UNITED STATES DISTRICT COURT FOR
THE DISTRICT OF COLUMBIA

IN RE: SUBPOENA TO MASSACHUSETTS INSTITUTE OF TECHNOLOGY	
RECORDING INDUSTRY ASSOCIATION OF AMERICA, Plaintiff, v. MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Defendant.	Misc. Act. No. 1:03-MS-00265 CASE NUMBER 1:03MS00265 JUDGE: Ellen Segal Huvelle DECK TYPE: Miscellanous DATE STAMP: 08/01/2003

MOTION TO ENFORCE SUBPOENA ISSUED TO THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY PURSUANT TO 17 U.S.C. § 512(h)

Pursuant to 17 U.S.C. § 512(h) and the Federal Rules of Civil Procedure, the Recording Industry Association of America (RIAA) hereby files this motion to compel the Massachusetts Institute of Technology's (MIT's) compliance with a subpoena issued by the clerk of this Court. *See Recording Industry Association of America v. MIT*, Misc. Act. No. 1:03-MS-00265 (D.D.C.). MIT has filed a motion to quash this subpoena in the United States District Court for the District of Massachusetts. (Attached hereto as Exhibit A.) But that court has no jurisdiction to quash a subpoena issued out of this Court. Because MIT has not complied with the subpoena and has no valid basis for failing to do so, this Court should compel MIT's compliance as soon as possible.

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. *Id.* 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*, 2003 WL 21488143, at *1 ("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 DMCA 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]

[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.

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 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. Prior to June of this year, no ISP refused 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.

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 that subpoena to MIT's DMCA designated agent, and provided information (in the form of an Internet Protocol (IP) address, date and time) sufficient to allow MIT to identify the infringer. After an exchange of correspondence in which MIT indicated its refusal to comply with the subpoena, MIT filed a motion to quash the subpoena in the United States District Court for the District of Massachusetts. Because only this Court can hear disputes over subpoenas issued by it, RIAA is filing this motion to enforce the subpoena; RIAA is also filing (in the District of Massachusetts) an opposition to MIT's motion to quash, arguing principally that the Massachusetts court has no authority to take any action with respect to subpoenas issued out of this Court.

ARGUMENT

The DMCA requires ISPs such as MIT to provide information sufficient to identify copyright infringers "notwithstanding any other provision of law." § 512(h)(5). RIAA delivered the subpoena to the person whom MIT has identified (as the DMCA requires) to be the contact for notifications of infringement. The DMCA requires nothing more to trigger the non-discretionary duty to disclose to RIAA the identities of individuals who have violated and continue to violate the copyrights of RIAA's members over the Internet. Because the subpoena was properly issued and delivered, this Court should compel MIT's compliance by requiring MIT to provide RIAA with the information requested in the subpoena. Moreover, given the DMCA's emphasis on expedition and the daily irreparable harm caused by the copyright infringement being committed here, RIAA requests that the Court act as expeditiously as possible in resolving this matter.

For its part, MIT has no substantive objection to the subpoena at issue in this case. MIT concedes that it must comply with a validly issued DMCA subpoena. MIT's sole argument appears to be that it must comply only with DMCA subpoenas issued out of the District of Massachusetts. That argument, however, is inconsistent with the language and purpose of the DMCA and, if accepted, would seriously undermine Congress's goal of ensuring that copyright owners can stop the massive infringement of their rights occurring daily on university and other computer networks. For all of these reasons, the Court should grant RIAA's motion and require MIT to comply as soon as possible.

I. MIT MUST COMPLY WITH DMCA SUBPOENAS, REGARDLESS OF ANY OTHER LEGAL OBLIGATIONS IT HAS

Under the DMCA, the service provider "*shall expeditiously disclose* to the copyright owner or person authorized by the copyright owner the information required by the subpoena,

notwithstanding any other provision of law and *regardless of whether the service provider responds to the notification*." § 512 (h)(5) (emphasis added). The words of the statute could not be more explicit. Thus, regardless of whether MIT has other obligations under other statutes or contractual agreements, it must nonetheless comply with a DMCA subpoena delivered to it. And it must comply expeditiously.

As Congress determined and as Judge Bates recognized in his two prior opinions on § 512(h), expedition is critical. *See Verizon I*, 240 F. Supp. 2d at 34; *Verizon II*, 257 F. Supp. 2d 244. Section 512(h) makes clear that the District Court clerk shall "expeditiously issue" the requested subpoena if all of the requirements are met and that, upon receipt, the service provider "shall expeditiously disclose" the information required by the subpoena. § 512(h)(5). The legislative history of § 512(h) describes issuance of the subpoena as a "ministerial" act, and emphasizes that it must be "performed quickly for this provision to have its intended effect." S. Rep. at 51. Without expedition, § 512(h) simply will fail to achieve the goals that Congress has for it.

