Illegal File Sharing 101

Higher education needs to reassess its response to illegal file sharing in the face of a shifting legislative landscape and evolving technology and business models

By **Kent Wada**

Happy 10th birthday to the Digital Millennium Copyright Act! The DMCA was enacted in 1998 to update U.S. copyright law for the digital age and encouraging innovation to flourish. At the time, no one guessed how intimate colleges and universities would become with its provisions. Only a year later, (the original) Napster was quietly unleashed on the world, dramatically impacting both the entertainment economy and higher education's role as network service provider and leading to ever-rising tension between the two communities.

Much of higher education's unease arises from the cost of dealing with illegal file sharing.[1] Illinois State University, for example, calculated a cost of $76 to process a first claim of copyright infringement and $146 for a second.[2] Responses range from simply passing along claims to elaborate programs architected with specific goals in mind. Higher education encompasses thousands of individual and individualistic institutions, each in a context of local cultural values, resources, and state laws. There is no single "right" approach to this complicated, multifaceted, nationally important, shared problem, yet we can draw from our collective experience for good ideas.

This article aims to impart information and raise issues that will help you think through what will best achieve your institution's goals—from student conduct to legal liability, from technology to digital entertainment services—in an era of digital downloading. Not

everything will apply to your institution, of course. But the 10th anniversary of the DMCA is an apropos moment to (re)assess what you do.

The DMCA: A Massively Abbreviated Primer

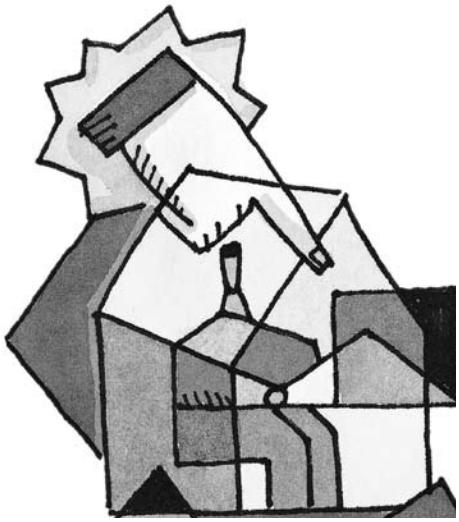
The usual disclaimer applies: this article is not in any way a substitute for proper legal advice. An excellent summary by the U.S. Copyright Office is available on its website.[3]

The DMCA reflects the digital context in several significant ways. Relevant to illegal file sharing, however, and what we mean when referring to the DMCA, is Title II, the "Online Copyright Infringement Liability Limitation Act," which is now Section 512 of the U.S. Copyright Act. As well, the recently reauthorized Higher Education Act (HEA) includes language that effectively modifies the DCMA framework for higher education.

Balancing Opposing Needs

Section 512 articulates a framework that recognizes that rights holders often cannot directly identify digital infringers of their works; only an online service provider (OSP) can map an IP address to an individual. (Colleges and universities are considered OSPs for their communities.) The framework represents a balance—a compromise—between the needs of copyright holders, who want to meaningfully enforce their rights by stopping alleged infringement as quickly as possible in a digital world where every second can see countless perfect copies created and distributed, and the desire of OSPs to be sheltered from liability for contributory copyright infringement due to the illegal acts of their customers. (Consider an analogy where two people used the telephone to plan a bank robbery: The phone company would not be considered responsible for their malfeasance.)

To achieve this balance, the DMCA allocates to rights holders the responsibility of identifying infringement of their works and making claims following specific conventions to the relevant OSP. Section 512 gives OSPs four optional and conditional means of



complying with such claims in return for a limitation of liability.[4] If one or more of these four liability limitation provisions applies to your institution, it enters a "safe harbor" that protects it from liability for subscribers' actions.

So when do these provisions apply to an educational institution? Two are relevant to illegal file sharing:

- §512(a), Transitory Digital Network Communications, where an institution acts as a conduit of network traffic—what we typically think of as an Internet service provider (ISP). Residence halls generally fall into this category, where the institution provides the network connectivity but does not own the end-user equipment (students own their computers).
- §512(c), Information Residing on Systems or Networks at Direction of Users, where systems owned by the institution (systems over which the institution has control, such as a web server or employee's institutionally owned desktop computer) are involved.

