Electronic Frontier Foundation

When Push Comes to Shove:
A Hype-Free Guide to Evaluating Technical Solutions to Copyright Infringement on Campus Networks

For years, university administrators have faced a growing challenge: fighting copyright infringement on campus networks. Confronting this challenge has not been easy and neither has choosing the right tool for the job. Universities that choose to take on this task have employed a range of strategies, from education in the residence halls, to increased enforcement of network use policies, to cooperating with the recording industry in its controversial litigation campaign against peer-to-peer (P2P) file sharers. Others have chosen to resist these tactics and stand with their students in motions to quash record industry subpoenas for student identities. Others are looking at adopting a different strategy: implementing technical solutions such as Audible Magic, Packeteer, or ICARUS. Some combine aspects of all the above.

With regard to technical solutions, the results have been mixed. Many of these tools fail to stop the majority of network infringement. Others bring about temporary peace, but only at the expense of limiting student access to critical resources and applications. In some cases, using the technology means conducting detailed surveillance of all campus network traffic, posing a threat to the privacy of the university community. In others, it means turning over to copyright holders "remote control" of access to the university network. The bottom line is that using technical tools to discourage infringement has significant trade-offs.

This paper is intended to help institutions of higher education critically evaluate the principal technological tools and policies being used to enforce copyright on campus networks.[1] It first explores where the goals of copyright holders and universities overlap and where they conflict. It then discusses the pros and cons of the major solutions and explores alternatives. Finally, it offers a series of questions designed to help university IT professionals develop criteria for evaluating future tools as they come to market.

Competing Goals

While there may be overlap in the desire to curb infringement, copyright holders and universities otherwise have very different interests. Copyright holders tend to be commercial entities with the primary goal of maximizing profit and shareholder value through legal enforcement and licensing. Universities, on the other hand, have a more public role that includes educating students, judiciously allocating scarce resources, and choosing institutional policies that are both ethical and prudent. Following is a sketch of how university goals "map" in relation to technical solutions endorsed by copyright holders.

[1] For some initial analysis of these issues, see Joint Committee of the Higher Education and Entertainment Communities, "University Policies and Practices Addressing Improper Peer-to-Peer File Sharing": <www.acenet.edu/AM/TemplateRedirect.cfm?template=/CM/ContentDisplay.cfm&ContentID=8503>.

Goal 1: Ensuring a High Quality Educational and Research Environment

The primary mission of the university is to provide an environment that fosters learning and research both in and out of the classroom. It's now commonplace for educators to provide students with the "basics" for completing a course of study via campus networks. They post syllabi on class websites, distribute course materials (including video lectures) online, and use email to offer students after-hours feedback on their work. Increasingly, educators are also asking students to publish their assignments online for peer review, participate in public discussions in class weblogs, and even take tests online.[2] Meanwhile, students continue to use the networks for such basic tasks as researching a paper or browsing the library catalog. This kind of access is not a luxury – it's a fundamental requirement for today's students.

But online learning doesn't stop there. For those studying computer engineering, media, music, art, and film, access to the network is a key to the lab, studio, or cutting room. Universities are hubs of innovation, and restrictions on essential resources for learning and experimentation have real costs. For example, both Google and Yahoo! were founded by Stanford University students who had access to an open, unfettered campus network that allowed them the freedom to write and deploy their own indexing and search applications using university networking resources. They didn't have to build Internet technologies on a locked-down facsimile of the Internet – they built them on the real thing. It is in this context that the decision to adopt a technical solution that disrupts "end-to-end" communication[3] or automatically bumps a student off the network should be carefully considered.

Goal 2: Properly Allocating Technical Resources

Maintaining a university's IT infrastructure is complicated, time-consuming, and expensive; moreover, campus IT departments must manage these issues with limited resources. Therefore, it is important to examine how technical solutions to copyright infringement will impact campus resources in both the short and long-term. How effective is the solution? How much does it cost today? How much will it cost next year? Will it require maintenance? Will it make the university too dependent on a particular vendor? Could these resources be better allocated elsewhere? Answers to these questions are critical to assessing whether or not a specific technology meets this goal.