MIT does not dispute that it has the information that RIAA is seeking, nor does it contend that complying with the subpoena is burdensome. MIT makes reference to the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, in the motion to quash filed in Massachusetts, but even that motion makes clear that FERPA provides no basis for refusing to respond to a DMCA subpoena. First, MIT concedes that FERPA would provide no basis for refusing to comply with a subpoena issued out of the District of Massachusetts. Second, the DMCA's injunction that ISPs comply "notwithstanding any other provision of law" trumps any obligation imposed by FERPA. Third, even under FERPA, the only obligation on MIT is to

attempt to notify students of the subpoena – which in no way prevents MIT from complying with the subpoena expeditiously.

MIT's only reason for refusing to comply is its claim that it must comply only with subpoenas issued out of the District of Massachusetts. As discussed below, that claim is wrong, and the Court should order MIT to comply with the subpoena issued from this Court as soon as possible.

II. THE SUBPOENA WAS VALIDLY ISSUED AND PROPERLY DELIVERED.

MIT claims that it does not have to respond to a subpoena issued by this Court and delivered to the DMCA agent that MIT was statutorily required to designate because the subpoena was not served within 100 miles of this district. As discussed below, while generally adopting procedures from Federal Rule of Civil Procedure 45, the DMCA does not impose this territorial limitation on subpoenas issued pursuant to the DMCA. Rather, Congress intended the DMCA subpoena process to be streamlined and expeditious to fulfill its functions; to that end, delivery of a subpoena to the ISP's DMCA designated agent must be understood to satisfy the statute's requirements.

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 compiling

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) ("[T]he 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.[2] Nonetheless, Congress viewed issuance and delivery of subpoenas as complementary to the process by which copyright owners send notices to the ISP's DMCA designated 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

---

[2]In *Verizon I*, an ISP argued that § 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. This Court wholly rejected that argument, finding that § 512(h) applies to all service providers performing all functions. *See Verizon I*, 240 F. Supp. 2d 24.

"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.[3] 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

---

[3]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 the goals of the DMCA.

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 DMCA agent, 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 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 other courts issued rulings contrary to *Bliss*, Congress itself made clear 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 of 1986, that nationwide service had been "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.[4] In *Browning,* the D.C. Circuit considered subpoenas issued by the FTC pursuant to 15 U.S.C. § 49. Section 49 read, 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]." 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

---

[4]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).

(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).[5]

For all of these reasons, the Court should find that Congress intended that DMCA subpoenas be served nationwide.

III. THIS COURT IS THE PROPER FORUM TO LITIGATE ENFORCEMENT OF RIAA'S SUBPOENA TO MIT.

It is well settled that only the court that issued a subpoena can quash that subpoena, and that other courts have no jurisdiction or authority to limit, quash, or, for that matter, enforce a subpoena from another court. *See* Charles Alan Wright & Arthur R. Miller, 9A *Federal Practice and Procedure*, § 2459 at 40-41 (2d ed. 1995) ("The 1991 amendments to Rule 45(c) now make it clear 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); *Pilcher v. Direct Equity Lending*, No. 99-1245-JTM, 2000 WL 33170865, at *4 (D. Kan. Dec. 22, 2000) (holding that 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 must

[5]Nothing in the language of 15 U.S.C. § 49 distinguishes it from the statute at issue here. Each statute 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; *Firestone Tire & Rubber Co.*, 455 F. Supp. at 1072; *FTC v. Cockrell*, 431 F. Supp. 558 (D.D.C. 1977). Thus, under either 15 U.S.C. § 49 or the DMCA, venue is proper in any court, but nationwide service is necessary to permit the investigation to proceed expeditiously.

be denied).[1] Rule 45 makes this plain by authorizing motions to quash solely in "the court by which a subpoena was issued." Fed. R. Civ. P. 45(c)(3)(A).

This Court – not the District of Massachusetts – is the arbiter for all objections to subpoenas issued from it. Indeed, MIT effectively concedes as much in the motion papers it filed in Massachusetts. The cases cited by MIT in its motion to quash 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. The News Corp., Ltd.*, 180 F.R.D. 391, 396-97 (D. Col. 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.