Qualifying for §512(a) essentially requires that the institution act as an ISP, moving data around for users and nothing more:

> …an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[5]

The institution must also adopt and reasonably implement a policy of terminating—in the appropriate circumstances—the accounts of subscribers who are repeat infringers. Such policies differ across institutions. Often the policy suspends a student's in-room network access while still allowing access from other campus areas. Unlike termination of a user's account (including e-mail) with a commercial ISP, where an individual could simply go to another ISP, such termination at a college or university would probably mean the student could no longer pursue his or her studies. Thus such policies need to be treated as an institutional rather than a computer-use issue.

Qualifying for the safe harbor of §512(c) sets a higher bar, as the systems involved are those over which the institution has direct control. To meet this standard, a Designated Agent to receive claims of copyright infringement must be on file with the Copyright Office and advertised prominently by the institution; the institution cannot receive a financial benefit directly attributable to the infringing activity; and the institution cannot have actual knowledge of infringement. When properly notified, the institution must act expeditiously to take down or block access to the material (or to restore access if a counter-notification is made). The same requirement exists as in §512(a) for a policy on repeat infringers, along with several other requirements.

Keep in mind that these safe harbors are entirely optional. They are additional means by which an institution can minimize legal risk, but traditional defenses such as fair use remain available.[6] Institutions will want to avail themselves of all possible defenses.

Policy Implications of the DMCA

Steven McDonald, a noted authority on the DMCA in higher education, has argued that colleges and universities often misunderstand these provisions, assuming that residence hall networks

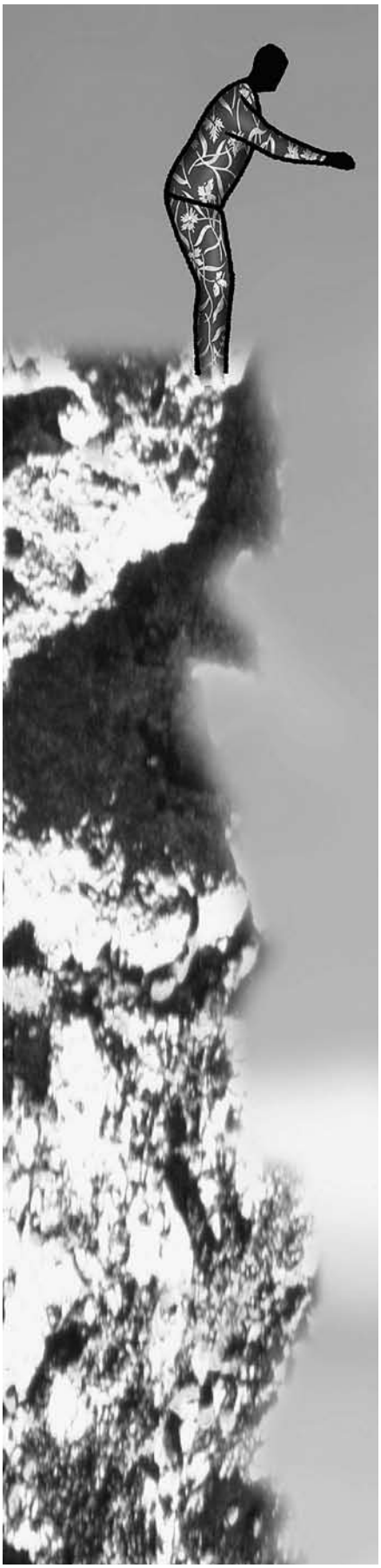
fall under §512(c) instead of §512(a).[7] In reality, §512(a) applies and effectively means that an institution's safe harbor would be maintained even if infringement claims received for residence hall networks were ignored—a view some commercial ISPs have taken for their networks (though that may be changing). Thus any institutional effort, such as education programs, that go beyond the basics to qualify for §512(a) is an institutional policy choice, not a legal requirement.

That said, many institutions comply with the higher standard required to qualify for §512(c) protection even for their residence hall networks because it demonstrates commitment to the value of intellectual property and promotes community ethical standards. Such institutions have a Designated Agent on file, act expeditiously when a claim is received, and so forth. And despite significant agreement on the applicability of §512(a) to residence hall networks, the issue has not yet been tested in the courts. Higher education attorneys would not like their institutions to be the test case. Then there's the Higher Education Act.

