I. Introduction

With the (largely illegal) use of peer-to-peer file-sharing software continuing to grow even in the face of nearly 8,000 RIAA lawsuits — so far — and the Supreme Court’s recent announcement that it will hear an appeal in MGM v. Grokster, a case that will determine the legality of the software itself, the issue of what to do about file-sharing will, once again in 2005, remain at the top of the cyberspace agenda on college and university campuses. But other issues will require attention as well: Newly issued guidance from the Federal Trade Commission indicates that, despite our best hopes, we are not exempt from CAN-SPAM regulations and must therefore plan for compliance in at least a few areas. And the issue that could be our worst nightmare — cybersecurity, and our potential liability for a lack thereof — will simply not go away.

II. File-Sharing

In 1999, Northeastern University freshman Shawn Fanning unleashed upon the world Napster, a software program that, for the first time, enabled computer users to share music with one another easily over the Internet. Napster quickly attracted the attention of college and university students, who had ready access to the substantial bandwidth required to operate the program; of college and university information technology offices, which saw their available bandwidth disappear virtually overnight; of the music industry, which (with considerable justification) feared lost sales and revenues — and, of course, of the lawyers, for whom copyright law, previously a sleepy backwater of the profession, soon became the Next New Thing.

Before long, the music industry and its lawyers succeeded in shutting down Napster the company, but Napster the idea proved to be a more elusive target. Almost as quickly as the first lawsuits were filed, numerous clones and variations of the Napster software appeared. These new programs exhibited an almost viral ability to
replicate, to hide deep within the Internet while they gained strength, and to adapt themselves to the interstices of the court rulings.

As its battle against the software providers bogged down in the face of these developments, the music industry opened up new fronts. At first, it attempted to enlist the colleges and universities and other ISPs that provide the “pipelines” that make file-sharing possible, through massive use of the DMCA’s “notice and takedown” procedure. More recently, when that effort yielded few concrete results, the industry’s trade association, the Recording Industry Association of America, began to sue the (alleged) users of file-sharing software, including a number of college and university students, grandmothers, and at least one 12-year-old. To date, the RIAA has filed 7,704 such lawsuits and settled 1,475 of them for a reported average of about $3,000. The industry also has been actively lobbying Congress — so far largely unsuccessfully — to impose substantial new responsibilities and liabilities on almost everyone involved in the process of file-sharing, no matter how remote or tangential their role may be. And, with somewhat more success, the industry has pushed the Bush administration to make file-sharing a top criminal priority.

College and university administrators attempting to sort this situation out have found themselves pulled in many different directions. On the one hand, colleges and universities produce substantial intellectual property and understand the need to protect it, while, on the other, they also wish to protect the concepts of academic freedom and fair use, as well as to avoid in loco parentis responsibilities. At a more practical level, rapidly increasing demands for bandwidth and costs of responding to DMCA notices are stretching already-thin institutional budgets. Then, too, colleges and universities wish to avoid liability both for themselves and for their students.

So, what should be done?

A. Law

While there is no one right answer to that question, whatever answer an institution chooses should, first, be grounded in an understanding of the relevant law, which, like Gaul (and to carry the war metaphor to the extreme), is divided into three parts:
1. **Liability of Users**

Whether it should be the law or not—a policy and philosophical issue best left to another day—there really is no question that those who use file-sharing software to trade copyrighted music over the Internet are engaged in massive copyright infringement under current law. The standard for copyright infringement is simple, direct, and broad: "Anyone who violates any of the exclusive rights of the copyright owner as provided by [the Copyright Act] . . . is an infringer of . . . copyright," 17 U.S.C. § 501(a). Among those exclusive rights are the rights to reproduce the copyrighted work and to distribute copies of the copyrighted work to the public, 17 U.S.C. § 106(1) and (3)—the very acts that are at the heart of almost every use of file-sharing software.

