Uncertain Liability of Schools for Student File Sharing

By Patrick M. Fahey and Susan S. Murphy

It has been said that a "perfect storm" for copyright piracy exists on college campuses, where technically savvy students have access to digital copies of copyrighted material over the Internet via state-of-the-art, super-fast computers.[1] In addition, those students have access to space on campus local area networks (LANs), providing them with the ability to share files with perceived privacy and anonymity. Industry groups—predominantly the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) (collectively, "the Associations")—have taken a two-pronged approach to combating this perfect storm. They have sought in the first instance to vindicate their rights against the direct infringers, bringing numerous copyright infringement lawsuits against students both for file sharing over the Internet and on LANs. The tide of student infringement is great, however, and reportedly growing stronger as students take full advantage of the privacy provided to them by campus LANs.[2] Accordingly, and with varying degrees of success, the Associations have attempted to convince schools to assume some responsibility for policing and preventing copyright infringement. The degree of cooperation that can be expected, however, is influenced by whether schools can be held legally accountable for the activities of their students. This article will examine the uncertainty surrounding potential secondary liability for copyright infringement faced by schools providing LAN access to their students.

Background

The Associations' efforts to curb illegal file sharing by college students are widely known. Less widely known, however, are the Associations' efforts to enlist colleges and universities to assume responsibility for policing student file sharing. What began in 2002 as an effort to inform schools about the problem has, since the issuance of the *Grokster* decision,[3] evolved into a claim that schools may bear some accountability for student piracy.[4]

Most recently, the Associations have focused their attention on file sharing on university LANs. In particular, the Associations are concerned because the students' use of private LANs severely inhibits their ability to police file sharing. This shift in focus resulted in a recent hearing before the Subcommittee on 21st Century Competitiveness of the House Committee on Education and the Workforce and a cautionary letter to 40 institutions, each of which the Associations claimed have a problem regarding student file sharing over their LANs.[5] In each forum, the message was the same: Schools must assume responsibility for policing their students.

Some schools have willingly accepted an active role in policing abuse, working with the Associations to implement programs to educate students and, in some instances, installing technological means to help monitor and/or prevent file sharing. Many schools, however, have balked at the Associations' demands.[6] Largely based on First Amendment and privacy concerns, these schools hesitate to police their students' computer use and potentially impinge on academic freedoms. The right balance between these competing interests has yet to be addressed by the courts, but the issue may soon come to a head. The Associations' April 2006 letter reiterated their desire to work with schools to combat piracy but cautioned that, when necessary, the Associations would enforce their rights. What those rights are, however, is unclear.

Congress, through the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512, has attempted to balance the differing interests of copyright holders and those entities that provide a fertile ground for file sharing—Internet service providers (ISPs). It is far from clear, however, how the DMCA would be applied in the present context, which involves file sharing on private LANs. It appears, therefore, in the absence of clear case law or statutory mandate, that the Associations and the schools, each of which have legitimate interests at stake, are left to sort out how to address the problem of LAN file sharing on their own.

Indirect Liability under the Copyright Act

A student who engages in illegal file sharing on a school-owned LAN subjects his or her school to the potential for secondary liability on two grounds: contributory infringement and vicarious liability. "One infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it."[7] It seems clear that merely providing students with LAN access would not give rise to indirect liability for copyright infringement. The Associations, however, have pointed to anecdotal evidence that copyright piracy is rampant in our schools. Combined with assertions that such infringement is easily detected, particularly within the control of school administrators, easily stopped, and outside of the reach of the Associations' ability to police infringement, the Associations could attempt to make a case for secondary liability of the schools.

Contributory Infringement

In order to establish that a school should be held contributorily liable for its students' copyright infringement, the copyright owners must establish both that a school knew or had reason to know of infringing file sharing taking place on its LAN and that the school caused, induced, or materially contributed to such infringement.[8]

Under traditional concepts of contributory liability, the Associations would encounter difficulty in establishing either knowledge or material contribution. Courts will not find the requisite degree of knowledge "merely because the structure of the system allows for the exchange of copyrighted material."[9] Rather, courts his-

Published in Intellectual Property Litigation, Volume 18, Number 2, Winter 2007.

torically have required strong indicia of constructive knowledge to establish that a defendant should have known that infringing activities were taking place.[10] Thus, a school would argue that the fact that the structure of its LAN allows for the exchange of infringing materials is insufficient to establish that it had knowledge—actual or constructive—of the infringement. Moreover, the mere provision of access to and space on a LAN seems an inadequate basis for a finding of material contribution.