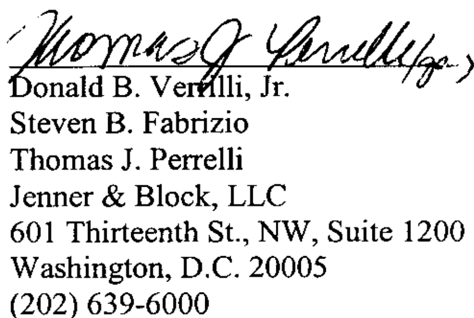
---

[1]*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").

CONCLUSION

For all of these reasons, this Court should order MIT to comply with the subpoena and disclose the information they seek as soon as possible.

Respectfully Submitted,



Donald B. Verrilli, Jr.
Steven B. Fabrizio
Thomas J. Perrelli
Jenner & Block, LLC
601 Thirteenth St., NW, Suite 1200
Washington, D.C. 20005
(202) 639-6000

Attorneys for the Recording Industry Association of America

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

July 31, 2003

CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing Motion to Enforce Subpoena Issued to the Massachusetts Institute of Technology Pursuant to 17 U.S.C. § 512(h) and the accompanying proposed order were served upon the following by Federal Express on July 31, 2003:

Jeffrey Swope
Palmer & Dodge LLP
111 Huntington Ave.
Boston, Massachusetts 02199

James A. Trilling

EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

In Re Subpoena to The Massachusetts Institute of Technology	Civil Action No. 03- -MBD (United States District Court for the District of Columbia Nos. 1:03MS00265)

MEMORANDUM OF THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY IN SUPPORT OF ITS MOTION TO QUASH SUBPOENAS AND FOR A PROTECTIVE ORDER PURSUANT TO FED. R. CIV. P. 45(c)(3)(A)

The Massachusetts Institute of Technology (MIT) moves to quash, and for a protective order regarding, a subpoena duces tecum served upon it by Recording Industry Association of America, Inc. (RIAA) under provisions of the Digital Millennium Copyright Act (DMCA). The subpoena was issued to MIT as part of what the recording industry has publicly announced is a nationwide initiative against copyright infringement committed by individuals who, without authority, offer copies of sound recordings for download over the Internet. Under that initiative, the RIAA is issuing subpoenas to providers of Internet services to discover the identities of individuals alleged to have infringed the copyrights of RIAA-member record companies. Once the individuals have been identified, the RIAA or its members plan to file claims for damages against them. College students have been identified by the RIAA as prime suspects in such alleged infringement.

MIT emphasizes at the outset that its motion is not intended to prevent the RIAA from obtaining information to which it is entitled under the DMCA, or to shield the disclosure of the identities of any individuals who are the subjects of the subpoena. The motion is instead filed solely for the purposes of:

- assuring that the subpoena is validly issued, because to the extent that the subpoena seeks information about MIT students that constitutes an "education record" pursuant to the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, MIT may disclose such information only in response to a "lawfully issued subpoena";
- assuring that the subpoena is issued from a nearby United States District Court, as required by Fed. R. Civ. P. 45(a)(2) and (b)(2), so that MIT has a convenient forum in which to seek judicial assistance regarding such subpoenas, which is a principal purpose of Fed. R. Civ. P. 45; and
- assuring that subpoena, when validly issued, allows MIT time to provide reasonable prior notice to any student whose education records may be produced in response to the subpoena, as required by FERPA.

If the RIAA issues a subpoena to MIT that satisfies these requirements of the Federal Rules of Civil Procedure and of federal law, MIT will of course provide the information that the subpoena rightfully requires it to produce, to the extent that such information is found, after a reasonably diligent search, to be in the Institute's possession, custody, or control.

Statement of Facts

The RIAA has served a subpoena upon MIT pursuant to the DMCA, 17 U.S.C. § 512(h), seeking information, including names, addresses, telephone numbers, and email addresses, sufficient to identify the alleged infringer of copyrighted sound recordings who has the specific Internet Protocol address identified in the subpoena. The subpoena requires production "on the 7th calendar day after the *issuance date* of Subpoena" (italics added), but was not served until several days after the issuance date, leaving MIT insufficient time to issue a prior notice to any student whose education record would be produced in response to the subpoena.

MIT sent the RIAA objections pursuant to Fed. R. Civ. P. 45(c)(2)(B), because the subpoena had not been lawfully issued and served in compliance with Fed. R. Civ. P. 45(b)(2), and because it required a response too soon to allow MIT to give the notice required by FERPA. By letter dated July 15, 2003, a copy of which is annexed to this memorandum as Attachment A, counsel for the RIAA rejected the objections of MIT and demanded compliance with the subpoena.

ARGUMENT

MIT has no objection to providing information responsive to the RIAA's request as long as that request is embodied in a lawfully issued subpoena, which is the only basis on which MIT can be required to respond, and which is also a requirement of FERPA. The subpoena must also allow MIT reasonable time to comply with its FERPA obligation to notify any students if his or her education record will be produced in response to the subpoena.

