FACE THE MUSIC:
THE LAW AND POLICY OF FILE SHARING

30th Annual National Conference on Law and Higher Education
Stetson University College of Law

February 21-24, 2009

Steven J. McDonald
General Counsel
Rhode Island School of Design

I. Introduction

. . . A plague o' both your houses!
They have made worms' meat of me . . .

– William Shakespeare, Romeo and Juliet, Act 3, Scene 1

With these, his last words, Romeo's friend Mercutio cursed both the Montagues and the Capulets, whose "ancient feud" resulted not only in great tragedy for themselves, but also in his own, unnecessary, and "collateral" death. Today, colleges and universities likewise find themselves on a battleground that is not of their own making, but on which they may suffer as much or more damage as the actual combatants: the file-sharing war.

That war began in 1999, when Northeastern University freshman Shawn Fanning created Napster and sent it forth into the world. 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 Internet users, who were mightily tempted by the new-found ability to acquire music for free; 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 lawyer gladiators 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 war against file sharing bogged down in the face of these developments, the music industry opened up new fronts. At first, it attempted to block use of file-sharing software through massive deployment of the DMCA's "notice and takedown" procedure. When that effort ran into legal obstacles and yielded few concrete results, the industry's trade association, the Recording Industry Association of America, began to sue the (alleged) users themselves, including a number of college and university students, not to mention grandmothers (one deceased) who allegedly were trading rap music, Macintosh owners whose computers were

incapable of running file-sharing software, and at least one 12-year-old – reportedly more than 30,000 defendants to date. See generally David Kravets, "File Sharing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation," Wired Threat Level Blog (Sept. 4, 2008), available at <http://blog.wired.com/ 27bstroke6/2008/09/proving-file-sh.html>. The industry also began actively lobbying Congress to impose substantial new responsibilities and liabilities on almost everyone involved in the process of file sharing, no matter how remotely or tangentially, and the Bush administration to make file sharing a top *criminal* priority.

The industry eventually did win its battle with the file-sharing software providers, when the Supreme Court ruled, in MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 919 (2005), that "one who distributes a device with the object of promoting its use to infringe copyright . . . is liable for the resulting acts of infringement by third parties." But by then, with the software already universally available, it was too late. And with file sharing continuing to flourish, the industry is now seeking to conscript into its service the colleges and universities and other ISPs that provide the "pipelines" that make file sharing possible, sending them a surge of "pre-litigation settlement letters" that in effect seek to require them to act as the industry's process servers and enforcers.

At the same time, file sharers – who for the most part are unquestionably engaged not only in massive copyright infringement, but also in massive self-denial – have not surrendered. With few, if any, substantive defenses to assert, they have fought back with largely procedural stalling tactics and "no proof" arguments that in many cases even a tobacco industry spokesperson would be embarrassed to make. And, much like the industry itself, they have sought to shift the costs and burdens of asserting their position onto their ISPs, including colleges and universities in particular. See, e.g., Ray Beckerman, Open Letter to Colleges and Universities Whose Students Have Been Targeted by the RIAA (2007) ("This is an historic opportunity for you to take steps to make the RIAA's litigation campaign more of a level playing field. . . . Accordingly, we believe you should oppose the RIAA's application for an order of discovery."), available at <http://recordingindustryvspeople.blogspot.com/2007/03/open-letter-to-universities-whose.html>; Joseph A. Hazelbaker, Letter to Ohio University (2007) ("Even if the subpoena is colorably lawful, Ohio University has a greater responsibility to its students . . . . Ohio University is in the best position to question both the propriety of the subpoena and the underlying complaint, and should do so before compromising student private information."), available at <www.ilrweb.com/viewILRPDF.asp?filename=capitol_does1-10_070523JHtoBN>.

College and university administrators caught in the middle of this war are conflicted as to what to do. On the one hand, colleges and universities produce substantial intellectual property themselves and understand the need to protect – and educate about – 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. Then, too, it is clear that some of the students the RIAA is targeting with its blunderbuss are not in fact file sharers, and few, if any, of those have the resources and knowledge necessary to defend themselves effectively. At a more practical level, rapidly increasing demands for bandwidth and costs of responding to DMCA notices and pre-litigation settlement letters are stretching already-thin institutional budgets. And, of course, colleges and universities wish to avoid liability, both legal and political.

The question, then, is what should we do – or, put another way, how can we avoid becoming casualties in the crossfire?

II. 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:

A. 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.

Copyright law, however, 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) (discussing with approval, though not expressly ruling upon, the "space shifting" rationale); RIAA, For Students Doing Reports (undated) ("Record companies have never objected to someone making a copy of a CD for their own personal use. We want fans to enjoy the music they bought legally."), available at <www.riaa.com/faq.php>. 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" that 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 ("Diamond . . . [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."); MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 923 (2005) ("the vast majority of users' downloads are acts of infringement").

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 work infringed in "willful" cases, 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. See, e.g., United States v. Repp, 464 F. Supp. 2d 788 (E.D. Wisc. 2006) (18-year-old uploader to "Elite Torrents" sentenced to six months of home confinement and three years of probation, ordered to conduct 25 hours of community service during each year of supervision, and fined $3,600). 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 at <www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>.