Goal 3: Discouraging Infringement While Protecting Academic Freedom and Privacy

Universities have a legitimate interest in discouraging their users from violating the law, including copyright law. Yet they also have a duty to protect the legitimate interests of university users, including the right to privacy and the right to make "fair use" of copyrighted materials – an activity central to academic life. The baby should not be thrown out with the bathwater; it is critical that privacy and academic freedom are not superseded by copyright infringement concerns.

Moreover, universities have a strong interest in seeing that when its members are accused

[2] See, for example, "Marxism and Cultural Studies," a course website by an instructor at Pomona College: <http://classes.plannedobsolescence.net/149/>

[3] See WIKIPEDIA, "End-to-end principle", <http://en.wikipedia.org/wiki/End-to-end_principle>.

of copyright infringement, they are treated fairly and equitably. Copyright holders today have powerful legal tools at their disposal to use against people accused of copyright infringement, and students have already become the victims of over-reach.[4] It is in the best interest of both the university and its faculty, staff, and students to develop policies that protect the privacy interest of the university community, while also providing sensible, transparent procedures for addressing claims of infringement.

Technical Solutions to Copyright Infringement

Following is a brief overview of the current major technical solutions currently being offered to control campus infringement. It is important to note that despite the heightened rhetoric surrounding the battle over P2P, none of these solutions are required by law. A university may be free of liability for students' activities despite not having taken any technical measures.[5] They are simply tools that may or may not be useful for combating infringement on a technical level.

Content Monitoring and Network Surveillance

Content-monitoring systems monitor networks for copyrighted material. For example, Audible Magic's CopySense is a hardware/software appliance that compares all data traveling over the network against a database of "acoustic fingerprints." The fingerprints are generated from copyrighted songs supplied by record companies. If a match is found between data on the campus network and a file in the database, the transmission can be terminated or simply logged for future disciplinary action.[6]

These systems look good on paper, especially to record companies. The Recording Industry Association of America (RIAA) even led a lobbying tour in Washington, DC, to sing the praises of Audible Magic to Congress. With content-monitoring and surveillance systems constantly scanning university networks for infringement, the RIAA argued, students will be technologically prohibited from using the networks for infringement. What the RIAA neglected to emphasize, however, was that the entire burden of purchasing, implementing, and maintaining these systems would then fall squarely on the shoulders of the universities that employ them. Neither the RIAA nor the

[4] For example, Diebold, Inc., a maker of electronic voting machines, accused two Swarthmore students of copyright infringement when they posted Diebold internal memos indicating security flaws in the machines on their student web pages. Diebold's accusations led to removal of the information from the pages. Yet, later, a California district court determined that Diebold knowingly misrepresented the facts, stating "No reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold's voting machines were protected by copyright." See <http://www.eff.org/legal/ISP_liability/OPG_v_Diebold/20040930_Diebold_SJ_Order.pdf>.

[5] In fact, use of some of these systems may expand the risk of liability for universities for copyright infringement. While it is beyond the scope of this paper to address, some courts have found that increasing institutional ability to intervene in employee or user copyright infringement can expose the institution to higher burdens and a higher duty not only to continue policing its system but also a duty to upgrade and improve its policing to the highest extent possible or face serious liability. See A&M RECORDS, INC. **v**. NAPSTER, INC., 239 F.3d 1004 (9th Cir. 2001): <http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm>.

[6] For more details on how CopySense works, see Chris Palmer's "Audible Magic – No Silver Bullet for P2P Infringement": <http://www.eff.org/share/audible_magic.php>

government has once offered to help fund or administer the necessary IT resources required to undertake such scanning.