The desires of the music industry notwithstanding, however, copyright law is not completely absolute; there are a few exceptions that potentially are applicable even to file-sharing, broadly conceived—most notably fair use. At this point, it generally is accepted—and rarely disputed even by the music industry—that making a copy of a song or CD that you already legitimately own, for your own personal use on your own MP3 player or computer, is a fair use and therefore not copyright infringement. Thus, to the extent that file-sharing software is used simply to effect such "space shifting", it raises few legal concerns. See, e.g., Recording Industry Ass'n of America v. Diamond Multimedia Systems, 180 F.3d 1072, 1079 (9th Cir. 1999) (copying one's own music to one's own MP3 player "is paradigmatic noncommercial personal use entirely consistent with the purposes of the [Copyright] Act"). See also in re Aimster Copyright Infringement Litigation, 334 F.3d 643, 652-53 (7th Cir. 2003), cert. denied sub. nom. Deep v. Recording Industry Ass'n of America, 540 U.S. 1107 (2004) (discussing with approval, though not expressly ruling upon, the "space shifting" rationale). In addition, under the "first sale" doctrine, it also is permissible to share a song or CD that you legitimately own by transferring physical possession of it (not a copy) to a friend, either temporarily or permanently. 17 U.S.C. § 109(a).

But despite these limited exceptions, it is even more clear that "sharing" the same song or CD indiscriminately with others by uploading it to the Internet or "borrowing" it by downloading it from the Internet constitutes copyright infringement. "Napster users who upload file names to the search index for others to copy violate plaintiffs' distribution rights. Napster users who download files containing copyrighted music violate plaintiffs' reproduction rights." A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001). See also id. at 1019 ("[D]iamond . . . [is] inapposite
because the methods of shifting in . . . [that] case[ ] did not also simultaneously involve distribution of the copyrighted material to the general public; the . . . space-shifting of copyrighted material exposed the material only to the original user.

Moreover, the stakes are quite high for those who do engage in such "sharing": Statutory damages can run as high as $150,000 for each individual infringement, 17 U.S.C. § 504 – a user sharing just 10 songs could thus potentially be liable for as much as $1.5 million – attorney fees and costs can also be awarded, 17 U.S.C. § 505, and even relatively minor infringements can result in substantial criminal fines and imprisonment, 17 U.S.C. § 506 and 18 U.S.C. § 2319. To make things worse, copyright infringement is a strict liability matter. Lack of knowledge or intent is not a defense to a copyright infringement suit (though it can be taken into account in setting damages); "innocent" infringement is infringement nonetheless. Information Infrastructure Task Force, Report of the Working Group on Intellectual Property Rights (1996) at p. 101, available online at <http://www.uspto.gov/web/offices/com/doc/ipti/ipti.pdf>.

2. Liability of Software Providers

Those who create and distribute the software that makes file-sharing possible also have potential copyright liability, though generally for contributory, rather than direct, infringement. "[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory infringer.'" Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971). The three primary elements of contributory infringement thus are (1) a direct infringement by someone else, (2) knowledge of that infringement, and (3) a material contribution to that infringement.

With direct infringement a given in this context, Napster, Aimster, Gnutella, and others have focused their defenses on the second and third elements. In doing so, they have relied in large part on Sony Corp. v. Universal City Studios, 464 U.S. 417 (U.S. 1984), the case in which the Supreme Court addressed whether Sony was contributorily liable for the infringements committed by users of its Betamax video recorder. The Court acknowledged that Sony had at least constructive knowledge that some Betamax purchasers would use the machines to commit copyright infringement. Applying a sort of cost-benefit test, however, the Court held that that was not enough: '[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable
purposes. Indeed, it need merely be capable of substantial noninfringing uses.” Id. at 442. In other words, the fault – and any liability – lies with those who choose to misuse equipment that can be used for both “good” and “bad” purposes, not with those who manufacture and distribute it.

The courts have split on the applicability of the “Sony defense” to file-sharing software. In both A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), and In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), the courts rejected that defense, finding in effect that the programs had been designed specifically for the purpose of copyright infringement, that there was no real evidence that they had ever been used for anything else, and, thus, that there was no public or social benefit at all to balance against the heavy cost to copyright owners. In Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *affd*, 380 F.3d 1154 (9th Cir.), *cert. granted*, 125 S. Ct. 686 (2004), however, the court found that “Grokster and [Morpheus] are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights”, and that there are in fact “substantial noninfringing uses for ... [their] software”. *Id.* at 1043. This split seems to be attributable at least in part to the differing architectures of the various programs – the more recent programs require much less ongoing involvement on the part of the distributors – but a cynic might attribute the true difference to the fact that the distributors of Grokster and Morpheus were simply more discreet about their intentions and did a better job of avoiding knowledge of their users' activities.

Regardless, the split should be resolved later this year. The Supreme Court has agreed to hear an appeal of the Grokster case, 125 S. Ct. 686 (2004), arguments are scheduled for March 29, and the decision should be issued by early July at the latest.

