UNITED STATES DISTRICT COURT FOR
THE DISTRICT OF MASSACHUSETTS

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Plaintiff, v. RECORDING INDUSTRY ASSOCIATION OF AMERICA, Defendant.	) Misc. Act. No. 1:03-MC-10209-JLT

OPPOSITION OF RECORDING INDUSTRY ASSOCIATION OF AMERICA TO MIT'S MOTION TO QUASH AND FOR A PROTECTIVE ORDER

The Recording Industry Association of America (RIAA) hereby files this Opposition to MIT's Motion to Quash a subpoena issued out of the District Court for the District of Columbia. *See Recording Industry Association of America v. MIT*, Misc. Act. Nos. 03-MS-265 (D.D.C.). For the reasons stated, MIT has filed its motion in the wrong court, and this court has no authority to quash a subpoena issued out of another federal district court. This Court should deny MIT's motion and dismiss this action. Moreover, even if the Court does reach the merits, it should deny MIT's motion because MIT has no basis for refusing to comply with the subpoena at issue.

STATEMENT OF FACTS

Internet Piracy

The technology that has made the Internet possible has also spawned massive illegal copying of copyrighted works. The greatest such threat arises from peer-to-peer (P2P) networks. By downloading P2P software, and logging onto a P2P network, an individual makes music and

video files on a home or office computer available to any Internet user worldwide. Until shut down by a federal court injunction, Napster was the most notorious P2P system. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Similar systems have arisen in Napster's wake, such as Kazaa, iMesh, Grokster and Gnutella. Approximately 90% of the content on such P2P networks is copyrighted material disseminated without authorization. *Id.* at 1013. There is no dispute that this uploading and downloading of copyrighted works is illegal. *Napster,* 239 F.3d at 1014-15; *In re Aimster Copyright Litigation*, No. 02-4125, 2003 WL 21488143 (7th Cir. June 30, 2003). Nonetheless, at any given moment, millions of people are using P2P networks to download copyrighted material or offer such material for others to download. More than 2.6 *billion* infringing music files are downloaded monthly. L. Grossman, *It's All Free*, Time, May 5, 2003, at 60-69.

A significant portion of this copyright piracy occurs on college campuses. Universities act as Internet Service Providers (ISPs) for their students, providing computing services and access to the Internet. In contrast to slower, dial-up service that some students may have at home, universities offer their students high-speed Internet connections that allow them to download and distribute files quickly and easily. *See Napster Was Nothing Compared with This Year's Bandwidth Problems*, Chronicle on Higher Education (Sept. 28, 2001). And students take advantage of this benefit: some universities have estimated that *95% of the traffic* on their university computer systems involves copying of files (mostly copyrighted music, video, and pictures) over P2P networks. *See* Internet Bandwidth Management at Kenyon, available at http://lbis.Kenyon.edu/about/test/bandwidth.phml; *see also* Change to Swarthmore's Internet Bandwidth Policy, available at http://www.swarthmore.edu/its/news/eeitems/87 (estimating the percentage of student traffic on P2P networks to be 90%). In response to this serious problem,

the recording industry and universities have worked cooperatively to educate students and stop copyright piracy over university computer networks.

The propagation of illegal digital copies over campus networks significantly harms copyright owners, and has had a particularly devastating impact on the music industry. *See In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 273 (D.D.C. 2003) ("*Verizon II*"). CD sales – the principal revenue source for most record companies – declined 7% in 2000, 10% in 2001 and 11% last year. *See* http://www.riaa.com/pdf/2002yrendshipments.pdf. Surveys show that the main reason for this precipitous drop in revenues is that people (especially teen-agers and college students) are downloading music illegally for free, rather than buying it. *See In re Aimster Copyright Litigation*, No. 02-4125, 2003 WL 21488143, at *1 (7th Cir. June 30, 2004) ("Teenagers and young adults who have access to the Internet like to swap computer files containing popular music."). According to a November 2002 survey by Peter D. Hart Research Associates, by a 2-to-1 margin, consumers report they are downloading more music and purchasing less.

