conferees intend that this Section be interpreted to be technology neutral and not imply that any particular technology measures are favored or required for inclusion in an institution's plans. The Conferees intend for each institution to retain the authority to determine what its particular plans for compliance with this Section will be, including those that prohibit content monitoring. The Conferees recognize that there is a broad range of possibilities that exist for institutions to consider in developing plans for purposes of complying with this Section.

Numerous institutions are utilizing various technology based deterrent in their efforts to

combat copyright infringement on their campuses. According to a report of the Joint Committee of the Higher Education and Entertainment Communities, many institutions of higher education have taken significant steps to deal with the problem. Indiana University, for example, hosts an extensive “Are you legal?” educational campaign for students on the issues, and enforces campus policies on proper use of the network. It acts on DCMA notices by disconnecting students from the network and requires tutorials and quizzes to restore service. Second offenders are blocked immediately and are sent to the Student Ethics Committee for disciplinary action.

Audible Magic’s CopySense Network Appliance provides comprehensive control over Peer-to-Peer (P2P) usage on a university’s network. The CopySense Appliance identifies and blocks illegal sharing of copyrighted files while allowing other legitimate P2P uses to continue. It filters copyrighted P2P content by sensing an electronic fingerprint unique to the content itself, which is very similar to the way virus filters operate.

Red Lambda’s “Integrity” is a network security solution dedicated to the management of file-sharing activities via protocols like P2P, IM, IRC, and FTP. This technology is able to detect all P2P, OS file-sharing, FTP, IM, proxy use, Skype and application tunneling over HTTP, HTTPS, DNS and ICMP protocols.

The University of Maryland, College Park, severely restricts bandwidth for residential networks and block certain protocols. It designed “Project Nethics” to promote the responsible use of information technology through user education and policy enforcement. A third violation can result in eviction from the university housing system. Montgomery College in Maryland enforces an Acceptable Use Policy on its wired and wireless networks.

Additional existing technological approaches can deter illegal file sharing by automatically processing notices sent by scanning vendors then taking actions such as messaging the user via browser redirection, applying the appropriate sanction and automatically re-enable browsing after a timeout or reconnect fee is paid. Other institutions use technology to appropriately manage their campus networks by limiting and/or shaping bandwidth, such as Packeteer’s packet shaping technology.

FN15. Warren G and Nate Dogg, [Regulate](#), on REGULATE...G FUNK ERA (DEF Jam/Death Row/Interscope Records 1994) (note: song is somewhat explicit, but bleeped).

FN16. § 668.43 Institutional information.

(a) Institutional information that the institution must make readily available upon request to enrolled and prospective students under this subpart includes, but is not limited to—

(10) Institutional policies and sanctions related to copyright infringement, including—

(i) A statement that explicitly informs its students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the students to civil and criminal liabilities;

(ii) A summary of the penalties for violation of Federal copyright laws; and

(iii) A description of the institution’s policies with respect to unauthorized peer-to-peer file sharing, including disciplinary actions that are taken against students who engage in illegal downloading or unauthorized distribution of copyrighted materials using the institution’s

information technology system.

FN17. § 668.14 Program participation agreement.

(b) By entering into a program participation agreement, an institution agrees that—

(30) The institution—

(i) Has developed and implemented written plans to effectively combat the unauthorized distribution of copyrighted material by users of the institution's network, without unduly interfering with educational and research use of the network, that include—

(A) The use of one or more technology-based deterrents;

(B) Mechanisms for educating and informing its community about appropriate versus inappropriate use of copyrighted material, including that described in §668.43(a)(10);

(C) Procedures for handling unauthorized distribution of copyrighted material, including disciplinary procedures; and

(D) Procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials by users of the institution's network using relevant assessment criteria. No particular technology measures are favored or required for inclusion in an institution's plans, and each institution retains the authority to determine what its particular plans for compliance with paragraph (b)(30) of this section will be, including those that prohibit content monitoring; and

(ii) Will, in consultation with the chief technology officer or other designated officer of the institution—

(A) Periodically review the legal alternatives for downloading or otherwise acquiring copyrighted material;

(B) Make available the results of the review in paragraph (b)(30)(ii)(A) of this section to its students through a Web site or other means; and

(C) To the extent practicable, offer legal alternatives for downloading or otherwise acquiring copyrighted material, as determined by the institution.