3. **Liability of Internet Service Providers**

Internet service providers, too, face potential liability for contributory infringement, but they also have an additional, and much more potent, defense: the Digital Millennium Copyright Act. Enacted in 1998, when file-sharing was “not even a glimmer in anyone’s eye”, Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004) (citation omitted), and designed to balance the interests of copyright owners with the desire to promote the Internet, the DMCA provides ISPs with four “safe harbors”
from liability for the conduct of their subscribers, account holders, and other users. Two of those safe harbors, for “hosted content” and for “conduit” transmissions, are of particular importance in this context.

To be eligible for any of the DMCA safe harbors, an ISP must first satisfy two general requirements: (1) it must adopt, “reasonably implement”, and inform its users of “a policy that provides for the termination in appropriate circumstances of . . . repeat infringers”, and (2) it must “accommodate” and “not interfere with” any standardized technical measures that copyright owners use to identify and protect their works. 17 U.S.C. § 512(i)(1). The ISP must then meet specific additional requirements for each safe harbor:

(a) “Information Residing on Systems or Networks At Direction of Users”

While property owners can sometimes be held liable for copyright infringements that others commit on their premises, an ISP can avoid liability for hosting others’ material on the ISP’s servers – in the words of the statute, for “the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider”, 17 U.S.C. § 512(c) – under the following circumstances:

- The ISP must not have either actual knowledge that specific material on the ISP’s system or network is infringing or awareness of facts and circumstances from which such infringement is apparent. 17 U.S.C. § 512(c)(1)(A). General awareness that file-sharing is occurring somewhere on the ISP’s system is not enough.

- If the ISP does obtain such knowledge or awareness, the ISP must “expeditiously” remove or disable access to the infringing material. Id.

- If the ISP has “the right and ability to control” the infringing activity, the ISP must not receive a direct financial benefit attributable specifically to that activity – for example, a percentage of sales, as opposed to a flat subscription fee. 17 U.S.C. § 512(c)(1)(B).

- The ISP must designate “an agent to receive notifications of claimed infringement”, register that agent with the Copyright Office, and make the
contact information for that agent available "on its website in a location accessible to the public". 17 U.S.C. § 512(c)(2).

- The ISP must comply with the "notice and takedown" procedure upon receipt of a "substantially complying" notice. 17 U.S.C. § 512(c)(1)(C).

(b) Transitory Digital Network Communications

The DMCA also provides immunity for infringing material that simply passes through an ISP’s system, from and to points outside that system: "A service provider shall not be liable for ... infringement of copyright by reason of the provider’s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections . . . ." 17 U.S.C. § 512(a). To be eligible for this "conduit" safe harbor, the ISP must meet the following requirements:

- The ISP must not initiate the transmission or select either the material or the recipients. 17 U.S.C. § 512(a)(1)-(3).

- The transmission must be carried out through an automatic technical process. 17 U.S.C. § 512(a)(2).

- The material must not be maintained on the ISP’s system either for longer than reasonably necessary for the transmission to take place or in a manner ordinarily accessible to anyone other than anticipated recipients”. 17 U.S.C. § 512(a)(4).

- The material must be transmitted without modification of its content. 17 U.S.C. § 512(a)(5).

Unlike the "hosted content" safe harbor, the "conduit" safe harbor does not require either that the ISP lack knowledge or awareness of infringing activity or that it comply with the notice and takedown procedure. And, yet, virtually all of the takedown notices that colleges and universities receive involve just such "conduit" activity: students using file-sharing software on their own computers, which they connect to the Internet through their institutions’ networks.
Does that mean that colleges and universities can – or should – simply ignore both their students’ clearly infringing conduct and the multitude of notices from copyright owners complaining about it? The answer to that question is a matter of:

B. Policy

While it is tempting to simply throw those notices away and move on to something more productive, there are a number of reasons why that may not be the best, or even a very good, option. First, there has been relatively little litigation under the DMCA so far, and as a result the precise meaning of its many requirements is still open to argument. Are you sure that you have sufficiently “informed” your students of your termination policy and that you have “reasonably implemented” it? Have you affirmatively determined whether your system architecture adequately “accommodates” standard copyright protection technology? Do you know exactly how long infringing material rests on your system as it makes its way from sender to recipient? If not, you may not be eligible for the conduit safe harbor, and may instead be subject to the contributory infringement standard. Under that standard, knowledge is relevant, and a notice arguably constitutes sufficient knowledge. (Note, however, that loss of the safe harbor does not by itself make you liable for copyright infringement; the copyright owner still must establish the underlying claim. See CoStar Group v. Loopnet, Inc., 373 F.3d 544, 555 (4th Cir. 2004) (“It is clear that Congress intended the DMCA’s safe harbor for ISPs to be a floor, not a ceiling, of protection.”))