In addition to the resources they consume, these solutions often are only able to offer stopgap solutions to the infringement problem. Content-monitoring systems rely on one important premise: that they will be able to examine all network traffic and compare every single bit transferred with a master database of prohibited material. If such systems cannot correctly understand or interpret the information on the network, then they cannot function accurately as a monitoring or enforcement system.

Today, most file-sharing applications transmit information in ways that content surveillance systems can observe, but that is changing swiftly. Newer file-sharing programs like Waste[7] already use encryption to protect P2P traffic from prying eyes and more such programs are projected to enter the market soon. There are also a number of cryptographic techniques that could easily be implemented in P2P systems, such as Secure Socket Layer (SSL) encryption. Such tools and techniques essentially stop content surveillance in its tracks. Encrypted traffic cannot be scanned for an acoustic fingerprint since all of its bits are scrambled to be unintelligible to anyone other than the decryption key holder. With use of encrypted P2P likely to become commonplace, especially if network monitoring becomes widespread, universities that have invested in such systems will be left with a high-cost, resource-intensive infrastructure that fails to serve the goal it was purchased to achieve. Universities considering the purchase of such systems should be cognizant of this clear barrier to long-term efficacy.[8]

Moreover, these systems cannot replace the proper judgment of experienced campus administrators. This is especially important in areas touching on academic freedom, such as fair use of copyrighted material. For example, consider a scenario where a law student studying copyright law has just read the Supreme Court case *Campbell v. Acuff Rose Music, Inc.*,[9] in which a company representing Roy Orbison sued the rap band 2 Live Crew for publishing a parody of Orbison's classic song, "Pretty Woman." In the case, the Supreme Court compared the two songs, pointing out that 2 Live Crew's use of the song was parodic and therefore a fair use of copyrighted material rather than infringement. The student, having just read the case, is eager to investigate how similar the two songs are and whether the Court was correct in its parody analysis. She goes online, finds a copy of each song, and begins downloading them so she can hear them for herself – a classic academic fair use. But suddenly, the downloading stops. The campus content surveillance system has detected that the songs the student wishes to download are acoustic matches to copyrighted material owned by Acuff Rose Music and 2 Live Crew's record label. It automatically terminates the download as well as the student's

[7] <http://waste.sourceforge.net/>
[8] Some vendors of content surveillance systems have responded to this criticism by suggesting that for every "upgrade" P2P programs make to avoid detection, they too will "upgrade" their appliance to see through it. While this approach is technologically suspect for encryption technology (i.e., unless you have the key, you cannot "upgrade" anything to detect the content of the message), even if it were successful, it locks in universities to particular vendors, making them dependent on signing expensive "service" contracts to avoid being stuck with an obsolete appliance.
[9] <http://supct.law.cornell.edu/supct/html/92-1292.ZS.html>

Internet access privileges for the night. Here, the content surveillance system worked exactly as it was designed. Yet the result is the inhibition of academic freedom with no effect on the prevention of infringement.

Another common example that can run up against the limits of content monitoring is when a member of the campus community wants to listen to a song from their music collection in someplace other than where they keep it. For example, suppose a staff member wants to listen to music in her office. She connects to her home computer over the campus network and decides to transfer a few albums onto her work computer so they can play in the background. The content-monitoring system detects these transfers and immediately tags the employee as a copyright infringer, automatically shutting down her network access privileges and forwarding a report of the incident to her supervisor for disciplinary action even though what she was attempting is perfectly legal.

Finally, and perhaps most importantly, content surveillance jeopardizes the privacy of the entire university community. Network surveillance technologies inevitably examine far more network traffic than just the "infringing" bits. A network infrastructure optimized for surveillance may invite additional monitoring and filtering obligations. If everyone knows that all Internet activities are routinely monitored, it will profoundly alter the kinds of research and intellectual exploration they are willing to engage in, to the detriment of the academic freedoms that are so important in higher education. This is particularly important when researching or reading about controversial issues such as HIV/AIDS or sexual abuse recovery.