FN18. Bob Dylan, [*The Times, They Are a-Changin'*](#), on THE TIMES, THEY ARE A-CHANGIN' (Columbia 1964).

FN19. Provisions related to peer-to-peer file sharing, for example, only affect schools that provide students with school-maintained and operated internet services; many small institutions lack the resources or need to provide such services and so will not be affected by the provisions. For those that will be affected, the Department is encouraging the adoption of best practices which should reduce institutional burden.

FN20. See 34 CFR § 668.41, 668.43. The proposed regulations reaffirm that such notice "must be made through an appropriate mailing or publication, including direct mailing through the U.S. Postal Service, campus mail or electronic mail. Posting on Internet or Intranet Web sites does not constitute notice. If the institution discloses the consumer information...by posting the information

on a Web site, it must include in the notice the exact electronic address at which the information is posted, and a statement that the institution will provide a paper copy of the information on request." See Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42391 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN21. See "[Dear Colleague Letter](#)," United States Department of Education, (June 4, 2010):

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For "willful" infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq;

See also Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42392 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF): "The Department will work with representatives of copyright holders and institutions to develop a summary of the civil and criminal penalties for violation of Federal copyright laws to include as part of the *Federal Student Aid Handbook* that an institution may use to meet this requirement" (emphasis added).

FN22. A working group made up of attorneys and policy makers from colleges and universities around the country analyzed language planned for use at a number of campuses and have been working on sample language that consolidates some of these versions. The members of that working group are Steve Worona, Director of Policy and Networking Programs at EDUCAUSE; Steve McDonald, General Counsel of the Rhode Island School of Design; Jack Bernard, Assistant General Counsel at the University of Michigan; Tracy Mitrano, Director of IT Policy at Cornell University; Kent Wada, Director, Strategic Information Technology and Privacy Policy at UCLA; Tim McGovern, Manager, IT Security Services,

Client Support Services at MIT; and the two authors of this NACUA Note.

The working group developed two samples, called the short sample and the long sample. These are unofficial samples, not endorsed by any official higher education organization, and are meant to supplement and provide options to the sample version published in the Federal Financial Aid Handbook:

Short Sample:

The unauthorized distribution of copyrighted material, including through peer-to-peer file sharing, may subject a student to criminal and civil penalties. The laws that govern copyright are not specific to any one technology. Students can violate the rights of a copyright holder using many different types of technology. Both uploading and downloading of files can pose a violation of the copyright law. Students should be cautious when obtaining any copyrighted material. As a rule of thumb, before a student receives anything for free, they should research whether that source provides material licensed by the copyright owner. [College] offers a list of licensed sources at [LINK].

Individuals who violate copyright law by illegally uploading and downloading copyrighted files may be subject to civil penalties of between \$750 and \$150,000 per song. These penalties are established by federal law. In the past, pre-litigation settlements offered by copyright owners have ranged from \$3,000 to \$4,000 and up while juries have issued verdicts of hundreds of thousands and even millions of dollars. In addition, a court may, in its discretion, grant the copyright owner reasonable attorney fees. Although criminal prosecution of students for file sharing is extremely rare, federal law lays out criminal penalties for intentional copyright infringement which can include fines and jail time.

In addition to potentially violating the law, unauthorized distribution or receipt of copyrighted material is a violation of the College's acceptable use policy. That policy states that [FILL IN POLICY PARAGRAPH]

Long Sample:

Before you share, beware! The unauthorized distribution of copyrighted material, including through peer-to-peer file sharing, may subject you to criminal and civil penalties. Although using peer-to-peer file sharing technology in itself is not illegal, *what* you share and *how* you share it may violate the law (just as while driving a car is legal, driving a car on the sidewalk at 90 miles per hour is not). The laws that govern copyright are not specific to any one technology; you can violate the rights of a copyright holder using many different types of technology. Both uploading and downloading of files can pose a violation of the copyright law, and the law applies for songs, videos, games, textbooks, and any other type of creative content.