The Higher Education Act

What would the DMCA look like had it been written after the implications of Napster were understood? We may be getting a glimpse through language in the reauthorization of the HEA that would require colleges and universities to take specific measures to combat digital piracy or risk fines and being cut off from federal student aid funds. (Two states have already adopted their own requirements.) These new requirements in some sense amend the DMCA framework for higher education: while the safe harbors still apply, there is now a different set of requirements with a different set of penalties for noncompliance.

These new requirements include proactive disclosures, fostering awareness of policies and law among students, and a certification by each institution (that is, someone will have to sign on the dotted line so certifying) that it has developed plans to effectively combat unauthorized distribution of copyrighted material on its network (with technology-based deterrents and legal entertainment offerings).



Much debate covered the requirements and wording,[8] but exactly how these legislative mandates will translate into operational reality has yet to be determined through a negotiated rulemaking process led by the U.S. Department of Education. This process began in the fall and is expected to continue through the fall of 2009, with regulations likely to go into effect July 2010. Be mindful, however, that the law is already in effect and that institutions are expected to make a good-faith effort in complying with it even absent the results of the rulemaking.

This rulemaking can be as important as the crafting of the legislation itself, and if you can be involved in the process, you should.[9]

Institutional Goals

What goals are most important to your institution? (Hint: You can't say "all." Try two or three.)

- Minimizing workload generated by the receipt and processing of DMCA claims of infringement and/or Recording Industry Association of America (RIAA) settlement letters.
- Minimizing network bandwidth consumed by illegal file sharing.
- Minimizing the institution's legal risk.
- Raising awareness of law, policy, and alternatives among your students to change behavior.
- Ensuring due process in student-conduct judicial proceedings.
- Protecting, to the extent possible, your students from or during legal action.
- Protecting institutional reputation.
- Taking a stand against the tactics of the entertainment industry to combat digital piracy (as distinguished from their assertion of copyright).
- Advocating for higher education's approach and interests at the federal or state level.
- Protecting privacy and academic freedom.

- Educating your students in copyright and intellectual property issues and in ethical behavior.
- Helping shape the national policy discussion about copyright in today's digital world.

These goals are roughly ordered from the operational to the conceptual and aren't directly comparable; some are incompatible. For example, if the institution's reputation is paramount, a ban on peer-to-peer (P2P) traffic is a possibility. Such a ban automatically addresses workload, bandwidth, and legal risk but also potentially encroaches on privacy and academic freedom. Outsourcing the residence hall network could make the entire issue someone else's problem (at least from an operational perspective).

Most institutions will establish a balanced combination of goals. In the ideal case, you could invest resources to address the immediacy of the illegal file sharing problem while simultaneously engaging in some activity that takes a more holistic, longer-term view of the copyright debate, whether by education of students or advocacy at a national level. This reflects the fact the DMCA speaks to rights holders and OSPs but not infringers (the students), whereas our institutions also want to address student behavior.

An Institutional Program to Curb Illegal File Sharing

Illegal file sharing occurs on campuses. What is a reasonable response by an institution? The following five areas suggest a framework for the purpose.

Institutional Policies

Most institutions have a statement about engaging in illegal file sharing or copyright infringement embedded in institutional policy, whether a network acceptable use policy or the student code of conduct. Having such a statement is a necessity, and the HEA essentially requires that your students be made aware of such policies.

Anecdotally, at the Joint Committee of the Higher Education and Entertainment Communities Technology Task Force workshop in May 2008, David Hughes, RIAA senior vice president for technology, extemporaneously listed critical factors he had observed at institutions that were, from his viewpoint, successfully combating illegal file sharing:

- Create a clear and unambiguous acceptable use policy.
- Ensure all users are made aware of the policy.
- Strictly and consistently enforce the policy.
- Implement a graduated response supported by available technology.
- Ensure that policy enforcement results in tangible consequences.