I. MIT IS REQUIRED BY FEDERAL LAW NOT TO DISCLOSE STUDENT RECORDS IN RESPONSE TO A SUBPOENA UNLESS THAT SUBPOENA HAS BEEN "LAWFULLY ISSUED."

FERPA defines an "education record" as records, files, documents, and other materials that "(i) contain information directly related to a student; and (ii) are maintained by an educational . . . institution" (20 U.S.C. § 1232g(a)(4)(a)). Educational institutions may not disclose personally identifiable information about a student from an "education record" except in lied circumstances (20 U.S.C. § 1232g(b)(2)). One such circumstance is when "such information is furnished . . . pursuant to any *lawfully* issued subpoena," as long as the educational institution provides the student notice in advance of complying with the subpoena (20 U.S.C. § 1232g(b)(2)(B)) (italics added).

As a result, MIT is obligated by federal law to assure that the RIAA subpoena that would require it to disclose student records was lawfully issued. (Of course, to the extent that information responsive to the RIAA subpoena was not an education record concerning a MIT student, the FERPA requirements would not apply. But without a lawfully issued subpoena, MIT would not be required to produce that information, either.)

II. THE RIAA SUBPOENA WAS NOT LAWFULLY ISSUED AND SERVED, IN VIOLATION OF FED. R. CIV. P. 45(a)(2) AND (b)(2)

The DMCA requires that "the procedure for issuance and delivery" of any subpoena issued pursuant to the DMCA "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" (17 U.S.C. § 512(h)(6)). The Federal Rules of Civil Procedure prescribe from which District Courts subpoenas to nonparties that require production of records may be issued, and where they may be

served, unless a statute of the United States authorizes service at any other place. Fed. R. Civ. P. 45(a)(2) and (b)(2). The RIAA subpoena violates those requirements of the Federal Rules of Civil Procedure because it was issued from the United States District Court for the District of Columbia and was served on MIT in Massachusetts to produce documents in Washington, D.C. Nothing in the DMCA permits service at any other places than those authorized by the Federal Rules of Civil Procedure.

1. **Fed. R. Civ. P. 45(a)(2) and (b)(2) require that a subpoena duces tecum be issued from a convenient United States District Court, so that a third-party like MIT may seek judicial assistance without the burden of travelling to a distant district.**

The Federal Rules of Civil Procedure provide protection to a third-party, like MIT, that receives a subpoena duces tecum, so that the recipient may avoid undue burden by having to litigate the validity of the subpoena in an inconvenient forum. The Rules accomplish this end by:

- first, providing that a subpoena for production of documents must issue from the court for the district in which the production is to be made (Fed. R. Civ. P. 45(a)(2)), and
- second, providing that subpoenas may only be served outside the district from which they issue if that place of service is "within 100 miles of the place of the . . . production specified in the subpoena" (Fed. R. Civ. P. 45(b)(2)).[1]

---

[1] In addition, service may be made "at any place within the state where a state statute or rule of court permits service of a subpoena issued by a state court of general jurisdiction sitting in the place of the . . . production . . . specified in the subpoena" (*id.*), in effect expanding the 100-mile rule to allow service anywhere in the Commonwealth for a subpoena that requires production in Massachusetts.

"[T]erritorial limitations on service of subpoenas are meant to prevent 'undue inconvenience' to witnesses" (9 James Wm. Moore et al., Moore's Federal Practice § 45.03[4][c] (3d ed. 2003)).

MIT does not contend that production of records responsive to the RIAA's subpoena would itself be inconvenient or burdensome. The Institute acknowledges that it could readily deliver the requested identification information to the RIAA's counsel in Washington, D.C.

But it is a completely different kind of undue inconvenience and burden that is at issue in this matter for MIT: whether MIT must go to the District Court for the District of Columbia to obtain protection from a subpoena, like the RIAA's in this case, that has been issued in violation of the Federal Rules of Civil Procedure and of FERPA. It is obviously significantly more inconvenient and burdensome for MIT to retain counsel to appear for it in the District of Columbia than to use local counsel routinely retained by it to represent it in courts located in Massachusetts.[2]

There can be no doubt that the RIAA subpoena was not issued and served in accordance with the territorial constraints of Fed. R. Civ. P. 45(a)(2) and (b)(2). *See, e.g.*,