Use technology wisely. You are responsible for the choices you make and should be cautious when obtaining any copyrighted material. As a rule of thumb, before you download anything for free, you should research whether that source provides material licensed by the copyright owner. [College] offers a list of licensed sources at [LINK].

Individuals who violate the copyright law, even unintentionally, by illegally uploading or downloading may be subject to civil penalties of between \$750 and \$150,000 per song! For those who download or upload dozens or hundreds of songs, penalties could reach into the millions of dollars. These penalties are established by federal law.

Content owners actively monitor file sharing networks and issue takedown notice to Internet Service Providers (including our college) requesting that the college remove these files or subpoenas requesting that the college turn over your contact information for the purpose of filing a lawsuit. Pursuant to State and Federal law, the college must comply with all valid subpoenas.

In the past, pre-litigation settlements offered by copyright owners prior to filing lawsuits against students have ranged from \$3,000 to \$4,000 and up while juries have issued verdicts against illegal file sharers of hundreds of thousands and even millions of dollars. In addition, a court may, in its discretion, grant the copyright owner reasonable attorney fees. Although criminal prosecution of students for file sharing is extremely rare, federal law lays out criminal penalties for

intentional copyright infringement which can include fines and jail time.

While it is generally accepted in copyright law that you may format-shift content, that is, you may rip a CD onto your computer and then listen to it on your iPod, that only applies for your own personal use. You may not then distribute that song file to others. To do so, is to violate the copyright law as is to download a file shared in this manner.

In addition to following the law, you must also follow college policy. Unauthorized distribution or receipt of copyrighted material is a violation of the College's acceptable use policy. That policy states that [FILL IN POLICY PARAGRAPH].

Cornell University Sample:

Welcome back, students! A couple of quick messages about important issues related to use of the Internet on the Cornell network.

As almost everyone knows, distributing copyright protected materials such as music, videos, software and electronic games without permission, is a potential violation of copyright law. Copyright violations can lead to both criminal and civil legal actions and penalties can run from \$750 to \$150,000 per infringement! Very large volume infringements have, in some rare circumstances, resulted in criminal investigations and prosecutions that included sentencing.

Content owners, such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), as well as network television such as Home Box Office (HBO), deploy detection services targeted to higher education networks such as Cornell. In the past, the RIAA in particular has sued students for copyright infringement, with settlements costing students and their families thousands of dollars. While Cornell has long objected to the targeting of higher education networks, and will not as a matter of policy monitor its network for content (as some schools do), we are both obligated by law to inform you of these kind of issues and want to let you know that special risks exist regarding the practice of file-sharing copyright protected materials on our network. If you are interested in more information about copyright law and contemporary issues, the IT Policy Office sponsors a free, optional tutorial available here:
<http://www.ecornell.com/cu-digital-copyright-education/>

Cornell does not sponsor an internal hosted music service, but we do maintain a web page that provides you with alternative legal media services available on the Internet.
<http://www.cit.cornell.edu/policies/copyright/music.cfm> A group of sites devoted to information about copyright law, peer-to-peer file sharing technology and the consequences of receiving Digital Millennium Copyright, or "take-down," notices, while using the Cornell network may be found here:
<http://www.cit.cornell.edu/policies/copyright/index.cfm> If you are unfamiliar with how peer-to-peer technology works and the implications of running such a program on the device you register to the Cornell network, please read through this material and feel free to call me with any legal or policy questions or the HelpDesk for technical advice.

Finally, The IT Policy Office has created an open and free Digital Literacy Program newly available this year. Focused on academic work and undergraduate research, this program offers information about copyright, plagiarism and privacy. <http://digitalliteracy.cornell.edu/> We hope that it will help you avoid some of the most obvious pitfalls of using information technologies in academic work and enhances your student experience at Cornell.