The Digital Millennium Copyright Act

Congress enacted the Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998), to encourage development of the Internet's potential, while at the same time protecting against the "massive piracy" of copyrighted works that Internet technology permits. S. Rep. No. 105-190, at 8 (1998) ("S. Rep."). The DMCA addressed two problems – (1) the threat of massive piracy, which could be committed anonymously over the Internet, and (2) the fear of ISPs, including universities, that they would be subject to massive liability for facilitating illegal conduct over their computer networks. The DMCA was the product of

extensive negotiations between ISPs, including universities, and copyright owners. *In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24, 38 n.11 (D.D.C. 2003) ("*Verizon I*").

In Title II of the DMCA, codified at 17 U.S.C. § 512, Congress addressed both concerns by carving out certain limitations on the liability of ISPs, including universities, while at the same time requiring ISPs to act swiftly when they are made aware of copyright infringement. *See* S. Rep. at 40 (Congress wanted there to be "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."). In order to take advantage of the liability limitations, universities must, for example, disable access to infringing material available from their networks when notified, *see* § 512(b)-(d), and terminate the accounts of students who are repeat copyright infringers. § 512(i)(1)(A). *See also* § 512(e) (special provisions addressing liability of universities arising out of conduct of university employees and students).

Critical to Congress's goals in the DMCA was to stop infringement on the Internet as expeditiously as possible. *See Verizon I*, 240 F. Supp. at 34 (noting "Congress's express and repeated direction to make the subpoena process 'expeditious.'"); S. Rep at 45 (when a service provider is notified of infringing activity, the limitation on liability is maintained only if "the service provider acts expeditiously either to remove the infringing material from its system or to prevent further access to the infringing material"). An individual Internet pirate can cause tens of thousands of infringing copies to be distributed in a single day. In the case of sound recordings that have not yet been released publicly, the economic impact of infringement can be devastating. Thus, Congress created streamlined procedures to ensure that the system would operate smoothly and efficiently. Congress required every ISP, including universities, to register a single DMCA contact with the United States Copyright Office to whom all notices of

infringement are to be sent. § 512(c)(2). Congress also formalized a system for "notice and take down," specifying in detail the information that copyright owners must provide to ISPs (the notice), which would automatically and immediately trigger the ISP's obligation to disable access to infringing material (the take-down).

Section 512(h), the provision at issue in this case, is a critical part of Congress's goal of providing streamlined procedures to stop Internet piracy as quickly as possible. Copyright owners cannot enforce their rights directly unless they can identify the infringers. Section 512(h) places on ISPs the obligation of providing the identity of subscribers who use their networks to infringe. Under § 512(h)(1), a copyright owner may request that "the clerk of any United States district court" issue a subpoena requiring an ISP to disclose the identity of copyright infringers when the copyright owner comes forward with good faith claims of infringement. A copyright owner must file with the clerk a notice of the same type as is routinely sent to the ISP's DMCA contact, as well as a sworn declaration that the information "will only be used for the purpose of protecting rights under this title." § 512(h)(2)(A), (C). Once the clerk has issued the subpoena – which Congress intended to be a ministerial function (S. Rep. at 51) – the copyright owner is to provide for "delivery" of both the subpoena and the notice to the ISP. In some, but not all cases, the subpoena and notice will trigger two different obligations – (1) to identity the infringer and (2) to take down the infringing material.[1]

Congress made clear that § 512(h) subpoenas were to be issued and complied with expeditiously, using that word three times in the statute itself and repeatedly in the legislative history. *See, e.g.*, § 512(h)(5) (requiring the ISP to "expeditiously disclose" the information

[1] Where an ISP is providing only conduit services, as defined in § 512(a), an ISP that receives a notice and subpoena must identify the subscriber, but may not need to take down any infringing material.

sought); S. Rep. at 51 (describing the need for expedition). Congress also specified that this obligation is not discretionary or conditioned on any other duties they might have: an ISP must comply with the subpoena "notwithstanding any other provision of law." § 512(h)(5). Congress also established procedures for enforcing DMCA subpoenas in federal court, providing that

> Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

§ 512(h)(6).

The Subpoenas At Issue

Since enactment of the DMCA, copyright owners have served hundreds of DMCA subpoenas. Prior to the nationwide enforcement effort it began in June of this year, RIAA had obtained approximately 100 subpoenas, all from the District Court for the District of Columbia. Those subpoenas were delivered to ISPs all across the country. At no time prior to this case did an ISP refuse to comply on the ground that the subpoena was issued from the wrong court.