Student Awareness

Campuses already provide information to students about policies and law using myriad communication vehicles: official letters to the student body, orientation sessions for incoming freshmen, parents' orientation sessions (aimed at those who may end up paying multi-thousand-dollar settlements), presentations to student groups, flyers, ads, articles, websites, and student government. These take time to develop, and a certain amount of local branding is needed. But why reinvent the wheel? There is already effective creative material out there that takes advantage of time-tested marketing and psychological tools. If those materials can be adapted with minimal effort, every institution can benefit. This is even more important now that the HEA requires disclosures about law, policies, and sanctions to students.

Nevertheless, awareness campaigns tend to be general and one-time (that is, annual) and therefore disconnected from actual occurrences of illegal file sharing. The University of Michigan developed "Be Aware You're Uploading" (BAYU) as a different approach. This service quickly notifies users when their computers are uploading using P2P technology; no content is examined to determine whether the upload is appropriate or inappropriate, and receiving a notice implies no judgment. The goals are entirely educational, but the notification gives a sense of immediacy.

A note of caution in crafting messages to students: P2P is constantly juxtaposed with danger and illegality, but the issue is more nuanced:

- Downloading ≠ bad. We download all the time, whether shareware or in the act of visiting a web page.
- Sharing ≠ bad. As Sir Isaac Newton said, "If I have been able to see farther than others, it is because I stood on the shoulders of giants."
- P2P ≠ bad. The technology is inherently neutral; it's the specific use that makes the difference.

Student Judicial Process and Teachable Moments

Many campuses have instituted an escalated response model to handling claims of infringement. A first strike might require a student to click on an agreement about future behavior. A second or third strike could require the student to talk to a campus official, whether from the IT department or the office of the dean of students. Implicit in any of these responses is the teachable moment: holding students accountable for their actions, but giving them an opportunity, at each step, to change their behavior.

Typically, network-related penalties are employed. An accused student's computer will have its connectivity disabled (sometimes still permitting access to the institution's resources for academic purposes) for a certain period of time (ranging from minutes to days to permanently) when an infringement claim is received. Subsequent claims for the same student would result in longer and longer disconnection times. Stanford University charges a reconnection fee ($100, $500, and $1,000) meant to deter illegal file sharing and defray the costs of processing claims. The University of Florida uses technology to block P2P traffic entirely in its residence halls, though exceptions can be made for legitimate academic purposes.

Many opportunities arise for teachable moments. For example, a student identified in a DMCA claim could be required

to take a quiz,[10] write an essay, watch a video,[11] or have their computer checked to ensure no P2P software is installed.[12] Properly approached, the intense, interactive nature of mandatory group discussions for students who received a first claim and interviews with the dean of students for subsequent alleged offenses can produce remarkable results.

Dean of Students and the Student Life Approach. A student life approach to curbing illegal file sharing implies that alleged copyright violations be considered violations of your student code of conduct rather than of your network's acceptable use policy. (Of course, any sanction by the dean of students could also include a network component.) Foremost among the benefits of this approach is that sanctions are in the context of all student conduct matters. This means two things: punishments are relative to punishments for all the other types of student misbehavior, whether academic dishonesty or alcohol abuse; and this activity may be seen as part of an overall pattern of behavior indicating a troubled individual needing help.

Another benefit of sanctions (observed at UCLA) is that students are often more concerned about a black mark on their academic record than about having to pay $3,000 in settlement fees. Difficult as the latter may be, the former could prevent aspiring doctors and lawyers from entering those professions. Foreign students have an even greater concern, as a change in their academic status will be reported to the federal government, potentially triggering loss of student status and all that entails.

If you believe that part of the educational mission is to help prepare students for life beyond university walls as ethical and informed citizens, involvement by student affairs is crucial. The teachable moments aren't just about illegal file sharing or copyright, but about being good citizens; they're not just about punishment, but about guidance.

Implications of Infringement Detection Methodologies. In May 2008, the RIAA clarified and reiterated its methodology for detecting infringement and the basis for sending claims of infringement.[13] Because claims are based on detecting the presence of content being made available rather than actual transmission of the content, there are important ramifications.

First, courts have not yet converged on whether "making available" content constitutes infringement.[14] (This is not the only question yet to be settled legally.) If claims of infringement are based on the "making available" theory but it turns out that making available does not constitute infringement, how will that affect your student conduct decisions?