Content surveillance changes this environment for online reading and research. By monitoring, logging, and/or keeping a copy of who sent what and when (a feature often available and implemented in these systems), these systems become repositories of surveillance information on every member of campus, including faculty and staff, cataloging their every interest and endeavor online.[10] Such data is extremely personal and sensitive, and the potential for its abuse could expose universities to serious political and legal risks,[11] including potential criminal liability for violation of wiretap laws.[12]

Traffic Shaping

Traffic-shaping tools allow administrators to put caps on the amount of bandwidth that the network devotes to different applications or users. These tools are used in situations in which many people share limited bandwidth and the administrator needs to prioritize certain tasks, such as secure networking (SSH) or sending email (SMTP). Using a

[10] For more about the legal and policy ramifications of logging Internet traffic, see EFF's "Best Practices for Online Service Providers" <http://www.eff.org/osp/>.

[11] See *Berkeley Theft Exposes Data of 100,000*, at <http://msnbc.msn.com/id/7320552/>.

[12] For example, monitoring the contents of student, faculty, or staff electronic communications, even over P2P networks, potentially violates federal and state criminal wiretapping statutes when done without the user's explicit consent. Even if your intention is to reduce copyright infringement, you might still run afoul of these laws and open you, your coworkers, and your university up to civil and criminal liability. Furthermore, even where you do get campus users' consent, such monitoring may be illegal under your state's wiretap statute: several states provide greater protection than the federal statute by requiring the consent of **all** parties before you can intercept communications content.

traffic-shaping tool, an administrator can set up simple rules governing which tasks have high priority and which do not. If network traffic is light, then users may be able to send and receive P2P traffic. But if people need to send email or do homework via the Web, the traffic shaper can give email and web traffic as much bandwidth as they need while throttling back P2P traffic until it no longer obstructs these other applications. Administrators can also differentiate by campus location, prioritizing laboratory computer traffic over ResNet traffic.

A well-known program for traffic shaping is Packeteer's PacketShaper. It may be the most popular way to regulate the amount of traffic on campus networks. PacketShaper is a hardware/software appliance that attaches to the network and sets boundaries on different types of traffic. Control over traffic can be very granular; an administrator may choose to control the amount of bandwidth allocated to each user, or the amount allocated to particular port numbers. Notably, PacketShaper, and traffic-shaping programs more generally, do not examine the *specific content* of data traveling over the network. They only ascertain the type and amount of data being transferred: email, web, P2P, etc. This has the clear advantage of protecting privacy and avoiding "false positive" enforcement actions based on misidentification of data's copyright status.

But there is a downside. Traffic-shaping tools are useful for allocating scarce network resources by host and port, but their ability to parse traffic from particular applications is limited. Like content-monitoring solutions, traffic shapers designed to stop a particular "flavor" of data – such as data from P2P applications – can be foiled with relative ease if students use encryption or protocol tunneling (both techniques are already being employed in modern P2P applications). That said, making bandwidth a scarce resource may force students to rethink how they use it,[13] and if reasonably implemented, would not likely lead students to try to avoid detection.

Firewalling and Technology Bans

Another quick-and-dirty way to address campus copyright infringement is to use a network firewall to block all data going to and from ports that are commonly used by P2P applications. The problem with this method is that it is often easy to fool firewalls into letting P2P traffic through. Users can send P2P data to an unexpected (and unblocked) port, or they can hide P2P traffic inside other traffic that looks like something unrelated, such as email or web traffic.

Some universities are taking this strategy a step further by banning entire classes of multi-purpose network applications. Penn State, for example,[14] bans students from running web servers despite the fact that they can be used for many activities that have nothing to do with copyright infringement. This kind of policy is especially troubling when you take into consideration the severe restriction on learning that it represents for

[13] Cornell University, for example, has implemented a campus-wide "bandwidth metering" solution. Network users are entitled to use two gigabytes of bandwidth per month without charge. Bandwidth usage above that quota results in a per-megabyte charge for off-campus traffic that is billed to the user. Cornell administrators believe that this metered approach has given students strong incentives to avoid "uploading" files to P2P networks.