The Associations, however, armed with mountains of statistical data and anecdotal evidence, have repeatedly notified schools that infringement is taking place on their systems. In these circumstances, the case can be made that there has been sufficient indicia of constructive knowledge to establish that the schools should have known of the illegal file-sharing problem. In conjunction with this quantum of knowledge, the Associations can show that the schools have the ability to identify illegal file sharing by, among other means, tracking bandwidth usage.[11] Moreover, with respect to material contribution, courts seem increasingly less willing to give a pass to those who turn a blind eye to blatant infringement taking place on their watch.[12]

Vicarious Liability

Knowledge of primary infringement is not an element of vicarious liability, which is imposed where one has the ability to control the infringement and derives a direct financial benefit from the illegal activity.[13] Thus, the degree to which a school may be on notice of the prevalence of student file sharing is irrelevant.

The Associations have a strong argument with regard to the first element of vicarious liability, as it seems clear that a school has sufficient control over the use of its LAN.[14] Where the ability to control is present, the "failure to police the conduct of the primary infringer" has been held sufficient to satisfy the first element.[15] It is not as clear, however, whether the financial benefit prong could be satisfied in such a case.

Courts historically have held that the financial benefit to the party charged with vicarious liability must be directly related to the infringing activity. Thus, in holding a department store vicariously liable for the copyright infringement of a concessionaire, the court in *Shapiro, Bernstein & Co. v. H.L. Green Co.* held that "[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials . . . the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation."[16] This concept of direct financial benefit extends to reach circumstances "where the availability of infringing material 'acts as a "draw" for customers.'"[17] A recent holding from the District of New Jersey extended the concept of direct financial benefit to reach the renting of booths at a flea market to vendors of infringing goods.[18]

The Associations have pointed to anecdotal evidence that copyright piracy is rampant in our schools.

It is difficult to see how the ability of students to share infringing files would bring any financial benefit to a school under a traditional analysis. Unlike conventional ISPs, schools do not charge their students for space on their LANs and, unlike websites such as Google or Yahoo!, schools do not derive revenues from student use of the LAN via advertising revenues or otherwise. Rather, the provision of computer access is part of the services provided to a school's students not unlike providing facilities for student groups to show movies or providing a library full of books.[19] However, if the link between the infringing activity and the financial benefit is sufficiently eroded, a school may risk being charged with vicarious infringement.

The problem of student file sharing on schools LANs does not seem to fit easily within either of the traditional concepts of secondary liability. Unfortunately, neither does this conduct fit easily within the parameters of the DMCA, which is meant to balance the competing interests of copyright owners and ISPs.

Limitation on Indirect Liability under the DMCA

The DMCA is meant to foster cooperation between service providers and copyright owners "to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[20] The DMCA provides certainty to service providers by setting forth certain statutory criteria that, if met, provide a safe harbor for service providers engaging in "(1) transitory digital communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools."[21] In addition, the DMCA provides two mechanisms (the subpoena provision and the notice and take down provision) that enable a copyright owner to protect itself from copyright infringement undertaken by a service provider's users, which is, in this case, students. Relevant to the current discussion are the exemptions for information residing on a service provider's system or network at the behest of the user and information location tools.

Limitations on Liability under the DMCA

The limitations on liability set forth in the DMCA are available only to entities that qualify as "service providers" pursuant to § 512(k)(1) and that otherwise meet the "conditions for eligibility" set forth in § 512(i).

The DMCA's definition of "service provider" is broad[22] and differs depending on the service provided. Thus, with respect to "transitory digital network communications," a service provider is an entity that offers transmission or routing or provides a connection for "digital online communications" between points specified by a user. For all other purposes, a "service provider" is defined more broadly to include the first category of entities, as well as providers of "online services or network access, or the operator of facilities therefor."

Whether a school that provides LAN access and space to its students will qualify as a "service provider" by virtue of providing "online services or network access" is an open issue. According to the legislative history, "online" means "over interac-

tive computer networks, such as the Internet," and thus would seem to reach LANs. A LAN is a network dedicated to sharing data among several single-user workstations or personal computers, which can be separated by distances of up to one mile.[23] Unlike the Internet, however, a LAN is private.[24] It is not clear whether this distinction would make a difference.