BMG Music v. Gonzalez, 2005 WL 106592 at *1 (N.D. Ill.), the first of the RIAA's cases to be litigated to judgment, starkly demonstrates these principles. Defendant Cecilia Gonzalez, who admitted to having downloaded 30 songs, argued that doing so was "fair use," on the theory that she was "just sampling" music before deciding whether to purchase it, and that, in any event, she was an "innocent" infringer because she did not know that what she did was illegal. Wholly unimpressed, the court granted summary judgment against her, holding that her fair use argument was "without merit" and that "ignorance is no defense to the law." The court then proceeded to award damages in the amount of $22,500, representing the *minimum* statutory penalty of $750 per each song infringed. Looked at from another angle, that amount also represented approximately 750 times what she would have paid had she bought those songs on iTunes – and more than three-fourths of her entire annual salary as a secretary at the time, before she was laid off. See Bob Mehr, "Gnat, Meet Cannon," Chicago Reader, Feb. 4, 2005, available at <www.chicagoreader.com/TheMeter/050204.html>.

Gonzalez's arguments fared even less well, and met with even stronger rhetoric, on appeal:

> Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying "fair use" if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute. Nor can she defend by observing that other persons were greater offenders; Gonzalez's theme that she obtained "only 30" . . . copyrighted songs is no more relevant than a thief's contention that he shoplifted "only 30" compact discs, planning to listen to them at home and pay later for any he liked.

430 F.3d 888, 891 (7th Cir. 2005).

Moreover, last fall, in the first of the RIAA's cases to go to trial, the jury took just five minutes to conclude that defendant Jammie Thomas not only had shared 24 songs illegally, but that she had done so "willfully," notwithstanding her protestations of complete innocence and absolute bewilderment at having been sued. "She's a liar," one of the jurors was later quoted as saying. David Kravets, "RIAA Juror: 'We Wanted to Send a Message,'" Wired Threat Level

Blog (Oct. 9, 2007), available at <blog.wired.com/27bstroke6/2007/10/riaa-juror-we-w.html>. After five more hours of deliberation, the jury awarded damages in the amount of $222,000 – a breathtaking $9,250 per song; two of the jurors had wanted to award the statutory maximum of $150,000 per song. Id.[1] While the Court subsequently ordered a retrial, calling on Congress to amend a statute authorizing damages that are "wholly disproportionate," "unprecedented," and "oppressive," Capitol Records, Inc. v. Thomas, 579 F. Supp. 2d 1210, 1227, 1228 (D. Minn. 2008), the fact remains that such damages are in fact authorized under current law.

The courts have also been largely unimpressed with the various procedural arguments, counterclaims, and other defenses that alleged file sharers have raised, including:

- Failure to state a claim upon which relief may be granted. See, e.g., London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 176-77 (D. Mass. 2008) ("The defendants may still argue that they did not know that logging onto the peer-to-peer network would allow others to access these particular files, or contest the nature of the files, or present affirmative evidence rebutting the statistical inference that downloads occurred. But these are substantive defenses for a later stage. . . . [Plaintiffs] are not required to win their case in order to serve the defendants with process."); Arista Records, LLC v. Greubel, 453 F. Supp. 2d 961, 964-66 (N.D. Tex. 2006) ("Greubel contends that the complaint must be dismissed because it consists of ambiguous, vague, and conclusory allegations and lacks sufficient specificity to state a claim for copyright infringement. He complains that the plaintiffs have filed a formulaic pleading that is identical to numerous copyright-infringement complaints that have been filed nationwide by recording companies and other copyright holders against individual computer users. . . . Greubel finally contends that the complaint must be dismissed in its entirety because Plaintiffs have not alleged by what specific acts and at what specific times he infringed their copyrights. . . . Plaintiffs need not list each and every individual act of infringement of their exclusive rights at this preliminary stage of the proceedings.").

- Rule 11 violations. See, e.g., Atlantic Recording Corp. v. Heslep, 2007 WL 1435395 at *6-*8 (N.D. Tex.) ("Plaintiffs' attorneys brought this lawsuit not for the purposes of harassment or to extort Heslep as she contends, but, rather, to protect their clients' copyrights from infringement and to help their clients deter future infringement. The evidence uncovered from MediaSentry's investigation shows that Plaintiffs' allegation of Heslep's alleged copyright infringement have [sic] evidentiary support and will likely have [sic] more evidentiary support through further investigation and discovery. . . . Taking aggressive action, as Plaintiffs have, to defend their copyrights is certainly not sanctionable conduct under Rule 11. . . . Finally, the Court concludes that sanctions are appropriate in this case, but not against Plaintiffs' attorneys. Rather, the Court concludes that sanctions are appropriate against Heslep's attorney, Thomas Kimble. Among the

[1] The movie industry has also now won at least one case at trial. In Paramount Pictures Corp. v. Davis, 2006 WL 2092581 (E.D. Pa.), the court awarded $50,000 in statutory damages and a permanent injunction against a self-employed computer consultant who had made a single movie available through eDonkey.

many prohibitions contained in Rule 11, is one prohibiting an attorney from filing a motion for the purposes of harassment and unnecessarily increasing the cost of litigation. . . . Kimble's frivolous motion for sanctions clearly does both. . . . For the foregoing reasons, Heslep's motion for sanctions is DENIED. It is further ORDERED that Kimble, personally, pay Plaintiffs' reasonable costs, including attorney's fees, incurred in defending against his client's baseless motion for sanctions.").