In June of this year, RIAA became aware of a significant copyright infringer using the MIT network to disseminate copyrighted music without the authorization of the copyright owners. RIAA learned of that user as anyone else would – by discovering him or her offering copyrighted music files to anyone that wanted them over the Internet. The individual used an alias, and was offering hundreds of copyrighted works to the world-at-large over one of the major peer-to-peer networks. RIAA downloaded a representative sample of the files being offered and ascertained that they were indeed illegal copies of copyrighted music. RIAA could not, however, determine the physical location of the infringer or his or her identity. All RIAA

could determine was that the MIT network was being used to disseminate the copyrighted files. RIAA also could not determine whether the individual was a student or an employee of MIT.

On July 2, 2003, pursuant to § 512(h), RIAA obtained from the clerk of the District Court for the District of Columbia a subpoena to MIT to identify the individual committing the copyright infringement. RIAA delivered the subpoena to MIT's DMCA designated agent. After an exchange of correspondence in which MIT indicated its refusal to comply with the subpoena, MIT filed a motion to quash the subpoena. Rather than filing the motion in the District Court for the District of Columbia – the court with the authority to enforce or quash the subpoena – MIT chose to file its motion in this District. In conjunction with this Opposition, RIAA is filing a motion to compel responses to the subpoena in the proper court – the District Court for the District of Columbia.

ARGUMENT

This Court has no authority to enforce, quash, or take any other action with respect to the subpoena in this case, which was issued by another district court. Thus, MIT's arguments should be decided in the pending motion to compel proceeding in the District Court for the District of Columbia, not in this Court. MIT will have every opportunity to raise its arguments in that forum.

But even if that were not true, this Court should deny MIT's motion. MIT does not object to the subpoena in this case because it is burdensome or because it requires disclosure of privileged information. MIT's only complaint is that it should not have to litigate disputes over the subpoena in the District of Columbia. MIT concedes it has *no* valid objection to the subpoena, except that it would prefer it to have been issued by a different court. But if MIT had accepted service, as it has the right and authority to do, there would be no dispute at all in this

case. The DMCA does not require copyright owners to jump through unnecessary hoops to obtain the information that ISPs, such as MIT, must provide "notwithstanding any other provision of law." § 512(h)(5). The DMCA expressly authorizes a copyright owner to obtain a subpoena from "any United States district court." In this case, RIAA obtained the subpoena and delivered it to the person whom MIT has identified (as the DMCA requires) as the contact for notifications of infringement. The DMCA requires nothing more to trigger the non-discretionary duty to disclose to RIAA the identity of some one who has violated and continues to violate the copyrights of RIAA's members over the Internet. Thus, if this Court does reach the merits, it should deny MIT's motion and require MIT to comply with the subpoena as soon as possible.

I. THIS COURT LACKS THE AUTHORITY TO QUASH SUBPOENAS ISSUED BY ANOTHER DISTRICT COURT.

It is hornbook law that only the issuing court can quash a subpoena, and that other courts have no jurisdiction or authority to limit, quash, or, for that matter, enforce a subpoena from another court. *See* 9A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, § 2459 at 40-41 (2d ed. 1995) (stating that "motions to quash, modify, or condition the subpoena are to be made to the district court of the district from which the subpoena issued."). The D.C. Circuit therefore has held that "only the issuing court has the power to act on its subpoenas" and "nothing in the Rules even hints that any other court may be given the power to quash or enforce them." *In re Sealed Case*, 141 F.3d 337, 341 (D.C. Cir. 1998). A motion to quash that is not filed with the issuing court "is fatally flawed because it has been filed with the wrong court," and it must be denied. *Pilcher v. Direct Equity Lending*, No. 99-1245-JTM, 2000 WL 33170865, at *4 (D. Kan. Dec. 22, 2000).