Good luck this year in your life and studies!

Tracy Mitrano tbm3@cornell.edu

Director of Information Technology Policy
<http://www.cit.cornell.edu/policies/>

Rhode Island School of Design Sample:

Over the past year, the recording, motion picture, and software industries have become increasingly aggressive in their campaign against peer-to-peer file sharing. The Recording Industry Association of America has filed lawsuits against some 26,000 alleged file sharers to date and is now targeting college students specifically. The Motion Picture Association of America has sued many thousands more – including at least one RISD student who allegedly had shared a single copy of a single movie. The Entertainment Software Association recently began a similar campaign of its own.

Most of these lawsuits are being settled, typically for payments in the range of \$3,000 to \$5,000 each, but the potential liability is significantly greater. Earlier this month, in the first of these lawsuits to go to trial, the RIAA won a judgment of \$222,000 against a woman who allegedly had shared just 24 songs – an astounding \$9,250 per song. And, arguably, even that was a “bargain.” Under applicable law, the amount of damages that can be awarded against an infringer can run as high as \$150,000 for each work infringed, and, in some circumstances, there can be criminal penalties as well.

The RIAA, MPAA, and ESA determine whom to sue by actively monitoring file-sharing networks and then issuing subpoenas to ISPs for the identities of the file sharers they find. RISD has not yet received such a subpoena, but it has received a number of infringement notices, which often are precursors to subpoenas and lawsuits, and would have no choice but to comply were it to receive one.

These tactics may seem misguided and heavy-handed, but the RIAA, MPAA, and ESA are correct that most file sharing constitutes copyright infringement. While it generally is accepted that “space-shifting” – ripping an MP3 from a CD you already own for your own personal use on your own computer or MP3 player – is “fair use,” the courts have held that it is not legal to then share that MP3 indiscriminately over the Internet. The technology may make it easy for you to do so, you may not be charging anything, you may be “publicizing” the artist in the process, and the music, movie, and software industries’ business practices may themselves be worthy of debate, but none of those justifications is a viable defense to a copyright infringement suit under current law.

At an institution devoted to the creation of art, we should be especially mindful of these issues. Artists’ and designers’ livelihoods are dependent in large part on the creation of, and the respect of others for, intellectual property. Just as you wish to protect the economic value of your own copyrights, so, too, do the musicians, filmmakers, and other fellow artists whose work is being traded over the Internet without appropriate compensation.

In addition, illegal file sharing is also a violation of RISD’s computer use policy. While RISD does not actively monitor its networks, it will respond to violations that come to its attention, and repeat infringers will be deprived of further network access.

Additional information about these issues can be found at the following:

NBC Universal Sample:

Additionally, David Green, Vice President for Public Policy Development at NBC Universal, has sent the following language as a potential sample to EDUCAUSE:

"Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or ³statutory² damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For ³willful² infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense."

FN23. See [Department of Education General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42393 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN24. EDUCAUSE maintains a page of ["role model"](#) campuses from which policy ideas and language may be researched.

FN25. For further explanation of the balance between network security and network function considered by the Department of Education, see Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42392 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN26. See Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42392 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

We are reprinting this brief discussion in its entirety here:

"Although there was some discussion of requiring an institution to effectively combat the unauthorized distribution of copyrighted material by only student users of the institution's network, the regulatory language on which tentative agreement was reached would apply the requirement more broadly to "users." This approach ensures that institutions will be more likely to deter and prevent downloads of copyrighted material by employees and members of the public that may use computers at a school library, for example, and also allow them to identify illegal downloads being made by students who are not accessing the computer systems using their student accounts. The Department believes that this approach meets the intent of the statute that institutions secure their networks from misuse by individuals who are given access to the networks."

FN27. See Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42391 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF). The final regulations did not further address this issue.

FN28. See <http://traindoc.cit.cornell.edu/copyright/vidPlayer480.html>.

FN29. See <http://bayu.umich.edu>.