- Inappropriate discovery. See, e.g., Warner Brothers Records, Inc. v. Souther, 2006 WL 1549689 at *2-*4 (W.D.N.C.) ("All of the motions now pending before the court have as their genesis defendant's assertion that she did not commit the alleged acts and that if someone else in her home did, she cannot be held liable for such conduct. Defendant also contends that plaintiffs are not entitled to the names and addresses of those others who may have had access to her computer, contending that there exists a federal privilege from disclosing such matters inasmuch as they may involve minors. . . . [D]efendant must realize that her (1) assertion of innocence or (2) her defense that persons other than she may have engaged in such conduct, may be challenged by plaintiffs not just at trial or in response to a motion for summary judgment, but through plaintiffs seeking discovery. . . . Simply put, plaintiffs have an absolute right to know who may have unlawfully infringed their copyrights, and defendant's failure to provide such information to plaintiffs or properly interpose objections is without legal support.").

- Failure to join an indispensable party. See, e.g., Interscope Records v. Duty, 2006 WL 988086 at *2 (D. Ariz.) ("Duty also argues that the alleged infringement would not have been possible without the use of Kazaa, and therefore the owner of Kazaa, Sharman Networks, Ltd. ('Sharman'), is a necessary and indispensable party to this suit. We disagree. The Recording Companies may have a viable claim against Sharman for direct, contributory or vicarious infringement. Furthermore, following this action, Duty may have a viable claim against Sharman for contribution. However, the possibility of related third-party liability does not preclude us from according complete relief among those already named as parties, nor does it represent sufficient harm to either Sharman or Duty to require joinder.") (citation omitted).

- Invasion of privacy. Id. at *3 ("More specifically, it appears that Duty claims that the Recording Companies committed this tort by accessing her Kazaa share folder, which is reproduced as exhibit B to the complaint. The Recording Companies argue that Duty fails to state a claim upon which relief can be granted because the information in the share file is public, and therefore, there is no seclusion. Duty does not dispute this fact; she merely argues that she did not put the sound recordings in the share file. She argues that Kazaa did so automatically. However, whether Duty or Kazaa acted, it is undisputed that the share file is publically [sic] available, and therefore Duty cannot show that the Recording Companies intruded upon her private affairs.").

- Abuse of process. Id. at *4 ("Duty claims that this is one case in thousands where the Recording Companies are suing individual users of peer-to-peer networks such as Kazaa in an effort to frighten users away from the networks, thereby putting the networks out of business. This might be true. . . . It is not, however, an abuse of the legal process to organize a large-scale legal assault on small-scale copyright infringers that together cause devastating financial losses. Moreover, it is not an abuse of the legal process if the

Recording Companies' goal in bringing these actions is to scare would-be infringers into complying with federal law, and thereby prevent the networks that allegedly facilitate the alleged infringement from doing so.").

- Copyright misuse. See, e.g., Interscope Records v. Kimmel, 2007 WL 1756383 at *5 n.3 (N.D.N.Y.) ("The viability of this defense is dubious at best. Defendant claims that Plaintiffs' concerted efforts to enforce their copyrights through joint investigation and litigation somehow violates [sic] the antitrust laws . . . and constitutes fraudulent conduct. Of course, enforcing a valid copyright, without more, is not copyright misuse.").

Moreover, the courts have on more than one occasion imposed default judgments as a spoliation sanction on defendants who had wiped their hard drives clean or otherwise destroyed evidence after being sued. See, e.g., Atlantic Recording Corp. v. Howell, 2008 WL 4080008 at *2-*3(D. Ariz.) ("It is implausible that Howell would destroy the only evidence that could exonerate him simply to remove KaZaA from his computer. It is entirely incredible that his systematic and pervasive destruction of every last bit of evidence pertaining to the claims against him was simply an effort to tidy up his computer. The timing and character of Howell's actions show that they were deliberately calculated to conceal the truth and that he willfully destroyed evidence to deceive the court. . . . Such circumstances demand the imposition of a default judgment against Howell. . . . The requested statutory damages of $750 per sound recording, a total of $40,500, will therefore be awarded."); Arista Records, LLC v. Tschirhart, 241 F.R.D. 462, 466 (W.D. Tex. 2006) ("In this case, defendant's conduct shows such blatant contempt for this Court and a fundamental disregard for the judicial process that her behavior can only be adequately sanctioned with a default judgment. No lesser sanction will adequately punish this behavior and adequately deter its repetition in other cases.").