The purpose of a motion to quash is "to remedy litigants' disputes regarding whether a subpoena is unduly burdensome, and pursuant to Rule 45, such objections are squarely within

the jurisdiction of the district court that issued the subpoena." *International Bhd. of Teamsters v. Eastern Conf. of Teamsters*, 162 F.R.D. 25, 28 (S.D.N.Y. 1995); *see also* Fed. R. Civ. P. 45(c)(3)(A) (authorizing motions to quash solely in "the court by which a subpoena was issued"). Thus, when a non-party objects to subpoenas as unduly burdensome, "their objections are properly the subject of a Rule 45(c)(3) motion brought in the Court that issued the subpoenas." *Id.*[2]

Application of these elementary rules of civil procedure requires dismissal of MIT's motion to quash. Indeed, MIT effectively concedes as much in its motion papers. The cases cited by MIT actually prove that this Court has no authority to act on MIT's motion. MIT Mem. at 6-7. Unlike MIT, the party seeking to quash the subpoenas in *Echostar Communications Corp. v. News Corp.*, 180 F.R.D. 391, 396-97 (D. Colo. 1998), filed its motion to quash in the same court that issued the subpoenas. And the court in *Kupritz v. Savannah College of Art & Design*, 155 F.R.D. 84 (E.D. Pa. 1994), refused to enforce a subpoena precisely because it had no jurisdiction to enforce a subpoena issued by another court. *Id.* at 88.

The District Court for the District of Columbia is the forum for adjudication of this dispute. That court issued the subpoena, that court has expertise with respect to DMCA subpoenas (having issued more such subpoenas than any other court and having authored the only opinions on the interpretation of § 512(h)), and the "burden" on MIT of litigating in the

[2]*See In re Digital Equip. Corp.*, 949 F.2d 228, 231 (8th Cir. 1991) (holding that where subpoenas were issued by District of Oregon, District Court in South Dakota "lack[ed] jurisdiction to rule" on objections); *Kearney v. Jandernoa*, 172 F.R.D. 381, 383 n.4 (N.D. Ill. 1997) (stating that "a motion to quash, under Rule 45(c)(3)(A), must be filed and decided in the court from which the subpoena issued"); *Armstrong v. Red River Entm't*, No. 96-50087, 1997 WL 739616, at * 1 (Bankr. E.D. Ark. Nov. 12, 1997) (holding that under Rule 45, "it is the court under whose authority the subpoena is issued which has jurisdiction over a motion to quash the subpoena"); *Lieberman v. American Dietetic Ass'n*, No. 94C5353, 1995 WL 250414, at *1 (N.D. Ill. Apr. 25, 1995) (holding that the court that issued a subpoena may quash it, and that "the case law confirms" that non-issuing court "has no such power").

District of Columbia is no greater than the burden on RIAA of litigating in Boston. Moreover, there is no burden on MIT whatsoever if it simply accepts service because it has no other objections to the subpoena.

II. IF THE COURT DOES DECIDE MIT'S MOTION, IT SHOULD DENY THE MOTION BECAUSE THE DMCA SUBPOENA WAS VALIDLY ISSUED AND PROPERLY DELIVERED.

A. A DMCA Subpoena Is Validly Delivered if Sent to the DMCA Designated Agent.

Subpoenas issued pursuant to the DMCA are not subpoenas issued pursuant to Rule 45. DMCA subpoenas are not broad discovery mechanisms, and a different set of rules applies to them. They are targeted to ensure that a discrete amount of information – information sufficient to identify infringers – is made available for the limited purpose of enabling a copyright owner to pursue its rights. DMCA subpoenas do not raise issues concerning burden on witnesses (because they do not require testimony of any kind) nor do they impose a burden of copying or compilation of documents (because they do not require production of documents). As MIT concedes, there is no burden on it in *complying* with the subpoena. MIT Mem. at 6. Compliance with the subpoena is simply a matter of a computer look-up, which takes minutes, but which must be done quickly before the records are destroyed and in such time as to allow the copyright owner quickly to halt the ongoing infringement. The burden of compliance in no way depends, however, on the court from which the subpoena is issued.

Moreover, the problem of massive copyright infringement on the Internet, to which § 512(h) is addressed, has two key characteristics. It is not limited to a particular state or territory – it is necessarily nationwide (indeed worldwide), to the extent that anything in cyberspace can be said to have a territorial locus. When a copyright owner seeks to track down an infringer, it has no idea where that infringer is and where the copyright owner might ultimately be forced to

file suit to obtain an injunction and damages (This is even true where the ISP is a university, because students may use the university network while away from school.). And, as Congress repeatedly made clear, the infringement must be addressed immediately because each minute that copyrighted files are being made available without authorization, they can potentially be downloaded by anyone in the world. *See Verizon II*, 257 F. Supp.2d at 273 (absent enforcement, "the apparent infringement of numerous copyrighted works made available over the Internet for universal downloading could continue unabated. The value of these copyrighted works could plummet further, as they are made available (at the push of a button) for the taking.").