---

[2] MIT filed its Motion to Quash Subpoenas and for a Protective Order in the United States District Court for Massachusetts, from which the subpoena should have issued, rather than in the United States District Court for the District of Columbia, from which the subpoena was wrongly issued. This Court should take jurisdiction of this matter despite the fact that Fed. R. Civ. P. 45(c)(3)(A) provides that motions should be made to "the court by which a subpoena was issued," because the RIAA issued the subpoena from the wrong court. A rule that relies on not imposing undue burdens to third parties should not require third parties to travel to an inconvenient forum to contest a subpoena that was not lawfully issued. As the Court said in *Echostar Communications Corp.* v. *The News Corporation, Ltd.*, 180 F.R.D. 391, 397 (D. Colo. 1998), "it is burdensome to expect . . . [the nonparties subpoenaed to produce documents in Georgia and New Jersey] either *to litigate the validity of the subpoena* here in Colorado, or to produce the documents here in Colorado" (italics added). *See also Kupritz* v. *Savannah College of Art and Design*, 155 F.R.D. 84, 88 (E.D. Pa. 1994) (court from which the subpoena should have issued

Kupritz v. *Savannah College of Art and Design*, 155 F.R.D. 84, 88 (E.D. Pa. 1994) (where subpoena was issued from the Southern District of Georgia for discovery in Pennsylvania, "[i]t was simply wrong"). The RIAA did not contend otherwise in its counsel's letter to MIT (Att. A).

2. The DMCA provides no exception to these requirements of Fed. R. Civ. P. 45(b)(2), and on the contrary requires that those rules be followed "to the greatest extent practicable."

The RIAA's contention that the subpoena was lawfully issued, as stated in its letter to MIT, is based upon the exception in Fed. R. Civ. P. 45(b)(2) that allows service in another place if a statute of the United States authorizes such service (Att. A, p. 1). The DMCA provides in 17 U.S.C. § 512(h)(1) that the representative of a copyright owner "may request the clerk of *any* United States district court to issue a subpoena" (italics added) for the identification of an alleged copyright infringer. Based upon this language, the RIAA contends that the DMCA permits nationwide service.

In fact, all that the phrase "any United States district court" signifies, by its plain meaning, is that a copyright holder need not go to any particular court to issue a DMCA subpoena, but may instead have it issued from any district in the federal court system that has authority to issue such a subpoena. Moreover, other language in the DMCA expressly refutes the RIAA's claim that the phrase "any United States district court" should be read to override the rules that normally limit which District Courts may issue subpoenas in particular cases. The DMCA expressly provides that "the procedure for *issuance* and *delivery* of the subpoena . . . shall be governed *to the greatest extent*

---

finds subpoena issued from wrong court invalid).

practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum" (17 U.S.C. § 512(h)(6)).

The United States Supreme Court long ago rejected the contention made by the RIAA. In *Robertson* v. *Railroad Labor Board*, 268 U.S. 619, 627 (1925) (Brandeis, J.), the Court held that the phrase "any District Court of the United States" means only a court that has jurisdiction under otherwise applicable rules to issue the subpoena. While that decision was issued before the Federal Rules of Civil Procedure existed, it is no less a determinative precedent. The statute at issue in the *Robertson* case gave an administrative board subpoena powers, and allowed that board "to invoke the aid of any United States district court" to enforce its subpoenas. Judicial procedure at that time was governed by the Judicial Code, which provided the rules for where such actions could be maintained based on the locations of the parties subpoenaed. The Court's holding in *Robertson* that the phrase "any United States district court" does not override otherwise applicable rules governing which court may issue a subpoena is therefore just as applicable in the context of the Federal Rules of Civil Procedure and the DMCA today.

The cases that the RIAA cited in its letter to MIT arguing that the DMCA authorizes nationwide service of process (Att. A, p. 2) are readily distinguishable. They arose under the Federal Trade Commission Act, which authorizes subpoenas to be enforced by "[a]ny of the district courts of the United States *within the jurisdiction of which such inquiry is carried on*" (15 U.S.C. § 49 (italics added)), and the Federal Election Campaign Act, which authorizes (in nearly identical language) subpoenas to be enforced by "[a]ny of the district courts of the United States *within the jurisdiction of which any inquiry is carried on*" (2 U.S.C. § 437d(b) (punctuation from the statute as it

read when interpreted by the court in the case cited in the RIAA letter, italics added)). The language in the DMCA that authorizes the issuance of subpoenas lacks the essential language, italicized in the previous quotes, that allows for nationwide service.

As this Court said in *Federal Deposit Insurance Corporation* v. *Abrams*, 893 F. Supp. 4, 5 (D. Mass. 1995) (internal quotations and citations omitted), "Congress knows how to authorize nationwide service of process when it wants to provide for it. That Congress failed to do so . . . argues forcefully that such an authorization was not its intention."