In a few, limited situations, however, the defendants have prevailed, at least temporarily:

- Inappropriate joinder of "John Doe" defendants. See, e.g., Fonovisa, Inc. v. Does 1-9, 2008 WL 919701 at *6 (W.D. Pa.) ("Other than alleging that Defendants used the same peer-to-peer network to access the internet and download and/or distribute the copyrighted recordings through the same ISP, Carnegie Mellon University, the Plaintiffs here have failed to allege any other facts to connect the Defendants. None of the Defendants downloaded and/or distributed the same copyrighted recordings belonging to the same set of Plaintiffs, and each of the Defendants accessed a different number of audio files on different dates. . . . Therefore, given the different factual contexts of the alleged infringement for each Defendant and the absence of any evidence showing joint action by Defendants, other than their use of the same peer-to-peer network to access the copyright recordings and the same ISP, the Court finds that Plaintiffs have failed to satisfy the requirements for permissive joinder under Rule 20(a). Accordingly, the Court will order the claims against Does # 1-2, and 4-9, be severed."); LaFace Records, LLC v. Does 1-38, 2008 WL 544992 at *3 (E.D.N.C.) ("In similar cases, other courts have commonly held that where there is no assertion that multiple defendants have acted in concert, joinder is improper."). See also Arista Records, LLC v. Does 1-27, 2008 WL 222283 at *6 n.5 ("[P]aragraph 20 of the complaint alleges that the claims against all defendants arise from the 'same series of transactions or occurrences' because the Doe Defendants have the same ISP (the University of Maine) and all engaged in file-sharing over the Internet using that ISP. The complaint wants, however, any allegation of

concerted conduct. . . . In my view, the Court would be well within its power to direct the Plaintiffs to show cause why they have not violated Rule 11(b) with their allegations respecting joinder. Separately, the Court may sever defendants sua sponte, pursuant to Rule 21, although dismissal of the action is not authorized. I appreciate that increased costs may redound to the defendants' detriment eventually, but it is difficult to ignore the kind of gamesmanship that is going on here with respect to joinder. . . . These plaintiffs have devised a clever scheme to obtain court-authorized discovery prior to the service of complaints, but it troubles me that they do so with impunity and at the expense of the requirements of Rule 11(b)(3) because they have no good faith evidentiary basis to believe the cases should be joined.").

- Attorney fees. See, e.g., Atlantic Recording Corp. v. Andersen, 2008 WL 2536834 (D. Ore. 2008) (awarding defendant $107,834 in attorney fees and costs when record company itself dismissed its case against her after two years of litigation); Capitol Records, Inc. v. Foster, 2007 WL 1223826 at *4 (W.D. Okla.) ("The plaintiffs assert that had the case continued, they would have proved their secondary liability claims. Specifically, they contend they would have been able to show that the defendant knew or 'should have known' that her Internet account was being used by a member of her household to infringe the plaintiffs' copyrights. That may be so. The plaintiffs, however, chose not to pursue the claim. The Court finds disingenuous the plaintiffs' assertion that 'had they been given an opportunity, they would have been able to prove vicarious infringement.' The plaintiffs were in no way deprived of an opportunity to prove their allegations. They moved, voluntarily, to dismiss their claims after the defendant had already made a substantial investment toward defending against those claims. . . . The plaintiffs contend that beginning on April 21, 2005, they gave the defendant 'repeated opportunities to end this litigation without paying anything.' Of course, that is not true. By the time the plaintiffs offered to dismiss their claims against the defendant, she had made a considerable litigation investment, and would have been required to pay those expenses already incurred. Furthermore, the plaintiffs offered merely to dismiss their claims without prejudice, thus leaving the defendant exposed to continued litigation in the matter. The plaintiffs also persist in conflating the defendant's daughter's infringement with liability on the part of the defendant. While the plaintiffs obtained a default judgment against the daughter, there has never been any finding of liability on the part of the defendant. On the contrary, she prevailed against the plaintiffs' claims."). But cf. Interscope Records v. Leadbetter, 2007 WL 2572336 at *4 (W.D. Wash.) ("In sum, Ms. Leadbetter did not obtain a judgment on the merits or a court-ordered consent decree in her favor, nor did she otherwise prevail on an issue in this case. Although the claims against her were dismissed, they were voluntarily dismissed without prejudice on Plaintiffs' motion. Under these circumstances, Ms. Leadbetter has not provided the Court with persuasive authority to support her position that she is a 'prevailing party' in this case . . . .").

Moreover, and perhaps more important, courts have begun to question the RIAA's theory that it is an infringement simply to make files "available" for others to download, even if no such downloading ever occurs:

> The court agrees with the great weight of authority that [the distribution right] is not violated unless the defendant has actually distributed an unauthorized copy of the

> work to a member of the public. The statute provides copyright holders with the exclusive right to distribute "copies" of their works to the public "by sale or other transfer of ownership, or by rental, lease, or lending." Unless a copy of the work changes hands in one of the designated ways, a "distribution" . . . has not taken place. Merely making an unauthorized copy of a copyrighted work available to the public does not violate a copyright holder's exclusive right of distribution.
>
> . . . [E]vidence that a defendant made a copy of a work available to the public might, in conjunction with other circumstantial evidence, support an inference that the copy was likely transferred to a member of the public. On its own, however, it does not prove that the copy changed hands. It only shows that the defendant attempted to distribute the copy, and there is no basis for attempt liability in the statute, no matter how desirable such liability may be as a matter of policy.