The DMCA balances the interests of copyright owners and service providers, in part, by providing copyright owners with a means to protect their rights through the notice and take down provision. The "notice" of the notice and take down provision must provide a school with sufficient information to identify and locate the infringing material. In the case of a private LAN, it is difficult to see how a copyright owner would be afforded the ability to police its rights, a factor that may militate against finding that the operators of LANs are "service providers" within the scope of the DMCA.

The limitations on liability set forth in the DMCA are available only to service providers that meet a series of threshold conditions. First, pursuant to § 512(k)(1)(B), the service provider must (1) have and implement a policy for the termination of repeat infringers' accounts; (2) inform users of its policy; and (3) accommodate and not interfere with standard technical measures. The implementation of a service provider's termination policy, including the procedure for receiving and conveying complaints, must be reasonable, and the service provider must not tolerate flagrant or blatant infringement by its users.[25]

Limitations on Liability for System Information or Location Tools

Pursuant to §§ 512(c) and (d), a school may avail itself of the DMCA's limitations on liability for infringing material or for links or directories to infringing material that are stored on its system or network by its students, provided that the school:

- Does not have actual or apparent knowledge of infringing material or links to infringing material residing on its system;
- If it does have actual or apparent knowledge, has acted expeditiously to remove or disable access to such material;
- Does not receive a direct financial benefit from the infringing activity where it has the right and ability to control such activity;[26]
- If notified of claimed infringement, responds expeditiously to remove or disable access to the infringing material; and
- Has designated an agent to receive notifications of claimed infringement.

Schools faced with the potential for secondary liability stemming from student file sharing on their LANs likely would invoke these safe-harbor provisions, but it is not clear whether they would be successful. Schools largely have taken the position that it is not their responsibility to police student LAN use. In this regard, it is important to note that § 512(m) expressly does not require service providers to monitor their systems for illegal file sharing in order to avail themselves of a safe harbor. A school that ignores obvious infringement, however, does so at its own risk.

In the case of a private LAN, it is difficult to see how a copyright owner would be afforded the ability to police its rights.

In light of the Associations' anecdotal evidence of rampant infringement, it is likely that the knowledge component of the safe-harbor provisions will be hotly disputed. While commentators argue that willful ignorance can never be equated with actual knowledge,[27] apparent knowledge will be found where "the service provider deliberately proceeded in the face of blatant factors of which it was aware."[28] Establishing apparent knowledge will require evidence that the service provider "turned a blind eye to red flags of obvious infringement."[29] Courts and commentators agree, however, that in light of the inherent difficulty in determining whether a particular work is infringing, "the 'red flag' must be brightly red indeed—and be waiving blatantly in the provider's face."[30]

The Associations, which represent the rights of numerous copyright owners, have a legitimate concern regarding student file sharing and may need to seek creative ways to enforce the rights of their members. Schools, on the other hand, have legitimate concerns regarding the First Amendment and privacy rights of their students and an understandable reluctance to stifle academic freedom. Ambiguities in the law of secondary liability may lead to litigation of these issues, in which case the extent of the protections afforded by the DMCA will be clarified. Until such clarification is provided, schools would be well advised to follow the provisions of the DMCA. ●

Patrick Fahey is a partner and Susan Murphy is an associate with Shipman & Goodwin LLP in Hartford, Connecticut.

Endnotes

[1] *The Internet and the College Campus: How the Entertainment Industry and Higher Education are Working to Combat Illegal Piracy: Hearing Before the Subcomm. on 21st Competitiveness of the House Comm. On Education and the Workforce*, 109th Cong. CQ Transcriptions, September 26, 2006, LEXIS, Legis Library, Poltrn File [Hereinafter *Hearing*] (opening remarks of Rep. Ric Keller and testimony of Cary Sherman, President, RIAA).

[2] *Hearing* (testimony of Dan Glickman, Chairman & CEO, MPAA) ("[N]early half, 44 percent of our industry's domestic losses, over $500 million annually, are attributable to college students.").

[3] *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 545 U.S. 913, ___, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005).

[4] Letter from Cary H. Sherman, President, RIAA and Graham B. Spanier, President Pennsylvania State University to College/University Presidents 1 (Aug. 16, 2005) (asserting that the ramifications for universities of the *Grokster* decision "are yet to be determined" but stressing that the Supreme Court unanimously held that "file-sharing companies and others who intentionally encourage or induce copyright infringement by third parties can be liable for infringement themselves"), *available at* http://www.acenet.edu/AM/Template.cfm?Section=Search&template=/CM/HTMLDisplay.cfm&ContentID=11713.