In enacting the DMCA and § 512(h), Congress sought to address both of these problems by providing for a streamlined mechanism for identifying infringers – wherever they may be – as quickly as possible. Congress wanted to ensure that copyright owners did not have to jump through hoops and that ISPs would cooperate with copyright owners in protecting their rights. Thus, § 512(h) talks in terms of "delivery" and "receipt" of subpoenas, not service by process servers. *See* § 512(h)(4) ("the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requestor for *delivery* to the service provider."); § 512(h)(5) ("Upon *receipt* of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose . . . ."); § 512(h)(6) ("Unless otherwise provided by this section or by applicable rules of court, the procedure for issuance and *delivery* of the subpoena . . . .").

Congress imposed the obligation to comply with DMCA subpoenas on all ISPs, regardless of whether they are also obliged to take down infringing material.[3] Nonetheless,

---

[3]In *Verizon I*, an ISP argued that the § 512(h) does not apply to ISPs that do not store infringing material or to ISPs that have no obligation to disable access to such material. The District Court for the District of Columbia wholly rejected that argument, finding that § 512(h) applies to all service providers performing all functions.

Congress viewed issuance and delivery of subpoenas as complementary to the process by which copyright owners send notices to the ISP's DMCA agent to trigger the ISP's obligation to take-down infringing material. § 512(c)(2)-(3). Section 512(h)(5) makes this understanding explicit, providing that "Upon receipt of the issued subpoena, *either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A)*, the service provider shall expeditiously disclose . . . ." Although traditional service would certainly be permissible, the DMCA does not require it; rather, DMCA subpoenas need only be sent (by mail or other means) to the DMCA agent that the statute requires the ISP or university to appoint.

Congress also made clear that legal requirements that might interfere with the expeditious subpoena process established by the DMCA are to be superseded. By using the phrase "notwithstanding any other provision of law," § 512(h)(5), Congress could not have been more clear: Any provision of law that would prevent the DMCA from operating as intended must yield. *See Saco River Cellular, Inc. v. Federal Communications Comm'n*, 133 F.3d 25, (D.C. Cir. 1998); *Liberty Maritime Corp. v. United States OMI Corp.*, 928 F.2d 413, 416 (D.C. Cir. 1991) (the language "notwithstanding any other provision of law" supersedes all other laws and a "clearer statement is difficult to imagine."). Indeed, where a statute commands that something must be done "expeditiously" and "notwithstanding any other provision of law," other statutory provisions that would cause delays or lengthy proceedings simply do not apply. *National Coalition to Save Our Mall v. Norton*, 161 F. Supp. 2d 14, 21 (D.D.C. 2001).

To interpret the DMCA as MIT does would seriously undermine Congress's goal of creating an expeditious mechanism for copyright owners. It would force copyright owners – who are being irreparably harmed every moment that the infringing files are being made available to the public at large – to have counsel in every one of the 94 judicial districts, ready at

a moment's notice to serve subpoenas.[4] That would slow the DMCA subpoena process and place an enormous burden on copyright owners, directly contrary to Congress's intent. Indeed, Congress intended to minimize the burden on copyright owners and place some burden – a very modest one in this circumstance – on ISPs, who receive enormous benefits under the DMCA in the form of limitations on their liability.

The language of § 512(h)(6), on which MIT relies, is not to the contrary. In § 512(h)(6), Congress provided that Rule 45 would generally apply, but also made clear that Rule 45 would not apply whenever it would conflict with § 512(h) or when application of Rule 45 would not be practicable, given the goals that § 512(h) advances. Here, imposition of the geographical limitations on venue or the mechanical requirements of service are simply not practicable, given the goals of § 512(h) and the urgent need to obtain information to stop the ongoing infringement. *See also National Coalition*, 161 F.Supp.2d at 21 (rejecting application of environmental laws where they would delay construction of monument that Congress specified should be completed "expeditiously" "notwithstanding any other provision of law").