III. BECAUSE MIT IS REQUIRED BY FERPA TO PROVIDE PRIOR NOTICE TO A STUDENT BEFORE DISCLOSING THE STUDENT'S EDUCATION RECORD IN RESPONSE TO A SUBPOENA, A LAWFULLY ISSUED RIAA SUBPOENA MUST ALLOW MIT REASONABLE TIME TO PROVIDE SUCH NOTICE.

The letter from the RIAA also disputed a second ground of objection filed by MIT, which was that the time the subpoena permitted for production was too short to allow MIT to satisfy its obligation under FERPA to provide any student prior notice if his or her education record would be provided in response to the subpoena (*see* p. 3, above). (MIT emphasizes that it does not content that FERPA prevents the disclosure of information about a student in response to a lawfully issued subpoena, but merely that FERPA requires MIT to give the student advance notice that his or her education records have been subpoenaed, so that the student has the opportunity to seek protection from that subpoena if he or she wishes to do so.)

While the DMCA provides (17 U.S.C. § 512(h)(5)) that, "notwithstanding any other provision of law," service providers that receive DMCA subpoenas must "expeditiously disclose" the information sought in the subpoena, those provisions cannot

be read to override a MIT's FERPA obligation to notify a student when a subpoena requires disclosure of the student's education records. As the Supreme Court said in *Morton* v. *Mancari*, 417 U.S. 535, 551 (1974):

> "The courts are not at liberty to pick and choose among congressional enactments, and when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective."

Nothing in the DMCA establishes the time boundaries for an "expeditious" disclosure. Permitting MIT to take the few days needed to provide a student reasonable FERPA notice would not conflict with MIT's DMCA obligation to supply information in a timely manner in response to a lawfully issued RIAA subpoena.[3]

The RIAA pointed out in its letter that FERPA excepts "directory information" from the definition of an "education record," and claimed that all its subpoena seeks is directory information (Att. A, p. 3). The RIAA is correct that, for a student who has not opted out of the provision,[4] colleges may disclose his or her name, address, and other such information that is typical of student directories (20 U.S.C. § 1232g(a)(5)). But the RIAA subpoena requires disclosure not merely of a student's name and address. It instead requires the disclosure of the name and address of the student who allegedly used a campus computer for copyright infringement. By coupling the name with the alleged

---

[3] The RIAA letter conceded that the delay between the issuance of the subpoena by the United States District Court for the District of Columbia (which subpoena states that responses are due within seven calendar days) and the RIAA's service on MIT left the Institute only two days in which to respond (Att. A, p. 3). The letter offered no explanation for the delay. The letter went on to suggest that MIT could satisfy its duties under FERPA by simultaneously notifying the student and producing the information (*id.*) That suggestion overlooks the FERPA mandate that such notice be "in advance" of disclosure of the education records (20 U.S.C. § 1232g(b)(2)(B)).

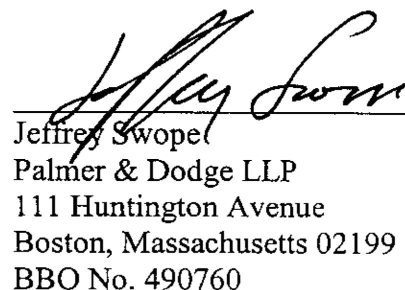
[4] Of course, RIAA's argument fails at the threshold for any student who has exercised his or her FERPA right to refuse permission for release even of directory information. But as explained in

activities, the information is no longer simply "directory," but is precisely the kind of information to which FERPA applies. If the position of the RIAA were correct, colleges and universities could be required to disclose "just the names and addresses" of students who received certain grades, who used campus counseling services, or who were subject to campus disciplinary proceedings. In each case, it is the question as well as the answer that would make any information provided more than mere "directory information."

CONCLUSION

For the reasons stated in this memorandum, MIT requests that the Court quash the subpoena served upon it (United States District Court for the District of Columbia Nos. 1:03MS00265), and further that the Court issue a protective order stating that, if and when the RIAA serves MIT with a lawfully issued subpoena, that subpoena must permit MIT sufficient time before the date set for production to give reasonable prior notice to any student whose education record may be produced in response to such a subpoena, as required by FERPA.

Respectfully submitted,



Jeffrey Swope
Palmer & Dodge LLP
111 Huntington Avenue
Boston, Massachusetts 02199
BBO No. 490760

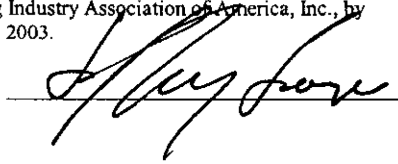
Dated: July 21, 2003

---

the remainder of this section, the more fundamental reason the argument of the RIAA fails is that it wrongly characterizes the information sought as "directory."