Second, content filtering technologies that look for actual transmission of content are not designed to look for the presence of content being made available. As a result, RIAA infringement detection programs might find alleged infringement while technology deployed in-house might not.

Third, other rights holders use differing detection methodologies requiring consideration of different issues. Rapid developments are occurring in this arena—check back often.

Legal Options for Digital Entertainment Services

How times have changed! Only a year ago, a handful of legal options for digital entertainment that could be offered by colleges and universities were largely ignored by students. Today, the digital entertainment marketplace is full of exciting experimental models.[15] Did you know that all 13 seasons of *South Park* are available online, legally and for free? Search portals such as hulu.com provide access to a large collection of television shows, movies, and clips, sometimes in high definition; modernfeed.com, in addition to being a neutral aggregator, offers access through devices such as the iPhone and iPod Touch; and Illinois State University's BirdTrax (http://www.birdtrax.ilstu.edu) points to music also. Amazon.com and Rhapsody offer music in MP3 format—free of digital rights management and thus untethered from the iPod—often for less than what iTunes charges. Nokia is bundling music access with cell phones, and Universal Music Group is looking to extend this model to other devices—something potentially of interest to students who balk at paying 99¢ for a song but think nothing of paying twice that to change the ringtone on their cell phone. The rapid change in this space makes it important to move carefully—the intent of the HEA requirements indicate that a variety of options would be acceptable.

This rapid evolution can sow confusion among students. For example, why is it okay to download a certain TV show from one site but not another, or through this technology but not that one? (It's the height of frustration to see an infringement claim for material that is legally available for free.) And what about sites that intentionally obfuscate the legality of access they offer to unlimited content for a monthly fee? Those are a complete scam. Information literacy may be the only solution.

Technology

The HEA requires higher education institutions to certify that they have "developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents." Such deterrents can include a range of possibilities, such as "bandwidth shaping, traffic monitoring to identify the largest bandwidth users, a vigorous program of accepting and responding to DMCA notices, and a variety of commercial products designed to reduce or block illegal file sharing."[16] Higher education institutions already employ many of these techniques, including UM's BAYU. Technology is an important component of any program to combat illegal file sharing.

Commercial products have been employed by some institutions with varying results. How effective are these products in detecting or prohibiting illegal file sharing? How costly are they to implement (vis-à-vis the workload costs they lower as claims theoretically go down)? What policy implications do they have?

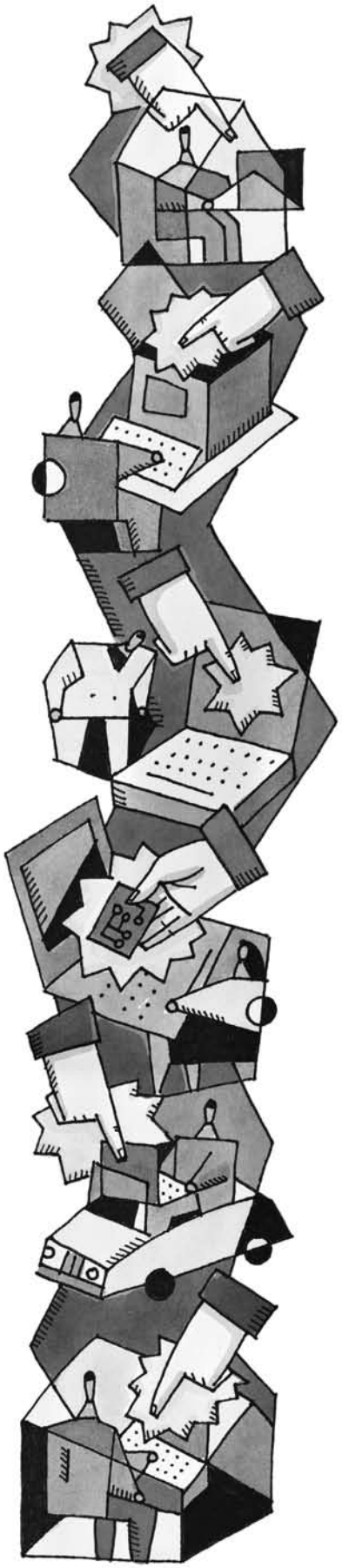
The Digital Citizen Project will have published results of numerous evaluations of commercial technologies. More

generally, a number of concerns with such technologies was articulated in a letter to education leaders in the House and Senate in April 2008 by the Association for Computing Machinery. These concerns include known technical counters; security risks; the undermining of freedoms, rights, and research; false positives; and costs.[17]