Because the DMCA is fully satisfied by delivery of the subpoena and infringement notice to the ISP's registered DMCA contact, RIAA has fully complied with the statute, and MIT must disclose the information sought as soon as possible.

B. Even If Traditional Service Is Required, the DMCA Authorizes Nationwide Service of Process.

The DMCA, by its terms, authorizes the issuance of DMCA subpoenas by the "clerk of any United States district court." § 512(h)(1). That provision, as well as the DMCA as a whole

---

[4]In tracking down a single infringer, a copyright owner may have to obtain multiple subpoenas to multiple ISPs. Forcing the copyright owner to go to multiple courts to identify one infringer is a burden that would seriously frustrate Congress's goals in the DMCA.

and its legislative history, compel the conclusion that Congress intended to authorize nationwide service of process..

"Congressional power to authorize nationwide service of process in cases involving the enforcement of federal law is beyond question." *Mariash v. Morrill*, 496 F.2d 1138, 1143 n.6 (2d Cir. 1974); *United States v. Congress Constr. Co.*, 222 U.S. 199 (1911). Moreover, Congress can authorize nationwide service either expressly or impliedly. *See Robertson v. Railroad Labor Bd.*, 268 U.S. 619, 622 (1925); *First Nat'l Bank of Canton v. Williams*, 252 U.S. 504, 509-10 (1920); *United States v. Bliss*, 108 F.R.D. 127, 135 (E.D. Mo. 1985) (holding that "[t]he doctrine of implicit authorization of nationwide service of process is firmly established in the law" and finding such authorization in CERCLA) (citations omitted).

Courts thus have found implied authorizations of nationwide service of process in statutes similar to the DMCA where there is an important regulatory purpose advanced by nationwide service and the burden on the party served is not great. For example, the court in *Bliss* found nationwide service to be authorized under CERCLA. The *Bliss* court rejected both the argument that Congress clearly knows how to authorize nationwide service because it has done so in other statutes and that silence in the text should prohibit such an implication. Rather, the court looked at the policy goals Congress sought to advance and determined that those factors, especially the policies behind CERCLA's goal of providing for comprehensive responses to environmental threats, compelled an implication of nationwide service. Notably, after holding that Congress could impliedly authorize nationwide service, a court in this district held that Congress had not intended nationwide service under CERCLA (prior to the Superfund Amendments) . *In re Acushnet River & New Bedford Harbor Proceedings*, 675 F. Supp. 22, 28-29 (D. Mass. 1987). That decision, however, proved to be incorrect. Congress itself noted that it

had intended nationwide service of process in CERCLA and explained that such service had been "implicit" in CERCLA's statutory scheme. H.R. Rep. No. 99-253(I), at 79 (1986) (explaining, in the legislative history of the Superfund Amendments, that nationwide service was "implicit" in the pre-amendment version of CERCLA). Congress nonetheless amended the statute to "confirm" that such process was available "to avoid future arguments on the issue." *Id.*

Just as with CERCLA, nationwide service is necessary here to "effectuate the purpose of the regulatory scheme" Congress created in the DMCA. *FTC v. Browning*, 435 F.2d 96, 100 (D.C. Cir. 1970). *Robertson v. Railroad Labor Board*, 268 U.S. at 622, cited by MIT, is not to the contrary. That case recognized Congress's power to authorize nationwide service, but decided – in the context of one statute only – that Congress had not intended such service. Cases subsequent to *Robertson* recognize that whether a statute authorizes nationwide service is a matter of legislative intent. *See, e. g., NLRB v. Gunaca*, 230 F.2d 542 (7th Cir. 1956), *vacated on other grounds*, 353 U.S. 902 (1957). Thus, the courts have found numerous statutes to authorize nationwide service of process, both expressly and impliedly.

For example, the D.C. Circuit has had occasion to consider these issues repeatedly under statutes authorizing the issuance of subpoenas by federal government agencies.[5] In *Browning*, the D.C. Circuit considered subpoenas issued by the FTC pursuant to 15 U.S.C. § 49. Section 49 reads, in part, "[a]ny of the district courts of the United States within the jurisdiction of which such inquiry is carried on may, in case of contumacy or refusal to obey a subpoena issued to any corporation or other person, . . . issue an order [compelling compliance with the subpoena]."