Second, even if you clearly are protected by the conduit safe harbor, your students are not, and they have virtually no other defense to a copyright infringement suit. Given the RIAA’s massive subpoena and litigation campaign, and the potentially millions of dollars of liability that even a casual file-sharer could face, do you feel any obligation to protect your students from themselves?

Third, Congress has been increasingly vocal about its displeasure with our perceived failure to “address these crimes aggressively”. Door to Door Piracy on University Campuses: Hearing before the Subcommittee on Courts, the Internet, and Intellectual Property, 108th Cong., 1st Sess. 6 (2003) (statement of Rep. Keller), available at <http://www.house.gov/judiciary/85286.PDF>, and increasingly sympathetic with the music industry. If we take a “not my problem” attitude in reliance on the DMCA, will Congress “fix” it with something much worse?
For all of these reasons, most institutions will find it preferable to pursue one or more of the following alternatives:

1. **Follow the notice and takedown procedure, or something like it, anyway.** Doing so will require time and effort, but, for the above reasons, it should be time and effort well spent. Moreover, the DMCA provides an additional immunity to ISPs for the “good faith” removal of or disabling of access to material claimed or believed to be infringing, which should minimize the risks of liability from the other direction. 17 U.S.C. § 512(g). Links to information about the DMCA procedures at several institutions are available at the end of this outline.

2. **Educate.** Not only is education a good idea generally, but it can also give us additional immunities even for the infringements of our employees in certain circumstances. See 17 U.S.C. § 512(e). Links to sample educational materials are listed at the end of this outline.

3. **Implement technical restrictions.** Some institutions have adopted bandwidth quotas – limiting users to a set number of bytes in or out during a given period – or bandwidth restrictions – slowing down the speed of transmissions – in an effort to reduce the significant bottlenecks and strains that file-sharing can cause our systems. Others have implemented “packet shaping” technology, which can distinguish between different types of traffic and give priority to those the institution considers most important – for example, e-mail and web traffic over file-sharing. See generally Scott Carlson, “Managing Bandwidth: Packet Shapers Control the Flow”, Chronicle of Higher Education, Jan. 30, 2004, at B7. While these restrictions generally have been implemented to preserve bandwidth and reduce costs, the consequent reductions in file-sharing also significantly reduce the legal risks associated with that activity. Still other institutions have installed filtering systems to block access to file-sharing altogether. See generally Jeffrey R. Young, “2 Universities Test Controversial Filtering Method to Block Illegal Trading of Music”, Chronicle of Higher Education, April 16, 2004, at A31. Links to additional information about these technologies are listed at the end of this outline.

4. **Harness market forces.** Cornell University recently instituted a usage-based billing model in an effort to bring the “irrational consumption” of
bandwidth under control. Under this model, known colloquially as "pay by the drink", each IP address is permitted up to 2 gigabytes of internet traffic per month for a flat fee of $3, with a surcharge of $.002 per megabyte over that. Cornell estimates that at least 80% of its users will never have to pay more than the basic monthly fee, but those who use the most bandwidth – including active file-sharers – may see significantly higher bills. Information on Cornell's program is available at <http://www.cit.cornell.edu/services/netrates/overview.html>.

5. **Offer alternatives.** Last academic year, Penn State and the University of Rochester entered into a blanket license with the new, legal Napster service, allowing their students unlimited (though "tethered") downloads from Napster’s catalog of nearly a million songs for free. In the first 24 hours that the service was available at Penn State, 3,000 students registered and downloaded 100,000 songs. More information about the program is available at <http://napster.psu.edu>. A number of additional institutions subsequently entered into similar arrangements with Napster or other such services, many of which began just this past fall. See Jeffrey R. Young, "Napster and 6 Colleges Sign Deals to Provide Online Music to Students", *Chronicle of Higher Education*, July 30, 2004, at A1; Brock Read, "Company Helps Professors Post Course Materials Online and Allows Students to Download Film", *Chronicle of Higher Education*, Feb. 6, 2004, at A25.