CERTIFICATE OF SERVICE

I hereby certify that I caused a true copy of the above document to be served upon Thomas J. Perrelli, Jenner & Block LLC, attorney of record for the Recording Industry Association of America, Inc., by telefacsimile on July 21, 2003.



ATTACHMENT A

JENNER&BLOCK

July 15, 2003

Jenner & Block, LLC
601 Thirteenth Street, NW
Suite 1200 South
Washington, DC 20005-3823
Tel 202 639-6000
www.jenner.com

Chicago
Dallas
Washington, DC

Thomas J. Perrelli
Tel 202 639-6004
Fax 202 636-6066
tperrelli@jenner.com

FACSIMILE AND MAIL

Mark C. DiVincenzo
Massachusetts Institute of Technology
Litigation & Risk Management Counsel
Senior Counsel's Office
77 Massachusetts Avenue
Building 12-090
Cambridge, MA 02139-4307

Re: Objections to DMCA subpoena from RIAA

Dear Mr. DiVincenzo:

I am writing on behalf of the Recording Industry Association of America in response to your objection to the subpoena served by RIAA pursuant to the Digital Millennium Copyright Act. For the reasons discussed below, your objections are not well-taken. We request that you withdraw them and comply with the subpoena as soon as possible.

As you are aware, Section 512(h) of the DMCA requires service providers, including universities providing internet access and other computer services to their students, to respond to subpoenas issued by "the clerk of any United States district court." 17 U.S.C. § 512(h)(1). Congress was crystal clear that this obligation on service providers was non-discretionary; indeed, Congress required service providers to comply with the subpoena "notwithstanding any other provision of law." 17 U.S.C. § 512(h)(5). This broad mandate was part of Congress's express intention to make the DMCA subpoena process as "expeditious" as possible – with the explicit goal of avoiding unnecessary conflict between copyright owners and service providers.

You have raised four objections to the subpoena served on you, none of which are consistent with the text or purpose of the DMCA. For the reasons explained below, we request that you withdraw your objections. If you do not, we will have no choice but to move to compel a response to the subpoena.

1. You claim that the subpoena is invalid because it violates Fed. R. Civ. P. 45(b)(2). That argument fails for multiple reasons. In the DMCA, Congress authorized "the clerk of any United States district court" to issue a subpoena. 17 U.S.C. § 512(h)(1). Through that language, Congress has expressly provided for issuance of subpoenas by any district court and nationwide service. In so doing, Congress recognized two things: 1) the non-physical nature of the Internet where infringing material, as well as the records that may pertain to such infringement, may reside anywhere and where infringing conduct necessarily occurs on a nationwide (indeed, international) scale and 2) the critical need for copyright owners to obtain information as soon as

Attachment A

possible so that they can stop and obtain redress for the ongoing infringement that is irreparably harming their interests.

The DMCA's reference to Rule 45 is not to the contrary. Section 512(h) does not incorporate all aspects of Rule 45; rather, pursuant to 17 U.S.C. § 512(h)(6), the provisions of Rule 45 are incorporated only "to the greatest extent practicable." Thus, where the DMCA itself extends authority beyond that of Rule 45 or where any requirement of Rule 45 is inconsistent with Congress's intent in enacting the DMCA, Rule 45's limitations must yield. Indeed, Rule 45 itself acknowledges that, where Congress has otherwise provided for service beyond the territorial limitations of the issuing district court, Rule 45(b)(2) simply does not apply. *See* Rule 45(b)(2) (allowing alternative service "[w]hen a statute of the United States provides thereof"). Congress has so provided in the DMCA.

Your argument is not only inconsistent with the text of the DMCA, but also with Congress's intent and the legislative history. As the D.C. Circuit has recognized, Congress may authorize nationwide service, either expressly or impliedly. Thus, the D.C. Circuit has held that a statute authorizing subpoenas and enforcement thereof in any district court provides for nationwide service where such service "effectuate[s] the purpose of the regulatory regime." *Federal Trade Commission v. Browning*, 435 F.2d 96, 100 (D.C.Cir. 1970); *Federal Election Commission v. Committee to Elect Lyndon LaRouche*, 613 F. 2d 849, 859 (D.C. Cir. 1980) (same); *Federal Trade Commission v. Cockrell*, 431 F.Supp. 558, 559 (D.D.C. 1977) (where inquiry is "nationwide," service anywhere in the U.S. and enforcement in the District of Columbia are appropriate).