[5] Letter from Cary H. Sherman, President, RIAA and Dan Glickman, Chairman & CEO, MPAA to College/University Presidents (April 27, 2006), *available at* http://www.mpaa.org/press_releases/2006_04_27_lan.pdf.

[6] *Hearing* (testimony of Cary Sherman,

President, RIAA).

[7] *Grokster,* 125 S. Ct. at 2776, 796–97 (citations omitted).

[8] *Perfect 10 v. Google, Inc.*, 416 F. Supp. 2d 828, 853 (C.D. Cal. 2006).

[9] *UMG Recordings, Inc. v. Sinnott*, 300 F. Supp. 2d 993, 998-99 (E.D. Cal. 2004) (internal quotation marks omitted) (emphasis in original) (quoting *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)).

[10] Such indicia have been established where, for example, a defendant had an active screening procedure or it reviewed user logs containing infringing files. *See Arista Records, Inc. v. MP3Board, Inc.*, No. 00Civ.4660(SHS), 2002 U.S. Dist. LEXIS 16165, at *16 (S.D.N.Y. Aug. 29, 2002) (citing cases).

[11] *Hearing* (testimony of Dan Glickman, Chairman & CEO, MPAA).

[12] *Arista Records, Inc. v. Flea World, Inc.*, No. 03-2670, 2006 U.S. Dist. LEXIS 14988, at *45–*51 (D.N.J. Mar. 31, 2006).

[13] *Google, Inc.*, 416 F. Supp. 2d at 856.

[14] *See A&M Records, Inc.*, 239 F.3d at 1023 ("The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.").

[15] *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

[16] 316 F.2d 304, 307 (2d Cir. 1963) (citation omitted).

[17] *A&M Records, Inc.*, 239 F.3d at 1023 ("Ample evidence supports the district court's finding that Napster's future revenue is directly dependant upon 'increases in user-base.' More users register with the Napster system as the 'quality and quantity of available music increases.'").

[18] *Flea World, Inc.*, 2006 U.S. Dist. LEXIS 14988, at *38–*44.

[19] *See*, *e.g.*, *Roy Export Co. Establishment v. Trustees of Columbia Univ.*, 344 F. Supp. 1350, 1353 (S.D.N.Y. 1972) (plaintiff unable to establish for purposes of injunction that university derived a financial benefit from the showing of two infringing films by a student group on campus in a facility provided by the school).

[20] H.R. Rep. 105–551, pt. 2 (1998).

[21] *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

[22] *In re Aimster Copyright Litigation*, 334 F.3d 643, 650 (7th Cir. 2003) ("Although the Act was not passed with Napster-type services in mind, the definition of Internet service provider is broad ('a provider of online services or network access, or the operator of facilities therefore,') and, as the district judge ruled, Aimster fits it."), *cert. denied sub nom. Deep v. RIAA, Inc.*, 540 U.S. 1107, 124 S. Ct. 1069, 157 L. Ed. 2d 893 (2004).

[23] *Local Area Networks*, COLUMBIA ENCYCLOPEDIA (6th ed. 2006); *Networks*, COLUMBIA ENCYCLOPEDIA (6th ed. 2006).

[24] H.R. Rep. 105–551, pt. 2 (1998).

[25] *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1102–03 (W.D. Wash. 2004).

[26] The inclusion of a vicarious liability standard seems confusing at first blush in the light of the DMCA's purpose of shielding qualifying service providers from liability for, among other things, vicarious liability. It appears, however, that a different standard is applied to the "control" prong of the analysis in the context of the DMCA. Specifically, courts have concluded that, with respect to the "control" prong, there must be something more than the mere ability to exclude users from the system. This distinction is based on the premise that "closing the safe harbor based on the mere ability to exclude users from the system is inconsistent with the statutory scheme" which is meant to "encourage some level of copyright enforcement activity by service providers, not to punish it." *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1181–82 (C.D. Cal. 2002).

[27] 3 Nimmer § 12B.04[A][1].

[28] *Corbis Corp.*, 351 F. Supp. 2d at 1108 (citations omitted) (internal quotation marks omitted).

[29] *Id*. (internal quotation marks omitted).

[30] *Google, Inc.*, 416 F. Supp. 2d at 853 n.19 (quoting 3 Nimmer § 12B.04[A][1]).