Atlantic Recording Corp. v. Howell, 554 F. Supp. 2d 976, 983-84 (D. Ariz. 2008) (citations omitted). See also Capitol Records, Inc. v. Thomas, 579 F. Supp. 2d 1210, 1226 (D. Minn. 2008) ("Liability for violation of the exclusive distribution right found in § 106(3) requires actual dissemination."). Should this position hold – which it appears likely to do – it will not stop the RIAA from proceeding, but it will require the RIAA to do more work to file and prove its case.

B. 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, KaZaA, LimeWire, Grokster, and others focused their defenses on the second and third elements. In doing so, they relied in large part on Sony Corp. v. Universal City Studios, 464 U.S. 417 (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 such general awareness was not enough: "[T]he sale of copying equipment . . . 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.

In MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), however, the Supreme Court rejected this "Sony defense" as largely irrelevant to the facts of the file-sharing case at hand:

> *Sony's* rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law. . . . For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential. Accordingly, just as *Sony* did not find intentional inducement despite the knowledge of the VCR manufacturer that its device could be used to infringe, mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.

Id. at 934-37 (footnote and citation omitted).

Under this standard, there was no real question but that Grokster and other producers of file sharing software, whose entire business models were expressly built on promoting and profiting from infringement by their users, were liable, and virtually all of them quickly shut down – at least at the *corporate* level. (Kazaa moved its operations to Vanuatu for "tax reasons.") The software itself, which by then was in nearly universal distribution, continued to operate unimpeded.

C. 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) (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.[2] Two of those safe

---

[2] Note that failure to fall within the safe harbors does not by itself make an ISP liable for copyright infringement; the copyright owner still must establish the underlying claim, and there are other potential defenses available under general copyright principles. See Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1158 n.4 (9th Cir. 2007) ("[T]he DMCA does not change copyright law; rather, 'Congress provided that [the DMCA's] limitations of liability apply if the

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

---

provider is found to be liable under existing principles of law.' As a result, '[c]laims against service providers for direct, contributory, or vicarious copyright infringement, therefore, are generally evaluated just as they would be in the non-online world.'") (citations omitted); 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."); Tur v. YouTube, Inc., 2007 WL 1893635 at *2 (C.D. Cal.) (The DMCA "does not purport to create separate standards for assessing claims of copyright infringement against online entities, but rather provides a partial defense thereto upon a showing that all of the statutory prerequisites . . . are met."); Fatwallet, Inc. v. Best Buy Enterprises Services, Inc., 2004 WL 793548 at *2 (N.D. Ill.) ("Nothing in the DMCA . . . creates liability for the ISP beyond that which already exists under copyright law generally. An ISP suffers no adverse consequences under the DMCA for its failure to abide by the notice. It is free to thumb its nose at the notice and it will suffer no penalty nor increased risk of copyright liability.")

Moreover, as the Ninth Circuit recently noted in Perfect 10, Inc. v. Visa Int'l Service Ass'n, 494 F.3d 788, 806-10 (9th Cir. 2007), being a "but for" cause of online copyright infringement is not in itself a sufficient basis for imposing liability:

> *Grokster* does not stand for the proposition that just because the services provided by a company help an infringing enterprise generate revenue, that company is necessarily vicariously liable for that infringement. Numerous services are required for the third party infringers referred to by Perfect 10 to operate. In addition to the necessity of creating and maintaining a website, numerous hardware manufacturers must produce the computer on which the website physically sits; a software engineer must create the program that copies and alters the stolen images; technical support companies must fix any hardware and software problems; utility companies must provide the electricity that makes all these different related operations run, etc. All these services are essential to make the businesses described viable, they all profit to some degree from those businesses, and by withholding their services, they could impair – perhaps even destroy – the commercial viability of those business. But that does not mean, and *Grokster* by no means holds, that they are all potentially liable as vicarious infringers. Even though they have the "right" to refuse their services, and hence the literal power to "stop or limit" the infringement, they, like Defendants, do not exercise sufficient control over the actual infringing activity for vicarious liability to attach. . . . We decline to create any of the radical new theories of liability advocated by Perfect 10 . . . .

See also Parker v. Google, Inc., 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006), aff'd, 242 Fed. Appx. 833 (3d Cir. 2007) ("When an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition is missing."); Field v. Google, Inc., 412 F. Supp. 2d 1106 (D. Nev. 2006) (discussing general infringement, implied license, and fair use principles).

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).

Under the first of these criteria, "a service provider 'implements' a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications. The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright." Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1109 (9th Cir. 2007) (citations omitted). Moreover, "[t]o identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement," id. at 1111, nor need it undertake factual investigations or make legal determinations when the situation is unclear, id. at 1112-14. "The DMCA notification procedures place the burden of policing copyright infringement – identifying the potentially infringing material and adequately documenting infringement – squarely on the owners of the copyright." Id. at 1113. See generally Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004); Io Group, Inc. v. Veoh Networks, Inc., 2008 WL 4065872 (N.D. Cal.); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

As for the second criterion, "'[s]tandard technical measures' refers to a narrow group of technology-based solutions to online copyright infringement," Perfect 10, Inc. v. CCBill, LLC, 488 F.3d at 1115, that "(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks," 17 U.S.C. § 512(i)(2). Few, if any, such measures have yet been developed.