Authorizing service of subpoenas nationwide is a key component of Congress's specific mandate that service providers "expeditiously disclose to the copyright owner . . . the information required by the subpoena." 17 U.S.C. § 512(h)(5). As the District Court for the District of Columbia has already held, the DMCA must be interpreted in light of "Congress's express and repeated direction to make the subpoena process 'expeditious.'" *In re: Verizon Internet Services, Inc. Subpoena Enforcement Matter*, 240 F.Supp. 24, 34 (D.D.C. 2003). "The statute contemplates a rapid subpoena process designed to quickly identify apparent infringers and then curtail infringement." *Id.* To interpret the statute as you suggest would vitiate Congress's fundamental goal in enacting Section 512(h).

Moreover, your argument is inconsistent with the remainder of Section 512. In Section 512, Congress sought to streamline the efforts of copyright owners and service providers in fighting against digital piracy. Congress thus required all service providers to, for example, establish a single point of contact for all DMCA take-down notifications, 17 U.S.C. § 512(c)(2), regardless of where those notifications come from. Congress expressly contemplated that DMCA subpoenas and take-down notices would be served in conjunction with each other. To suggest that Congress intended service providers to disable access to infringing material in response to requests nationwide, but to ignore the subpoenas to identify infringers that accompany those notices makes little sense.

In contrast to the irreparable harm that occurs every day to copyright owners while the infringement at issue in this case is allowed to continue, requiring compliance with a subpoena issued in the District of Columbia works no hardship on the university or any other service provider. The DMCA does not require witnesses to travel or give testimony; it only requires production of limited, specific information that is easily retrieved from your files. Regardless of where the subpoena is issued, a service provider can easily comply and is subject to virtually no burden.

Your refusal to provide information is also inconsistent with the practice of DMCA subpoenas to date. Since enactment of the DMCA and prior to its most recent enforcement effort, RIAA has obtained and served over 100 subpoenas under the DMCA. Each of those subpoenas was issued by the clerk of the United States District Court for the District of Columbia. No service provider has ever previously objected to those subpoenas on the ground that you now raise. Other ISPs understand the statute as RIAA does – it authorizes issuance of subpoenas by any district court and service wherever the service provider resides.

2. Your complaint that the subpoena requires production of information too quickly is also not well-taken. The DMCA makes clear that a service provider must respond to the subpoena "expeditiously." 17 U.S.C. § 512(h)(5). Given that the computer look-up required to comply cannot take more than a few minutes (as other service providers have conceded), there is no basis to claim two days are insufficient to obtain and disclose the information required. In any case, this objection has clearly been mooted with the passage of time.

3. You also suggest that the Family Education Rights and Privacy Act, 20 U.S.C. § 1232g(b)(2), somehow prevents the university from complying with its obligations under the DMCA. That argument is also without merit. FERPA does not in any way preclude compliance with the DMCA. As an initial matter, the provisions of FERPA could not trump the university's obligation to respond to a DMCA subpoena. Congress made clear that service providers must comply with DMCA subpoenas "notwithstanding any other provision of law." Such language makes manifest Congress's intent that other legal obligations must give way to the urgent need to stop ongoing violations of law.

In any case, the university's obligations under FERPA do not in any way conflict with its obligations under the DMCA. FERPA applies only to "personally identifiable information in education records *other than directory information*." 20 U.S.C. § 1232g(b)(2) (emphasis added). Under the statute, "directory information" expressly includes the very identifying information that the DMCA requires the university to provide. Thus, FERPA, by its own terms, does not even apply to the information that the subpoena compels. Moreover, under FERPA, the only obligation on the university would be to notify the student and/or parents of the student. Thus, even if FERPA did apply, the university could easily comply with both statutes by notifying the student, while also expeditiously disclosing the information to the copyright owner. For all of these reasons, FERPA provides no basis for objecting to the subpoena in this case.

4. You claim that the word "information" is vague and does not identify the "documents" sought under the subpoena. That objection misconceives the nature of a DMCA

subpoena. RIAA does not seek documents from the university. Rather, pursuant to express statutory authority, RIAA seeks "information sufficient to identify the alleged infringer." 17 U.S.C. § 512(h)(3). In the ordinary case, we believe that name, address(es), phone number(s), and e-mail address(es) should be sufficient to identify the infringer. That is all that we are asking MIT to provide at this time, and thus the claim that the request is overbroad or vague is simply incorrect.

For all of these reasons, we request that you withdraw your objections and disclose the information required by the subpoena as soon as possible. Please do not hesitate to contact me (202-639-6004) if you have questions or wish to discuss this matter further.

Sincerely,

Thomas J. Perrelli