[5]In many respects, a DMCA subpoena is similar to an administrative subpoena. Each is issued without the act of a judge and without a pre-existing litigation. Like administrative subpoenas, DMCA subpoenas are enforceable in court, pursuant to provisions established by Congress. *See ICC v. Brimson*, 154 U.S. 447 (1894) (discussing administrative subpoenas).

The court distinguished § 49 from the statute at issue in *Robertson.* Unlike that statute, § 49 was a special grant of jurisdiction "to that court or those courts sitting in the district or districts in which the inquiry is being conducted." *Browning*, 435 F. 2d at 99. But that grant did not ensure that the agency would be able to conduct a nationwide investigation efficiently; only nationwide service of process of subpoenas enforceable in such courts would do so. For that reason and because to conclude otherwise would sharply limit the investigative authority of the FTC, the court found "an implied grant of authority for extraterritorial service of process in order to effectuate the purpose of the regulatory scheme." *Id.* at 100; *see also FTC v. Jim Walter Corp.*, 651 F.2d 251 (5th Cir. 1981) (adopting the *Browning* court's reasoning). The logic of *Browning* has been applied to other contexts involving federal agency subpoenas, including those issued by the Federal Election Commission, *FEC v. Committee to Elect LaRouche*, 613 F. 2d 849, 855 (D.C. Cir. 1979), and by the National Highway Traffic Safety Administration (NHTSA), *United States v. Firestone Tire & Rubber Co.*, 455 F. Supp. 1072 (D.D.C. 1978).[6]

For all of these reasons, if the Court decides to rule on the merits, it should find that Congress intended that DMCA subpoenas be served nationwide.

III. FERPA PROVIDES NO BAR TO COMPLYING WITH THE DMCA.

Contrary to MIT's argument, MIT Mem. at 9-10, none of the provisions of the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, presents an obstacle to MIT's expeditious compliance with RIAA's subpoena.

---

[6]Nothing in the language of 15 U.S.C. § 49 distinguishes it from the statute at issue here. Each specifies special rules for venue, but neither makes specific reference to nationwide service of process. Contrary to MIT's claim, 15 U.S.C. § 49 does not limit venue in any significant way because, like the copyright owner's investigation of infringement here, the FTC's inquiries are frequently, if not usually, nationwide in scope. *Jim Walter Corp.*, 651 F.2d at 254; *FTC v. MacArthur*, 532 F.2d 1135 (7th Cir. 1976); *LaRouche*, 613 F.2d at 855; *FTC v. Cockrell*, 431 F. Supp. 558 (D.D.C. 1977); *Firestone Tire & Rubber Co.*, 455 F. Supp. at 1072. Thus, under either statute, venue is proper in any court, but nationwide service is necessary to permit the investigation to proceed expeditiously.

The DMCA requires ISPs, including universities, to comply with DMCA subpoenas "notwithstanding any other provision of law." § 512(h)(5). Congress could not have used more mandatory language – universities must comply regardless of their other obligations under the law. The DMCA trumps whatever obligations MIT has under FERPA, and MIT therefore is required to respond to DMCA subpoenas as soon as it is able.

But even if the DMCA did not have this trumping language, FERPA does not apply to a DMCA subpoena, which seeks only the "identifying information" of name, address, telephone number, and e-mail address. FERPA expressly does not apply to the provision of "directory information," which is defined as:

> the student's ***name, address, telephone listing***, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

20 U.S.C. § 1232g(a)(5)(A) (emphasis added).[7]

MIT's argument that FERPA applies so that the college must notify its student in advance of the copyright owner taking action is inconsistent with the clear purpose of the DMCA to allow a copyright owner to obtain the information "expeditiously." The need for quick action is plain in cases of Internet piracy, because the infringement is likely ongoing and a copyright owner needs to act quickly to stem the harm being caused. In the present case, the infringer is distributing hundreds of songs without authorization and may well be continuing to do so. Moreover, the DMCA itself protects any privacy interest such an individual may have by ensuring that information obtained pursuant to a DMCA subpoena can "only be used for the

[7] RIAA's subpoena also seeks an e-mail address, which is not part of FERPA's definition of "directory information," for the obvious reason that the statute pre-dated electronic mail technology. The Department of Education's implementing regulations, however, do include the student's "electronic mail address" in its definition of "directory information." 34 C.F.R. § 99.3.

purpose of protecting rights under [the federal copyright laws]." § 512(h)(2)(C) (requiring copyright owners to file a declaration to that effect).