6. **Outsource.** In the latest alternative to surface, a few colleges have simply handed the responsibility for their residence hall networks over to third-party vendors, much as many colleges previously have done with cable television. See Vincent Kieman, "Outsourcing the Dorm Network", *Chronicle of Higher Education*, December 3, 2004, at A31. In so doing, they generally have been able to increase the amount of bandwidth available to their students while eliminating interference with their academic networks and in some cases reducing or capping costs – and, of course, passing the legal headaches off to someone else.

C. **Subpoenas**

Regardless of which of these approaches they choose, colleges and universities are increasingly likely to find themselves confronted with subpoenas from the RIAA seeking information about students engaged in file-sharing on the institution's networks.
The DMCA established a subpoena process through which copyright owners could obtain “information sufficient to identify the alleged infringer of the [copyright owners’] material” on an expedited basis, before even filing a lawsuit. 17 U.S.C. § 512(h). Through what is either, depending upon your point a view, a drafting error or a deliberate policy choice, however, that process is not available in “conduit” cases – which likely include 99.9% of all file-sharing. In re: Charter Communications, Inc., Subpoena Enforcement Matter, 2005 U.S. App. Lexis 31 (8th Cir.); Recording Industry Ass’n of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003), cert. denied, 125 S. Ct. 309 (2004).

Despite this setback, the RIAA can still obtain the information it needs by first filing individual “John Doe” lawsuits against alleged infringers and then serving normal litigation subpoenas on their ISPs – or on anyone else likely to have relevant information. To be sure, that process is more time-consuming, expensive, and cumbersome than the DMCA process, but it also allows the RIAA to obtain much more extensive information about the alleged infringers and offers those infringers little in the way of procedural or other protections. The scope of what is considered “relevant” for purposes of a litigation subpoena is quite broad, and claims to a First Amendment right to file-share anonymously have met with little sympathy from the courts. See, e.g., Sony Music Entertainment, Inc. v. Does 1-46, 326 F. Supp. 2d 556, 564-67 (S.D.N.Y. 2004) (“in contrast to many cases involving First Amendment rights on the Internet, a person who engages in P2P file sharing is not engaging in true expression. Such an individual is not seeking to communicate a thought or convey an idea. Instead, the individual’s real purpose is to obtain music for free... In sum, defendants’ First Amendment right to remain anonymous must give way to plaintiffs’ right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.”) (citations omitted).

A college or university that receives a subpoena for such information should first verify that it is a litigation, not DMCA, subpoena and that it was issued by a court having jurisdiction over the institution. If so, the institution will be required to comply, although, to the extent that the information sought pertains to a student, the institution will also be required to comply with FERPA by giving the student “reasonable” advance notice before turning the information over. See Elektra Entertainment Group, Inc. v. Does 1-6, Civil Action No. 04-1241, unreported (E.D. Pa. Oct. 13, 2004). The institution has no legal obligation to contest the subpoena on the student’s behalf, and, given the
educational efforts that most colleges and universities have long since implemented on this subject, precious little moral obligation to do so, either.

III. CAN-SPAM

Since January 1, 2004, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, the federal government’s effort to bring unwanted “spam” e-mail to a halt, has been in effect, if not exactly effective. Although the intent of that statute was quite clear from the start — highlighted by its acronym, CAN-SPAM — little else about it has been, including in particular whether it applies to messages sent by nonprofit organizations such as colleges and universities.

The language of the statute offered considerable hope that we would be exempt from its provisions altogether. It defined the key term for what is regulated, “commercial electronic mail message”, as a message “the primary purpose of which is the commercial advertisement or promotion of a commercial product or service”, 15 U.S.C. § 7702(2)(A) (emphasis added), suggesting that nonprofits were not within its scope.

Unfortunately, however, new regulations from the Federal Trade Commission that just took effect on February 18 make it clear that “noncommercial” and “nonprofit” are not the same thing: “CAN-SPAM does not set up a dichotomy between “commercial” and “nonprofit” messages. Rather, it focuses on messages whose primary purpose is to sell something, as distinguished from ‘transactional or relationship messages,’ informational and editorial messages, and (relevant to nonprofit entities) messages seeking a charitable contribution.” 69 Fed. Reg. 50091, 50100 (Aug. 13, 2004) (emphasis in original). Thus, the FTC concluded, “[i]t is possible that a message from a nonprofit could meet the definition of “commercial electronic mail message” (e.g., an e-mail message sent by a nonprofit hospital offering medical screening in exchange for a fee). There is no reason that recipients of such an e-mail message should forfeit the protections afforded by CAN-SPAM.” 70 Fed. Reg. 3110, 3112 (Jan. 19, 2005).