FN30. See Policy at Stanford University on [Residential Computing](#).

FN31. It should be noted that, in the experience of the authors, the strongest discipline systems are those in which technology professionals and student affairs professionals work together to create meaningful educational lessons for students accused of illegal file sharing. Each party brings to the table an independent skill; the IT professional can explain in summary or detail exactly what the student is accused of while the student affairs professional brings experience in appropriate and effective disciplinary and educational methods. It is the team approach that has the best chance of effectively educating students.

FN32. While the proposed regulations cited the diversity of higher educational institutions and stated that it would thus be up to the institution itself to determine "how many and what type of technology-based deterrents it uses as a part of its plan...every institution must employ at least one." See Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42392 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN33. See Department of Education [General and Non-Loan Programmatic Issues](#); Final Rule, 74 Fed. Reg. 55902, 55926 (Oct. 29, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

FN34. See Paul Cesarini, [Of Gladiators, and Bandwidth Realities](#), EDUCAUSE REVIEW, VOL. 42, NO. 4, July-Aug. 2007.

FN35. Privacy concerns are often raised in content filtering discussions since, by their nature, they are examining all network traffic. See Kent Wada, [Illegal File Sharing 101](#), EDUCAUSE QUARTERLY, Vol. 31, no. 4, Oct.-Dec. 2008. In addition, their efficacy is questionable. See Andy Guess, [Can Anyone Police File Sharing](#), INSIDE HIGHER ED, Aug. 3, 2007.

FN36. See <http://movielabs.com/ACNS/>.

FN37. See Kent Wada, [Illegal File Sharing 101](#), EDUCAUSE QUARTERLY, Vol. 31, No. 4, Oct.-Dec. 2008.

FN38. The list, which is updated regularly by EDUCAUSE staff, may be accessed and linked to here: <http://www.educause.edu/Resources/Browse/LegalDownloading/33381>.

FN39. See Department of Education [General and Non-Loan Programmatic Issues](#); Final Rule, 74 Fed. Reg. 55902, 55910 (Oct. 29, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

We are reprinting this brief discussion in its entirety here:

"We do not believe that simply not blocking legal alternatives for downloading or otherwise acquiring copyrighted material qualifies as "offering" legal alternatives. The requirements of Sec. 668.14(b)(30)(ii)(A) and (B), that an institution must periodically review the legal alternatives and make available the results of the review to its students through a Web site or other means, support the notion that an institution's actions in this area must be active, rather than passive. We note, however, that an institution must offer such legal alternatives "to the extent practicable." Thus, how or whether the institution offers such alternatives is controlled by the extent to which it is practicable for the institution to do so. As stated in the preamble to the NPRM (74 FR 42393), the Department anticipates that individual institutions, national associations, and commercial entities will develop and maintain up-to-date lists of legal alternatives to illegal downloading that may be referenced for compliance with this provision. The requirement that, as a part of an institution's plans for combating the unauthorized distribution of copyrighted material, the institution must include the use of one or

more technology-based deterrents is statutory (see section 485(a)(1)(P) of the HEA) and we do not have the authority to remove this requirement. Moreover, we believe that the requirement that an institution's plans include procedures for periodically reviewing the effectiveness of the institution's plans for combating the unauthorized distribution of copyrighted material is essential for institutions to comply with the requirements in section 485(a)(1)(P) and 487(a)(29) of the HEA."

FN40. Id.

FN41. See e.g. <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/07/AR2009020700684.html>.

FN42. Examples include Choruss and a program of the Berkman Center at Harvard University, see e.g. [EDUCAUSE Live segment from March 3, 2009](#). See also, [Choruss Music Project Changes Plans Again, Spins Off From Warner](#), CHRONICLE OF HIGHER EDUCATION, WIRED CAMPUS BLOG.

FN43. Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42391 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF). The final regulations did not further address this issue.

FN44. See Department of Education [General and Non-Loan Programmatic Issues](#); Proposed Rule, 74 Fed. Reg. 42380, 42393 (Aug. 21, 2009) (to be codified at 34 CFR Parts 600, 668, 675 et al.) (PDF).