[14] < http://www.freedom-to-tinker.com/archives/000606.html>

students of computer engineering. For example, NASA recently decided to employ the popular P2P technology of Bittorrent to help reduce bandwidth demands on its servers for its massive and revolutionary World Wind program.[15] Without access to such applications, students who wished to study NASA's use of this alternative distribution model would not be able to do so. Bans of this kind also stymie other kinds of student-initiated innovation – neither Yahoo! or Google could have been created had Stanford imposed this kind of ban on its campus network.[16]

Automated Copyright Notice System (ACNS)

Developed by several entertainment companies, this system allows copyright holders to terminate a student's network access by sending a copyright complaint in a machine-readable XML document. The XML-formatted complaints authorize a campus application to send a takedown notice to the relevant network user. If the user does not remove his or her allegedly infringing materials, ACNS automatically cuts off the user's network access. A technical summary for the system reads: "ACNS is an open-source, royalty-free system that universities, ISPs, or anyone that handles large volumes of copyright notices can implement on their network to increase the efficiency and reduce the costs of responding to the notices."[17]

UCLA has already implemented a system like ACNS. Unfortunately, an automated system like this can quickly become indistinguishable from giving copyright owners "remote control" over campus network access. Because systems like ACNS have no way to verify the authenticity of either the sender of the complaint or its contents, network operators have suggested that jokesters or vandals could send "spoof" letters to the system in order to cut off the network connections of people they don't like. Further, the system again bypasses any consideration of whether the student is making fair use of copyrighted material. This kind of rigidity may be effective in stopping some infringement, but it's also likely to stop perfectly legitimate activity as well. At a time when campus network access is quickly becoming an educational requirement for students, delegating the question of network access to third parties seems unwise. In addition, the time, money, and energy that university IT personnel may have to spend sorting out these mistakes may present significant costs and burdens on already limited resources.

Implementation: Hard vs. Soft Technical Sanctions

All these mechanisms (firewalls, traffic shaping, content analyzers, ANCS notices) are going to have unintended consequences, including "spoofability." These network defenses can also become new attack vectors.

For example, as we note above, if CopySense is automatically set to kick people off the network, a student could spoof another students' IP address, upload a Metallica tune to her professor's FTP drop box, and get both kicked off the network.

[15] <http://opensource.weblogsinc.com/entry/1234000957039301>

[16] For an in-depth discussion of how unplanned and tangential experimentation can lead to ground-breaking innovations, see Eric von Hippel, *Democratizing Innovation* (MIT Press 2005).

[17] <http://mpto.unistudios.com/xml/ACNS_Summary.doc>

For this reason, these mechanisms, if they are to be used at all, should employ "soft" rather than "hard" sanctions. Throttle instead of disconnect; de-prioritize instead of deny. This makes the cost of mistakes much lower, while still providing adequate protection for copyright.

Additionally, content problems are not network problems, and treating them as such will have negative side effects without enough benefit to justify them. One would imagine that combining CopySense with a soft policy ("If it matches our copyrighted materials database, rate-limit it") would be the ideal. But it's not ideal for three reasons: CopySense will still have false positives and false negatives, non-copyrighted data transfers might still be hogging all the bandwidth, and the application may create privacy-related risks to the university.

A better solution may be to dynamically generate fine-grained (e.g. at the transport layer circuit level) policies based on administrator-defined constraints. For example, an administrator could decide that a campus research laboratory needs 10 megabits per second (Mbps) at all times; that secure shell (SSH) is the highest priority, but usually needs very little bandwidth; and that the public website is also high priority, and must always have at least 2Mbps available to it. Another alternative may be to impose subcharges on users for outbound or inbound Internet traffic above a certain threshold, as Cornell University does.