Infringement-curbing technologies raise a policy concern. Safeguarding privacy is fundamental to avoiding a chill on academic freedom—the right to inquire, the right to learn, the right to teach, freely and without intimidation. Technologies that monitor content over an institution's network to identify or prohibit P2P sharing of copyrighted material can violate this privacy. It's important to distinguish the real concern: not content monitoring per se (after all, antivirus software does this), but crossing the threshold from the routine, automated inspection of traffic into surveillance, or the monitoring of behavior. Second, the DMCA assigns responsibility for finding infringement to rights holders. How this assignment of responsibility interacts with the new requirements in the HEA is unclear.

Technology can also aid in automating handling of DMCA claims. The Automated Copyright Notice System (ACNS)[18] developed by Universal Studios and Universal Music in 2003 provides a general framework for efficiently handling DMCA claims. An underlying XML schema defines a standard format for structuring information in a DMCA claim so that claims become consistently machine-readable. (For those of you who process claims for your institution, it's the part at the bottom of, or attached to, each notice enclosed between "tags" that look like <Infringement> and </Infringement>.) UCLA's quarantine system and those of some other institutions employ the design principles of ACNS. At the May 2008 Technology Task Force workshop, one outcome was an agreement to review the schema and update it based on the experience gained since its original definition.

Finally, some interesting opportunities arise from new products and



services. One is *redirection*. What if, when searching for a certain song or video, alongside regular search results (which may point to illegal copies) were legal alternatives? Making the service opt-in sidesteps privacy issues, and many people are willing to give up some privacy when they perceive a benefit in return. Enabling technologies can work hand-in-hand with gatekeeper technologies to deter illegal file sharing.

Assessing Your Program

What does it mean to succeed? That illegal activity decreases, of course, but also that the institution has effectively educated students and changed their behavior over the longer term.

The only metric in common use at present is the raw number of DMCA claims received by an institution. To higher education, this number is a mistrusted and opaque proxy for measuring prevalence of illegal activity, with little correlation to institutional effort. For example, a spike in claims issued by the RIAA in May 2008 resulted from enhancing the effectiveness of the detection technology used, even though nothing had changed on campuses.[19]

A good metric would not be easy to design and would depend on transparency and trust between higher education and other rights holders. Another outcome of the May 2008 Technology Task Force workshop was an agreement to look at better metrics. By the time this article is published, progress may have been made.

UCLA uses *recidivism*—individuals who receive a second or subsequent claim—as a measure of its effectiveness at changing students' behavior. A second claim raises the question "What part of this didn't you understand the first time?" The varied and often insightful answers help guide the campus's program. Based on such input, in October 2007 UCLA began holding mandatory workshops for first-time claim recipients. This group workshop, led by the Dean of Students Office, is an intense, interactive experience. Following its introduction, the recidivism rate has dropped to zero.

RIAA Early Settlement Letters and Lawsuits

For some time, the RIAA has sued students for copyright infringement. More recently, it began offering individuals the option to settle out of court; if the settlement offer isn't accepted, a lawsuit follows. These early settlement letters—distinct from infringement claims—hold several implications for colleges and universities.

Foremost is an institutional policy decision. As with DMCA claims, the RIAA depends on the ISP to identify the individual it wants to offer a settlement and to pass the offer along. Will your institution do so? There is no legal requirement—these offers operate outside the framework of the DMCA. Many institutions forward such offers so that their students have all options available to them, despite the costs to the institution and the risk of being perceived as part of the RIAA's initiative. Some institutions, such as the University of Wisconsin–Madison, have decided not to forward these settlement offers. Another decision is whether receipt of a request to pass along an early settlement letter triggers the student conduct judicial process, or is seen entirely as a private matter between two external parties.