In addition to these two general requirements, the ISP must then meet specific additional requirements for each safe harbor:

1. "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)(i)-(ii). General awareness that file sharing is occurring somewhere on the ISP's system is not enough, Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004), and even "red flags" about specific materials may not suffice, Perfect 10, Inc. v. CCBill, LLC, 488 F.3d at 1113-14.

- If the ISP does obtain such knowledge or awareness, the ISP must "expeditiously" remove or disable access to the infringing material. 17 U.S.C. § 512(c)(1)(A)(iii).

- 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). See generally Perfect 10, Inc. v. Visa Int'l Service Ass'n, 494 F.3d 788, 802-06 (9th Cir. 2007); Perfect 10, Inc. v. CCBill, LLC, 488 F.3d at 1117-18; Ellison v. Robertson, 357 F.3d at 1078-79. An ISP is not required to structure its service "to prevent infringing activity from occurring on its site" or, if it cannot do so "given the current volume of its business, . . . to either hire more employees or to decrease its operations and limit its business to a manageable number of users." Io Group, Inc. v. Veoh Networks, Inc., 2008 WL 4065872 at * 20 (N.D. Cal.) (Rejecting plaintiff's "not-so-subtle suggestion . . . that, if Veoh cannot prevent infringement from ever occurring, then it should not be allowed to exist. . . . The DMCA was intended to facilitate the growth of electronic commerce, not squelch it.").

- 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). See generally Perfect 10, Inc. v. CCBill, LLC, 488 F.3d at 1112-13.

2. 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). (Ironically – or intentionally? – use of the various blocking and filtering software being promoted by the music industry, such as Audible Magic, could arguably disqualify an ISP from relying on this safe harbor.) However, the legislative history of the DMCA indicates that "'selection of the material' . . . means the editorial function of determining what material to send, or the specific sources of material to place on-line," H.R. Rep. No. 105-551, pt. 2, at 51 (1996), and is "not intended to discourage the service provider from monitoring its service for infringing material," H.R. Rep. No. 105-796, at 73 (1996).)

- 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). See generally Ellison v. Robertson, 357 F.3d at 1081 (14-day availability of USENET posting on AOL was "'transient' and 'intermediate' within the meaning of § 512(a)").

- 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 and pre-litigation settlement letters 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 and letters from copyright owners complaining about it? The answer to that question is a matter of:

III. Policy

While it certainly is tempting to simply throw those notices and letters 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 still has been relatively little litigation under the DMCA, 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.

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 (short of true innocence). 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 the allegedly "many schools [that] have turned a blind eye toward piracy," An Update – Piracy on University Networks, Hearing before the Subcommittee on Courts, the Internet, and Intellectual Property, 110th Cong., 1st Sess. 2 (2007) (statement of Rep. Berman), available at <http://frwebgate.

access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:33812.pdf>[3], 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? Indeed, in the recent reauthorization of the Higher Education Act, Congress has already required us to develop "plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents," as well as to "offer alternatives to illegal downloading." Higher Education Opportunity Act, H.R. 4137, 110th Cong. § 493(a) available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h4137enr.txt.pdf>. Even more onerous requirements may be on the way.

And, fourth, colleges and universities do have a significant stake in the future of intellectual property, and we therefore should have a voice in the debate over it.

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 may 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 also can give us additional immunities even for the infringements of our employees in certain circumstances. See 17 U.S.C. § 512(e). A copy of RISD's most recent educational material about file sharing is attached, and links to sample educational materials from other institutions are listed, at the end of this outline. The University of Michigan's "BAYU" program takes a different – and intriguing – educational tack: An automated system notifies users by e-mail when they appear to be uploading files using peer-to-peer file-sharing technology. The system does not examine content, and no attempt is made to determine what any particular upload consists of or whether it is illegal. The e-mail simply advises users to "be aware you're uploading" – a fact of which many truly are not aware – and that their activity is visible, and it leaves to them the decision what to do about it. Information on BAYU is available at <http://www.bayu.umich.edu>.

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

---

[3] Video of the hearing is available at <http://www.archive.org/details/gov.house.judiciary.20070308b>.

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, or to automate the "notice and takedown" process, see, e.g., UCLA, Online Copyright Infringement Claims Procedure for UCLA Housing Residents, available at <www.resnet.ucla.edu/dmcaprocess_letter.html>. Links to additional information about these technologies are listed at the end of this outline.

4. Harness market forces. Cornell University has 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 5 gigabytes of Internet traffic per month for a flat fee of $2.50, with a surcharge of $.0015 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, but not only, active file sharers – may see significantly higher bills. Information on Cornell's program is available at <www.cit.cornell.edu/ncs/netrates/overview.html>.