Technical solutions that meet these constraints should be sufficient. If the dormitory network is using so much bandwidth that someone in the research lab can't spider the Web for an experiment, such policies could throttle back the dorm transmission control protocol (TCP) sessions. It wouldn't matter whether the bandwidth problem was caused by file sharing or a student's personal website suddenly getting lots of hits from a site like Slashdot. The approach would be to operate under a set of constraints, throttling gently and specifically. There would be no need for expensive content analysis – just cheap transport layer and network layer pattern-matching. A tool like Packeteer's PacketShaper would be useful for this approach.

Alternatives

As we have shown, there are no easy technical "fixes" for copyright infringement on campus. In some cases, university administrators risk threatening a wide range of legitimate university objectives for an expensive, temporary, or minimally effective solution. In others, as is the case with technology bans, administrators are choosing to restrict or remove actual educational resources – putting students with both formal and informal interests in such diverse topics as computer science, engineering, digital art, and online journalism at a distinct disadvantage, especially when compared to students at universities with less restrictive policies. While fighting infringement is important, it shouldn't mean that universities are forced to invade users' privacy or offer a "second class" education to students entering a world where technological expertise is increasingly important.

This is why many universities may want to minimize or reject technical solutions altogether and choose instead to emphasize other strategies for combating infringement. As discussed earlier, there is no general legal obligation on universities to implement technical measures to monitor networks or to police infringement.

Campus Adoption of Authorized Download Service

One alternative solution, spearheaded by Penn State, is to pay for campus-wide access to authorized music services like Napster. The goal is to lure students away from copyright infringement with legal ways to download music.

A problem with this approach is that it requires everyone to pay for services that many may not be interested in or able to use.[18] At some schools, students have protested these fees, saying that they don't want to pay for a download service that they haven't chosen.[19] Recently, the Tennessee Board of Regents rejected an RIAA proposal that would have cost the state school system over $23 million per year for student access to Napster. It also remains unclear whether making students purchase access to Napster-like programs curtails the use of file-sharing programs, which offer a much wider variety of music. If students continue to file-share, then the lawsuits against students and the burden on the campus IT staff to monitor and enforce network policies are likely to continue in spite of the substantial fees paid to RIAA-endorsed services.

Alternative Efforts to License Legal Music

Another solution is something the record labels themselves could offer: voluntary collective licensing. As EFF notes in our white paper[20] advocating this solution, the concept is simple. The music industry forms one or more collecting societies, which then offers licenses so file-sharers can "get legit" in exchange for a reasonable regular payment. The money collected then gets divided, ASCAP-style, among rights-holders based on the popularity of their music. With legal “all-you-can-eat” file-sharing, artists get paid and students have no incentive to break the law. Neither lawsuits nor expensive network monitoring are needed.

The RIAA has yet to offer any school this kind of license, but the more universities express interest, the more likely it is that the record labels will consider it. The advantage over a service like Napster is that with Napster, a university still risks lawsuits against students who continue to file-share “on the side.” In addition, the IT staff still bears the burden of enforcement responsibilities. Collective licensing would put an end to the lawsuits and eliminate the need for any IT resources to be devoted to policing peer-to-peer music downloading.

Clear Acceptable Use Policies

Many schools, such as the University of Michigan, have developed clear acceptable use policies for their campus network and prominently display these policies on websites

[18] For example, Apple Computer’s popular iPod music player and Macintosh computers will not support music purchased from Real Networks’ *Rapsody* service or Napster.
[19] <http://news.com.com/2100-1027_3-5103918.html>
[20] <http://www.eff.org/share/?f=collective_lic_wp.html>

where users can easily read through them.[21] These policies explain what copyright infringement is and some even show how to use typical P2P programs in non-infringing ways. A number of schools require staff, faculty, and students to read network use policies before getting an account on the campus network. When properly informed, these users are better able to distinguish between legitimate and illegitimate uses of copyrighted materials.