On the other hand, it seems likely that few e-mail messages sent out by nonprofit entities will meet the statutory definition. Under the new regulations, an e-mail will be deemed to have a “primary purpose” that is “commercial” only if it either:

(a) consists “exclusively of the commercial advertisement or promotion of a commercial product or service”; or
(b) contains both "commercial" and "transactional or relationship" information and

(i) a "recipient reasonably interpreting the subject line of the ... message would likely conclude" that the message is commercial in nature or

(ii) the transactional or relationship content does not appear in at least substantial part at the beginning of the message; or

(c) contains both "commercial" and other, nontransactional and nonrelationship content and

(i) a recipient "reasonably interpreting the subject line of the ... message would likely conclude" that the message is commercial in nature or

(ii) a "recipient reasonably interpreting the body of the message would likely conclude" that it is commercial in nature.

16 C.F.R. § 316.3(a) (emphasis added). Thus, it appears likely that the only college and university e-mail messages likely to fall within the ambit of the statute are those whose sole or primary purpose is to promote alumni travel opportunities, athletic tickets, logoed apparel, and the like. Note, however, that the statute applies equally to both bulk messages and messages addressed to a single individual.

For those messages that are subject to the statute, the requirements are relatively few and not particularly burdensome: generally speaking, the messages must include a clear and conspicuous identification that the message is an advertisement or solicitation (which need not necessarily be in the subject line), an effective opt-out mechanism for recipients who do not want to receive further such messages, and a valid return e-mail address (or similar "Internet-based mechanism" for replies) and physical postal address for the sender. In addition, the messages must not include false or misleading "headers", subject lines, or content. 15 U.S.C. § 7704. Even without CAN-SPAM, these requirements would be good customer relations practices for reputable businesses.

One final note: Although the statute applies to nonprofits, the FTC has no enforcement jurisdiction against nonprofits, and unhappy recipients of spam have no private right of action. Any enforcement action against nonprofit colleges and universities would have to be brought by a state attorney general or an "adversely affected" ISP – neither of which seems likely, absent egregious circumstances.
Additional detail on the statute is available in the resources listed at the end of this outline.

IV. Cybersecurity, Cybernegligence, and Cyberliability

Scarce a day passes now without new reports of computer security breaches, and colleges and universities, which have extensive but diffuse and often casually managed systems, are not infrequently the target. At the same time, and perhaps in part as a result, an increasing number of new privacy-oriented statutes – GLBA, HIPAA, and more – is upping the stakes for the owners and operators of those compromised systems. Most frightening of all, however, may be the prospect of simple common law negligence actions for “allowing” such intrusions to happen.

While it is impossible to quantify just how much security is enough to satisfy the negligence standard, it is clear that colleges and universities can no longer afford to ignore the issue. At a minimum, they should carefully scrutinize, and continue to monitor, their security practices to ensure they are up to date and in line with “industry standards”, as well as plan now for how they would handle a serious incident. Doing so will almost certainly require the designation of a team including representatives from your information technology, law enforcement, legal, risk management, and public relations departments, among others. Further information on how to go about the task is available in the resources listed at the end of this outline.

V. Additional Resources

A. File-Sharing

1. Law

   Full text of the DMCA provisions concerning ISP liability:
   <http://www4.law.cornell.edu/uscode/17/512.html>

   Copyright Office summary of the DMCA:

   ACE white paper on file-sharing:
   <http://www.acenet.edu/washington/legalupdate/2003/P2P.pdf>
2. **Policies, Procedures, and Educational Materials**

ACE summary of institutional responses:
<http://www.acenet.edu/hena/pdf/P2P2.pdf>

Colby College:
<http://www.colby.edu/info.tech/news/fall03copyright.html>

Cornell University:
<http://www.cit.cornell.edu/oit/policy/memos/dmca.html>

Hamilton College:
<http://www.hamilton.edu/college/its/copyright>

Saint Louis University:
<http://www.slu.edu/DMCA>

UCLA:
<http://www.today.ucla.edu/2004/040511news_files.html>

University of Colorado:
<http://www.colorado.edu/copyright/index.html>

University of Texas:
<http://www.utsystem.edu/ogc/intellectualproperty/dmcaisp.htm>