We are reprinting this brief discussion in its entirety here:

"As the specifics of a plan will be determined by an institution, the Department believes that the institution is in the best position to determine the appropriate criteria to assess its plan. In some cases, appropriate assessment criteria might be process-based, so long as the institution's information system information does not contradict such a determination. Such process-based criteria might look at whether the institution is following best practices, as laid out in guidance worked out between copyright owners and institutions or as developed by similarly situated institutions that have devised effective methods to combat the unauthorized distribution of copyrighted material. In other cases, assessment criteria might be outcomebased. The criteria might look at whether there are reliable indications that a particular institution's plans are effective in combating the unauthorized distribution of copyrighted material. Among such indications may be "before and after" comparisons of bandwidth used for peer-to-peer applications, low recidivism rates, and reductions (either in absolute or in relative numbers) in the number of legitimate electronic infringement notices received from rights holders. The institution is expected to use the assessment criteria it determines are relevant to evaluate how effective its plans are in combating the unauthorized distribution of copyrighted materials by users of the institution's networks."

FN45. Dr. Dre and Snoop Dogg, [The Next Episode](#) (Aftermath/Interscope 1999) (somewhat explicit, but bleeped).

FN46. The RIAA maintains a blog on the vagaries of illegal downloading and their negative effect on business, see http://www.riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law. The Association, along with other content suppliers, have long predicted that file sharing will result in their ultimate demise. Four months after the September 11, 2001 attacks, Jack Valenti, the late President of the MPAA, compared the fight against file sharing to a terrorist war, see Amy Harmon, [Black Hawk Download: Pirated Videos Thrive Online](#), NEW YORK TIMES, Jan. 17, 2002. This is the same MPAA leader who said of the VCR that it was "to the American film producer and the American public as the Boston strangler is to the woman home alone." See Home Recording of Copyrighted Works: Hearing on H.R. 4783, H.R. 4794, H.R. 4808, H.R. 5250, H.R. 5488, and H.R.

5705 Before the Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary, 97th Cong. 8 (1982); David Fagundes, *Property Rhetoric and the Public Domain*, 94 MINNESOTA L.R. 652, 664, f.n. 58 (2010).

FN47. For example, a [2008 Tennessee state law](#) governed file sharing at public colleges and universities.

FN48. Semisonic, [Closing Time](#), on FEELING STRANGELY FINE (MCA 1998).

FN49. Recall that, just as with a car or a handgun, the technology may be useful, although certain uses of that technology certainly are illegal.

FN50. For an ironically *pirated* image of the first warning screen of a DVD, [see http://www.filmschoolrejects.com/images/fbiwtf_wide.jpg](http://www.filmschoolrejects.com/images/fbiwtf_wide.jpg). Note that the text of the warning is not available anywhere on the Internet, and unauthorized use of the logo which prohibits unauthorized use of content *is itself* prosecutable under Federal law. [See http://www.fbi.gov/ipr/](http://www.fbi.gov/ipr/).

AUTHORS:

[Joseph Storch, Assistant Counsel, State University of New York Office of University Counsel.](#)

[Heidi Wachs, Director of IT Policy, Privacy Officer, and DMCA Agent, Georgetown University.](#)

RESOURCES:

NACUA Resources:

- [NACUA Page on Copyright: P2P Resources and Links](#)

Additional Resources:

- [EDUCAUSE Page on Complying with peer-to-peer requirements of the Higher Education Opportunity Act](#)
- [EDUCAUSE Page on Peer to Peer File Sharing](#)
- [Recording Industry Association of America Page on Campus Downloading](#)
- [Recording Industry Association of America and Allied Organizations Page on File Sharing](#)
- [Motion Picture Association of America Page on Copyright Information](#)
- [Electronic Frontier Foundation Information on File Sharing](#)

[NACUANOTES Homepage](#) | [NACUANOTES Issues](#)
[Contact Us](#) | [NACUA Home Page](#)

"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."