Of course, even those who are well-informed about copyright infringement may continue to violate the law. This is why schools should also have simple, coherent policies that spell out what will happen to users suspected of infringement. For example, a policy could explain how infringement is a violation of the campus honor code or code of judicial conduct and detail what the procedures and penalties are for students who violate these codes. Unlike the technical measures outlined above, codes like these have been developed and tested over time and there are often safeguards in place to protect privacy and due process. Policies should also outline the process by which IT department will notify a user when a copyright takedown notice is received and let them know how long he or she has to respond. IT departments should make it a priority to respond quickly to users who provide evidence that the materials they've posted or hosted are not infringing.

In the event that a situation escalates, there should be a procedural structure in place to provide the user with the information he or she needs to respond properly to infringement claims. While a Digital Millennium Copyright Act (DMCA) compliance officer is helpful in dealing with liability issues, it's also critical that university administrators and counsel work together to give users the resources and support necessary to make appropriate decisions about how to proceed.[22]

Copyright Tutorials

When new students move into the dormitories at UC Berkeley, IT staff members who manage the residential network conduct mandatory classes for anyone signing up to use the network. In these classes, students are informed about the campus acceptable use policies and given face-to-face tutorials on proper use of network resources, including copyrighted materials. Tutorials provide another opportunity for IT staff to help users understand the nuances of copyright law before they use the network. Users can be informed that the RIAA is actively monitoring university networks for P2P file sharing activity. They also provide a great opportunity to talk to users about the more creative and positive sides of copyright law, such as fair use and adaptation of images and stories from the public domain. Tutorials also support an educational environment, allowing for exploration and discussion of the reasons behind use policies with university staff members. Moreover, unlike technologies such as CopySense, tutorials can be updated and changed every year without great expense.

Other Educational Options

In addition to university-led education efforts, independent groups like the American

[21] <http://www.umich.edu/~policies/>
[22] See, e.g., discussion at <http://blogs.law.harvard.edu/cmusings/2003/11/20#a501>

Library Association are developing free materials[23] that explore the notion of balance in copyright law – not just unfettered enforcement. This perspective is a welcome attempt to enrich the important conversation about how copyright law and technology interact in the academy.

Conclusion

Universities are increasingly being pressured to take action against copyright infringement. While implementing a technical solution may appear to be the easiest path, that's not necessarily the case, and it's not necessarily the best choice from the university's educational perspective. We encourage university administrators to look beyond the hype surrounding P2P and evaluate their options with a dispassionate eye. Technical solutions can be useful, but they are also frequently blunt instruments for dealing with a complex problem like infringement on campus networks. Rather than rush to join the technology "arms" race, we hope that universities will take a moment to consider the ramifications adopting such technologies can have on both the academic environment on campus as well as their IT resources and priorities. In the end, we believe a solid focus on providing an environment that fosters education on a range of issues, including copyright, is the best solution.

[23] See <http://www.wired.com/news/digiwood/0,1412,64543,00.html>

Appendix:
Questions to Ask Vendors If You're Considering a Technical Solution

1. Will I have to upgrade the software/hardware associated with your solution if students start encrypting or hiding their traffic? If so, how much time, money, and effort will that take?

2. Does this solution require monitoring of all traffic? (In other words: can you or the technology provider locate P2P traffic without also monitoring other student activities such as emailing and web surfing?)

3. How flexible is the proposed technology? Does it recognize traffic from multiple P2P programs and systems? Can it recognize P2P traffic if it's tunneled inside HTTP?

4. Will your company offer my campus a refund and/or indemnification against liability if the product fails adequately to detect infringement or violates privacy laws?

5. Have outside parties conducted an analysis of the effectiveness of this product? What were their findings?

6. Have outside parties evaluated the privacy implications of using this product on a computer network? What were their findings?

7. What are the annual costs for upgrades or service? Is there anything that won't be covered by these fees?

8. How flexible are the policies of the proposed solution? Do I have the option to implement hard vs. soft enforcement actions?