5. Offer alternatives. A significant number of institutions have entered into blanket licenses with legal music services such as Napster (in its "new and improved" legal version) or Ruckus, allowing their students unlimited (though "tethered") downloads for free. 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; UCLA, Get Legal, available at <getlegal.ucla.edu>. However, the popularity of these services has generally been modest at best, see Brock Read, "More Colleges Strike Up Music-Sharing Deals, Despite Lukewarm Response," Chronicle of Higher Education, Sept. 2, 2005, at A41, and some institutions have let their subscriptions lapse.

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 Kiernan, "Outsourcing the Dorm Network," Chronicle of Higher Education, Dec. 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.

IV. Subpoenas and Pre-Litigation Settlement Letters

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, 393 F.3d 771 (8th Cir. 2005); Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003); In re Subpoena to University of North Carolina at Chapel Hill, 367 F. Supp. 2d 945 (M.D.N.C. 2005).

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, while motions to quash such subpoenas have been filed on numerous grounds, virtually all have failed:

- First Amendment right to file share anonymously. See, e.g., UMG Recordings, Inc. v. Does 1-4, 2006 WL 1343597 at *2 (N.D. Cal.) ("A person who uses the Internet to download or distribute copyrighted music without permission is engaging in the exercise of speech, but only to a limited extent, and the First Amendment does not protect the person's identity from disclosure."); Sony Music Entertainment, Inc. v. Does 1-40, 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); Elektra Entertainment Group, Inc. v. Does 1-9, 2004 WL 2095581 at *3 (S.D.N.Y.) ("First Amendment protection of anonymous speech, like other kinds of speech, is subject to limits. Most importantly in the present context, the First Amendment 'does not protect copyright infringement.'") (citation omitted).

- Lack of personal jurisdiction. See, e.g., id. at *5 ("Doe No. 7 has also argued that plaintiffs have not established that personal jurisdiction may be exercised over him or her. Doe No. 7 argues that although the plaintiffs have traced the IP address used by Doe No. 7 to NYU, 'that does not automatically mean that the defendants can be found in New York.' While that may be true, a ruling on personal jurisdiction at this stage in the litigation is premature . . . . Doe No. 7's motion is accordingly denied, with leave to renew following expedited discovery."); Virgin Records America, Inc. v. Does 1-35, 2006 WL 1028956 at *3 (D.D.C.) ("The first reason that Defendant's Motion to Quash is without merit is because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the *identity* of the Defendant. . . . [A] court cannot render any kind of ruling on personal jurisdiction or catalog a

defendant's contacts with the relevant jurisdiction before the defendant has actually been named.").

- Impropriety of *ex parte* subpoenas. See, e.g., Capitol Records, Inc. v. Doe, 2007 WL 2429830 at *1 (S.D.Cal.) ("In accordance with Federal Rule of Civil Procedure 26(d), discovery does not commence until parties to an action meet and confer as prescribed by Federal Rule of Civil Procedure 26(f), unless by court order or agreement of the parties. A court order permitting early discovery may be appropriate 'where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party.' . . . [T]he Court finds good cause to grant Plaintiffs' Application . . . . [W]ithout such discovery, Plaintiffs cannot identify the Doe Defendant, and thus cannot pursue their lawsuit to protect their copyrighted works from infringement."); UMG Recordings, Inc. v. Does 1-4, 2006 WL 1343597 at *2 (N.D. Cal.) ("Plaintiffs have no other way to obtain this most basic information, which is necessary to advance the lawsuit by enabling Plaintiffs to effect service of process. Postponing disclosure of information until the normal course of discovery is not an option in the instant case because, without disclosure of Defendants' names and contact information, the litigation cannot proceed to that stage.").[4]

- Violation of FERPA. See, e.g., Interscope Records v. Does 1-14, 558 F. Supp. 2d 1176, 1180-81 (D. Kan. 2008) ("FERPA is not a barrier to the University of Kansas' disclosure of this information . . . ."); UMG Recordings, Inc. v. Doe, 2008 WL 2949427 at *6 (N.D. Cal.) ("[A]s long as FERPA's notification provisions are complied with, FERPA does not prevent an educational institution from releasing a student's personal [sic] identifiable

---

[4] To be sure, a few courts have quashed *ex parte* subpoenas, though on grounds that are at best unclear and in some cases seemingly quite clearly wrong. See, e.g., Interscope Records v. Does 1-7, 494 F. Supp. 2d 388, 390-91 (E.D. Va. 2007) (apparently holding that § 512(h) of the DMCA is the exclusive means of obtaining a subpoena for "conduit" ISPs, even though it does *not* authorize the issuance of subpoenas to "conduit" ISPs, and "[t]he Court is unaware of any other authority that authorizes the *ex parte* subpoena requested by plaintiffs"). Other such cases seem to be holding simply that *ex parte* subpoenas should not be issued unless there is a mechanism for the subjects of the subpoenas to be notified and given an opportunity to file their own motions to quash before their identities are revealed (as FERPA already would require for any subpoena directed to a college or university for information about its students). See, e.g., Capitol Records, Inc. v. Does 1-16, 2007 WL 1893603 at *1 (D.N.M.) ("[T]he Court sees no need to act on an *ex parte* application. Rather, it would appear appropriate that Plaintiffs and the University of New Mexico confer on an appropriate process to ensure that, if a subpoena is served, the University not turn over information until it has given notice to individual subscribers that a subpoena has been issued and allow those subscribers to intervene in this proceeding to protect disclosure of sensitive information. Moreover, *ex parte* proceedings should be the exception, not the rule."); LaFace Records, LLC v. Does 1-5, at *3 (W.D. Mich.) ("[T]his Court **GRANTS** PLAINTIFFS' Application for Leave to Take Immediate Discovery **WITH MODIFICATIONS.** As the application was brought *ex parte*, both the ISP and the individuals who may be implicated should have an opportunity to move to quash or modify the subpoena.") (emphasis in original).