MIT suggests that coupling the student directory information sought by RIAA with the "copyright infringement" modifier somehow alters the quality of the information, rendering it "more than mere 'directory information.'" MIT Mem. at 10-11. But MIT cites no authority whatsoever for this proposition, and the parade of horribles that MIT suggests has no application here. RIAA does not dispute that in the absence of statutory or other authority, universities cannot disclose "all students who make A's" or "all students who have sought counseling." But RIAA does not seek to link grades, receipt of counseling services, or disciplinary history (things that may themselves be "education records," as defined by statute) with particular student identities. Rather, RIAA seeks to link evidence of copyright infringement – in the form of pirated files being made available from the student's own computer – with the student's identity. Such pirated files are not themselves education records and linking them with directory information does not make them so. A student's use of the school's Internet-access facilities to infringe copyrighted materials cannot be seriously analogized to seeking counseling services. These latter activities are not only lawful – as compared to copyright infringement – but they also share a student privacy component that is utterly lacking here. The infringer in this case has made available the contents of his or her computer and the pirated music files on that computer to anyone in the world who wants them – there could be no less private activity.[8]

[8]Nor does the fact that RIAA has provided the IP address to the university change the nature of the information sought. That address – which is public when a person uses the Internet to infringe copyrights over a P2P network – is not itself a private "education record." It merely identifies a particular Internet session, is thus not "directly related to a student" and not kept in the student's education file. 20 U.S.C. § 1232g(a)(4)(A)(i).

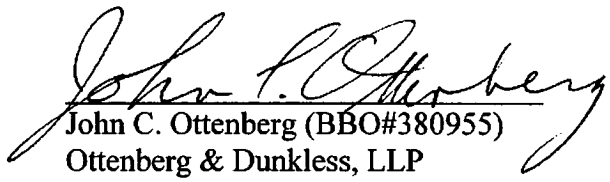
Finally, even if FERPA did apply, it does not prevent MIT from complying expeditiously with a DMCA subpoena. At most, FERPA would require the university to attempt to notify a student at the time of disclosure (or immediately prior to disclosure) of information in response to a subpoena.[9] A statutory requirement that notice must be given under FERPA does not provide any legal basis for delaying compliance, nor is there any practical reason for a delay. The information sought in the RIAA subpoena can be collected in a matter of *minutes* (via a simple search of computer records). There is thus no basis for MIT's argument that it was not given sufficient time for compliance. MIT Mem. at 9-10. Moreover, whatever argument MIT may once have had based on the expeditious response required by the subpoena, that argument is now moot. MIT cannot be heard to complain that it did not have enough time to notify the student by the time it filed its motion.

[9]MIT's argument with regard to those students who opt out of the school's directory listing is equally without merit. MIT Mem. at 10. MIT is confusing the disclosure of "directory information" pursuant to a subpoena, 20 U.S.C. § 1232g(b)(2)(B), with the publication of such information in a student directory, 20 U.S.C. § 1232g(a)(5)(A). That students can opt to keep their "directory information" out of the school's student directory has no bearing on the school's obligation to comply with a valid subpoena.

CONCLUSION

For all of these reasons, the Court should deny MIT's motion and dismiss this action or, if the Court considers the merits, order MIT to comply with the subpoena as soon as possible.

Respectfully Submitted,



John C. Ottenberg (BBO#380955)
Ottenberg & Dunkless, LLP
101 Arch Street
Boston, Ma. 02110
(617)342-8600

Donald B. Verrilli, Jr.
Steven B. Fabrizio
Thomas J. Perrelli
Jenner & Block, LLC
601 Thirteenth St., NW
Washington, D.C. 20005
(202) 639-6000

Matthew J. Oppenheim
Stanley Pierre-Louis
Recording Industry Association
of America
1330 Connecticut Ave., NW
Suite 300
Washington, D.C. 20036

August 1, 2003

Attorneys for the Recording Industry Association of America

C:\Gateway\WPfiles\WPFILES\RIAA\MIT Opp to motion to quash.FINAL.doc