Institutions also have to deal with two related legal requirements. First, the RIAA typically sends a preservation notice to the institution at or about the same time as it makes a request to forward an early settlement offer. The preservation notice directs the institution to maintain records relevant to the alleged infringement (log file entries that map an IP address to an individual[20]). If the student does not accept a settlement offer and a lawsuit is initiated, a subpoena can be expected from the RIAA requiring your institution to disclose the student's identity. The intersection with FERPA requirements to protect student privacy means you will need to notify the student of the subpoena and give the student sufficient time to take action prior to disclosing the information to the RIAA. It would be inappropriate to disclose any information without a proper legal instrument requiring you to do so.

There must be a continuing national discourse about appropriately balancing protections with sufficient space in the framework for innovation to flourish

You can expect some inconsistency. For example, the process used to generate DMCA claims of copyright infringement is apparently separate from the process used to choose individuals for early settlement offers. This means that some students may go through your judicial process following receipt of a claim and believe the matter has been dealt with only to subsequently receive a settlement offer (or be sued); others might only get a settlement offer.

Another inconsistency is that some preservation notices are not followed by early settlement letters. And because the RIAA does not know the identities of the students involved, the same person could receive multiple settlement letters or claims. MIT has written an excellent briefing on the types of orders and requests that an institution can receive, together with what they mean.[21]

Another source of confusion can arise from conflicts with the student conduct judicial process. Often, one of the requirements for reconnection to the network when a student receives a claim of infringement is to remove the allegedly infringing material from his or her computer. On the other hand, early settlement offers direct students to preserve such material.

Bottom line, it is important to recommend to students who receive an early settlement offer that they get legal advice, whether through an on-campus student legal services office or otherwise. In the former case, attorneys regularly communicate with one another on this topic and can provide anonymity when negotiating and paying a settlement.

Higher Education and the Entertainment Industry

In a 2007 paper, Terry Gray aptly captured some common ground between the two communities in articulating that "rights holders should be compensated for their intellectual property" and that "the sharing of copyrighted files without authorization and beyond any reasonable definition of fair use is and should be illegal."[22] After all, higher education institutions are also creators and consumers of intellectual property (consider the parallel with the illegal sharing of digital textbooks and the issuance of infringement claims by some university presses).

And so, collectively, higher education has invested tremendous time, thought, and resources into the immediate and longer-term problem of illegal file sharing. Yet the missions of the two communities are very different.

Educational institutions play a prominent role in shaping students' lives. A natural focus would be integrating understanding of copyright and intellectual property into our curricula—issues important to the nation's economy and to our students as they enter the workforce. UCLA, for exam-

ple, offers an undergraduate seminar on intellectual property developed and taught by the vice provost for intellectual property.

As research institutions, we can also work with the entertainment industry to understand what consumers really want, to examine new business models, and to craft programs that curb illegal file sharing. Illinois State University's Digital Citizen Project[23] is a terrific example. Among other goals, it aims to "significantly impact illegal piracy on campus using a multi-faceted approach to confront pervasive attitudes and behaviors in peer-to-peer downloading of movies, music, and media." The project looks at what students actually do versus what they say they do. In such ways do we need to move beyond the rhetoric that obstructs discussion and look for concrete actions that can start to build trust between higher education and other rights holders.

There must be a continuing national discourse about appropriately balancing protections with sufficient space in the framework for innovation to flourish. (The DMCA predates not only Napster, but also Google, YouTube, TiVo, eBay and the Slingbox: does it still represent the right balance? What will future innovations bring?) It's important for higher education to articulate and advocate for the fundamental principle that copyright law is intended to advance knowledge and that protection should inure to the public good. Here's to the next 10 years, DMCA. *e*

Acknowledgments

I am grateful to Warren Arbogast (Boulder Management Group), Amy Blum (UCLA), Jonathan Curtiss (UCLA), Greg DePriest (NBC Universal), Marc Hoit (North Carolina State University), Steven McDonald (Rhode Island School of Design), Craig Seidel (MovieLabs), and Heidi Wachs (Georgetown University) for so generously sharing their time, expertise, and insight.