3. **Technical Restrictions**

Columbia University's network bandwidth quota:

UC Berkeley's bandwidth limitation FAQ:
<http://www.rescomp.berkeley.edu/bernice/bandwidth/faq>

University of Texas's usage and bandwidth limitations:
<https://management.pna.utexas.edu/faqs/faq?band.html>
Joint Committee of the Higher Education and Entertainment Communities Technology Task Force:
<http://www.educause.edu/issues/rfi>

4. General Background

Copyright Issues in Digital Media (Congressional Budget Office analysis):
<http://www.cbo.gov/ftpdocs/57xx/doc5738/08-09-Copyright.pdf>

Protecting Creative Works in a Digital Age
<http://judiciary.senate.gov/special/feature.cfm>

Copyright and Digital Media in a Post-Napster World:
<http://cyber.law.harvard.edu/media/wp2005>

How Not to Get Sued by the RIAA for File-Sharing:
<http://www.eff.org/IP/P2P/howto-notgetsued.php>

RIAA v. The People:
<http://www.eff.org/IP/P2P/riaa-v-thepeople.php>

Subpoenadefense.org:
<http://www.subpoenadefense.org>

B. CAN-SPAM

Full text of the statute

Independent Sector summary
<http://www.independentsector.org/programs/gr/spam.htm>

Northeastern University compliance guidelines
<http://www.help.neu.edu/can-spam_0704.pdf>

C. Cybersecurity

EDUCAUSE Security Task Force
<http://www.educause.edu/security>
Computer and Network Security in Higher Education
<http://www.educause.edu/LibraryDetailPage/5667?ID=PUB7008>

Liability for Negligent Security: Implications for Policy and Practice
(excerpt from above book)
<http://www.educause.edu/fr/library/pdf/pub7008h.pdf>

IT Security for Higher Education: A Legal Perspective

CERT Coordination Center
<http://www.cert.org>

CERT: How Much Security is Enough?
<http://www.cert.org/governance/adequate.html>
SAMPLE LETTER CONCERNING MP3 FILE-TRADING (January 2005)

To all faculty, staff, and students:

We are writing to alert you to some important recent developments in the Recording Industry Association of America’s continuing campaign against the use of peer-to-peer file-sharing programs, such as Kazaa, LimeWire, and BitTorrent, for the purpose of trading copyrighted music. As you may be aware, the RIAA, which constantly monitors file-sharing networks, has filed lawsuits against more than 7,700 users of file-sharing programs, has settled approximately 1,475 of those suits for an average of $3,000-$5,000 each, and has vowed to continue filing hundreds of additional such suits each month. To our knowledge, no one at RISD has been named a defendant in any of those suits, but, over the past several months, RISD has received six separate notices from the RIAA alleging that specific individuals have engaged in illegal file-sharing on our network. Such notices are often the precursor to lawsuits.

These tactics may seem heavy-handed, but the RIAA is correct that most music 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 do it for free, you may be “publicizing” the artist in the process, and the music industry’s business practices and ethics may themselves be worthy of criticism, but none of those things 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 would 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.

The use of file-sharing programs has significant practical implications as well. File-sharing is bandwidth-intensive and thus can significantly interfere with all users’ ability to perform college-related work. Indeed, at times, file-sharing traffic has consumed our entire available bandwidth, leaving no capacity at all for anything else. In addition, the files available through file-sharing frequently are infected with computer viruses. We believe that the virus infestations that brought our network to a halt several times last fall may have been associated with file-sharing traffic.

In the coming months, we will be taking steps to address these issues further, which may include imposing additional technical restrictions on file-sharing. To the extent that we learn of specific individuals engaged in illegal file-sharing, we will enforce our computer use policy, which prohibits the use of RISD computer resources to engage in copyright infringement. Under that policy, repeat infringers can be deprived of network access. We also will be discussing with the Student Alliance the possibility of making a subscription-based music service available to the campus, as some other schools have done. And if there is sufficient interest, we will hold an open forum on the general topic in the near future.

We appreciate your consideration of this information.

Joe Deal
Provost

Ned Dwyer
Associate Provost for Student Affairs

Kazuhiko Hasegawa
Associate Vice President for Information Technology

18