information, in response to a Rule 45 subpoena issued by a court in an Internet infringement action."); LaFace Records, LLC v. Does 1-5, 2008 WL 513508 at *2 (W.D. Mich.) ("The subpoena provision in FERPA overrides the privacy concerns that statute protects.").

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) (attached). The institution has no legal obligation to contest the subpoena on the student's behalf, no standing to raise defenses that the student might have individually, 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.

The RIAA's latest tactic, the blanketing of colleges and universities (and perhaps other ISPs) with "pre-litigation settlement letters," appears to be motivated by a desire to avoid the costs and other, procedural obstacles associated with John Doe lawsuits and subpoenas. While there is even less legal basis for such letters – they do not even purport to be "takedown" notices, which are not applicable in the "conduit" context in any event – they are nevertheless worth taking seriously. The RIAA will eventually find the file sharers to whom such letters are directed anyway if it really wishes to do so – and it clearly does – and these letters offer those file sharers an opportunity to resolve their cases more quickly and cheaply than through litigation. Moreover, passing the letters along is not an affirmation that the RIAA's assertions are correct, nor does it deprive the recipients of any factual or legal defenses they may have. In fact, if anything, it gives the recipients more time to prepare and assert any such defenses. Increasingly, however, schools are questioning whether they should participate at all in the process. Catherine Rampell, "Antipiracy Campaign Exasperates Colleges," Chronicle of Higher Education, Aug. 15, 2008, at A1.

V. Conclusion

Where be these enemies? Capulet! Montague!
See, what a scourge is laid upon your hate,
That heaven finds means to kill your joys with love.
And I for winking at your discords too
Have lost a brace of kinsmen . . . .

Go hence, to have more talk of these sad things;
Some shall be pardon'd, and some punished . . . .

– William Shakespeare, Romeo and Juliet, Act 5, Scene 3

Additional Resources

A. Law

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

Copyright Office summary of the DMCA:
<www.copyright.gov/legislation/dmca.pdf>

ACE white paper on file sharing:
<www.acenet.edu/AM/Template.cfm?Section=Government_Relations_and_Public_Policy&template=/CM/ContentDisplay.cfm&ContentID=19133>

ACE/EDUCAUSE/NASULGC/AAU memo re: new Higher Education Act reauthorization requirements concerning P2P:
<net.educause.edu/ir/library/pdf/epo0815.pdf>

B. Policies, Procedures, and Educational Materials

ACE Summary of University Policies and Practices Addressing Improper Peer-to-Peer File Sharing
<www.acenet.edu/AM/Template.cfm?Section=Government_Relations_and_Public_Policy&template=/CM/ContentDisplay.cfm&ContentID=8503>

Cornell University:
<www.cit.cornell.edu/policy/copyright>

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

Illinois State University:
<www.digitalcitizen.ilstu.edu>

Indiana University
<filesharing.iu.edu>

Ohio University
<www.ohio.edu/students/filesharing.cfm>

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

UCLA:
<getlegal.ucla.edu/illegal_file_sharing_FAQ.htm>

University of Chicago:
<nsit.uchicago.edu/policies/filesharing/>

C. Technical Restrictions

Columbia University's network bandwidth quota:
<www.columbia.edu/cu/policy/bandwidth-frame.html>

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

Joint Committee of the Higher Education and Entertainment Communities, Workshop on Requirements for Technological Control of Illegal File Sharing on College and University Networks:
< http://net.educause.edu/ir/library/pdf/CSD5170.pdf >

Common Solutions Group review of infringement-suppression technologies:
<www.stonesoup.org/docs/copyright-technology.pdf>

D. General Background

Joint Committee of the Higher Education and Entertainment Communities*:*
<www.acenet.edu/AM/Template.cfm?Section=Government_Relations_and_Public_Policy&TEMPLATE=/CM/HTMLDisplay.cfm&CONTENTID=23911>

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

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

How Not to Get Sued for File Sharing:
<www.eff.org/wp/how-not-get-sued-file-sharing>

RIAA v. The People:
<w2.eff.org/IP/P2P/riaa-v-thepeople.php>

RIAA v. The People: Five Years Later:
<http://www.eff.org/wp/riaa-v-people-years-later>

Recording Industry vs. The People Blog:
<recordingindustryvspeople.blogspot.com>

MPAA v. The People:
<w2.eff.org/IP/P2P/MPAA_v_ThePeople>

Subpoenadefense.org:
<www.subpoenadefense.org>

EDUCAUSE memo re: "folder-based" vs. "transmission-based" DMCA notices:
<www.educause.edu/ir/library/pdf/epo0807.pdf>