Endnotes

1. Throughout this article, any reference to "illegal file sharing" should be read as "unauthorized distribution of copyrighted material." The former phrase is used because its meaning is well understood, if inaccurate.
2. David Greenfield, "Processing DMCA Complaints at Illinois State," http://www.digitalcitizen.ilstu.edu/documents/ISUGreenfield%20-%200607%20-%20DMCA%20Process.pdf.
3. U.S. Copyright Office, "Summary of the Digital Millennium Copyright Act of 1998," December 1998, http://www.copyright.gov/legislation/dmca.pdf.
4. There are also special rules concerning the application of these limitations to nonprofit educational institutions, when faculty or graduate students are engaged in teaching. But these are unlikely to occur in the context of illegal file sharing.
5. U.S. Copyright Office, "Summary of Digital Millennium Copyright Act."
6. "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks," Joint Committee of the Higher Education and Entertainment Communities Education Task Force, http://www.acenet.edu/AM/Template.cfm?Section=Search&section=Legal_Issues_and_Policy_Briefs1&template=/CM/ContentDisplay.cfm&ContentFileID=2091.
7. Another twist for state institutions is the Eleventh Amendment to the U.S. Constitution, which speaks in part to the sovereign immunity of states: States cannot be sued in federal court without their consent, and thus state institutions cannot be sued for copyright violations. Asserting such a position as a matter of policy, however, is likely inconsistent with defending our own copyrights.
8. See the EDUCAUSE analysis of HEA provisions, July 30, 2008, http://net.educause.edu/ir/library/pdf/epo0813.pdf.
9. Memorandum, "HEOA Requirements and Next Steps Related to Peer-to-Peer (P2P) File Sharing on College and University Networks," August 11, 2008, http://net.educause.edu/ir/library/pdf/epo0815.pdf. See also Terry W. Hartle, "Peer to Peer File Sharing and the Higher Education Reauthorization," August 21, 2008; go to http://connect.educause.edu/term_view/P2P+File+Sharing, then click on "HEA Webcast."
10. Cornell Digital Copyright Education Program Mini-Course Demo, http://www.ecornell.com/copyrightdemo/.
11. On the Intellectual Property Institute website, see http://law.richmond.edu/ipi/whatdoyouthink.htm; and the University of Wisconsin–Madison explanation of copyright infringement, http://www.cio.wisc.edu/security/copyright.aspx.
12. Removing or disabling P2P software can be difficult to do properly. The University of Chicago maintains a page of instructions (http://nsit.uchicago.edu/groups/security/guidelines/), but offering students a local service to properly remove such software, perhaps as part of a larger "tune up" to check for outdated security software, could be helpful.
13. EDUCAUSE provided an interpretation of this in its statement on "folder-based" versus "transmission-based" DMCA notices, May 12, 2008, http://www.educause.edu/ir/library/pdf/epo0807.pdf.
14. Worth reading is the court order in Atlantic v. Howell, which raises several issues in what legally constitutes infringement, available at http://www.eff.org/files/filenode/atlantic_v_howel/Atlantic%20v%20Howell%20SJ2%20order.pdf.
15. The Electronic Frontier Foundation has proposed an entirely different model, a Voluntary Collective License system for music; see http://www.eff.org/deeplinks/2008/07/how-make-filesharing-legal.
16. H.R.4137 Higher Education Opportunity Act, http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.04137:.
17. Letter to education leaders in the House and Senate cautioning against legislative provisions requiring universities to use filtering software to handle copyright infringement on their networks April 15, 2008, http://www.acm.org/usacm/weblog/wp-content/USACM_Filtering_Final.pdf.
18. For a definition of ACNS, see http://mpto.unistudios.com/xml/.
19. See the EDUCAUSE statement on DMCA notices, http://www.educause.edu/ir/library/pdf/epo0807.pdf.
20. Log retention times could be reduced specifically for the purpose of not being able to comply with preservation notices. However, the general—and wise—rule of thumb about retaining any information, log files or otherwise, is to determine what the business need is for the records, and then implement procedures to keep them for that period of time and no longer.
21. "If You Are Issued a Copyright Infringement Notice," http://web.mit.edu/ist/topics/security/copyright/notices.html.
22. Terry Gray, "On Network-based Copyright Enforcement," June 2007, http://staff.washington.edu/gray/papers/copyright-enforcement.html.
23. See the project's home page at http://www.digitalcitizen.ilstu.edu/.

Kent Wada (kent@ucla.edu) is Director of IT Strategic Policy at UCLA in Westwood, California.