United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 16, 2003 Decided December 19, 2003

No. 03-7015

Recording Industry Association of America, Inc.,
Appellee

v.

Verizon Internet Services, Inc.,
Appellant

Consolidated with
03-7053

Appeals from the United States District Court
for the District of Columbia
(No. 02ms00323)
(No. 03ms00040)

Andrew G. McBride argued the cause for appellant. With him on the briefs were John Thorne, Bruce G. Joseph, and Dineen P. Wasylik. Deanne E. Maynard entered an appearance.

Megan E. Gray, Lawrence S. Robbins, Alan Untereiner, Christopher A. Hansen, Arthur B. Spitzer, and Cindy Cohn were on the brief for amici curiae Alliance for Public Technology, et al., in support of appellant.

Donald B. Verrilli, Jr. argued the cause for appellee Recording Industry Association of America, Inc. With him on the brief were Thomas J. Perrelli and Matthew J. Oppenheim.

Scott R. McIntosh, Attorney, U.S. Department of Justice, argued the cause for intervenor-appellee United States. With him on the brief were Roscoe C. Howard, Jr., U.S. Attorney, and Douglas N. Letter, Attorney, U.S. Department of Justice.

Paul B. Gaffney, Thomas G. Hentoff, Eric H. Smith, Patricia Polach, Ann Chaitovitz, Allan R. Adler, Joseph J. DiMona, Robert S. Giolito, and Chun T. Wright were on the brief for amici curiae Motion Picture Association of America, et al., in support of appellee Recording Industry Association of America. David E. Kendall entered an appearance.

Paul Alan Levy, Alan B. Morrison, and Allison M. Zieve were on the brief for amicus curiae Public Citizen.

Before: Ginsburg, Chief Judge, and Roberts, Circuit Judge, and Williams, Senior Circuit Judge.

Opinion for the Court filed by Chief Judge Ginsburg.

Ginsburg, Chief Judge: This case concerns the Recording Industry Association of America's use of the subpoena provision of the Digital Millennium Copyright Act, 17 U.S.C. s 512(h), to identify internet users the RIAA believes are infringing the copyrights of its members. The RIAA served two subpoenas upon Verizon Internet Services in order to discover the names of two Verizon subscribers who appeared to be trading large numbers of .mp3 files of copyrighted music via "peer-to-peer" (P2P) file sharing programs, such as

KaZaA. Verizon refused to comply with the subpoenas on various legal grounds.

The district court rejected Verizon's statutory and constitutional challenges to s 512(h) and ordered the internet service provider (ISP) to disclose to the RIAA the names of the two subscribers. On appeal Verizon presents three alternative arguments for reversing the orders of the district court: (1) s 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others; if the statute does authorize such a subpoena, then the statute is unconstitutional because (2) the district court lacked Article III jurisdiction to issue a subpoena with no underlying "case or controversy" pending before the court; and (3) s 512(h) violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously. Because we agree with Verizon's interpretation of the statute, we reverse the orders of the district court enforcing the subpoenas and do not reach either of Verizon's constitutional arguments.*

## I. Background

Individuals with a personal computer and access to the internet began to offer digital copies of recordings for download by other users, an activity known as file sharing, in the late 1990's using a program called Napster. Although recording companies and music publishers successfully obtained an injunction against Napster's facilitating the sharing of files containing copyrighted recordings, see A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), millions of people in the United States and around the world continue to

---

* The district court's jurisdiction to issue the orders here under review is not drawn into question by Verizon's Article III argument. See Interstate Commerce Comm'n v. Brimson, 154 U.S. 447, 476-78 (1894) (application of ICC to enforce subpoena issued by agency in furtherance of investigation presents "case or controversy" subject to judicial resolution).

share digital .mp3 files of copyrighted recordings using P2P computer programs such as KaZaA, Morpheus, Grokster, and eDonkey. See John Borland, File Swapping Shifts Up a Gear (May 27, 2003), available at http://news.com.com/2100-1026-1009742.html, (last visited December 2, 2003). Unlike Napster, which relied upon a centralized communication architecture to identify the .mp3 files available for download, the current generation of P2P file sharing programs allow an internet user to search directly the .mp3 file libraries of other users; no web site is involved. See Douglas Lichtman & William Landes, Indirect Liability for Copyright Infringement: An Economic Perspective, 16 Harv. J. Law & Tech. 395, 403, 408-09 (2003). To date, owners of copyrights have not been able to stop the use of these decentralized programs. See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003) (holding Grokster not contributorily liable for copyright infringement by users of its P2P file sharing program).

The RIAA now has begun to direct its anti-infringement efforts against individual users of P2P file sharing programs. In order to pursue apparent infringers the RIAA needs to be able to identify the individuals who are sharing and trading files using P2P programs. The RIAA can readily obtain the screen name of an individual user, and using the Internet Protocol (IP) address associated with that screen name, can trace the user to his ISP. Only the ISP, however, can link

the IP address used to access a P2P program with the name and address of a person - the ISP's customer - who can then be contacted or, if need be, sued by the RIAA.

The RIAA has used the subpoena provisions of s 512(h) of the Digital Millennium Copyright Act (DMCA) to compel ISPs to disclose the names of subscribers whom the RIAA has reason to believe are infringing its members' copyrights. See 17 U.S.C. s 512(h)(1) (copyright owner may "request the clerk of any United States district court to issue a subpoena to [an ISP] for identification of an alleged infringer"). Some ISPs have complied with the RIAA's s 512(h) subpoenas and identified the names of the subscribers sought by the RIAA. The RIAA has sent letters to and filed lawsuits against

several hundred such individuals, each of whom allegedly made available for download by other users hundreds or in some cases even thousands of .mp3 files of copyrighted recordings. Verizon refused to comply with and instead has challenged the validity of the two s 512(h) subpoenas it has received.

A copyright owner (or its agent, such as the RIAA) must file three items along with its request that the Clerk of a district court issue a subpoena: (1) a "notification of claimed infringement" identifying the copyrighted work(s) claimed to have been infringed and the infringing material or activity, and providing information reasonably sufficient for the ISP to locate the material, all as further specified in s 512(c)(3)(A); (2) the proposed subpoena directed to the ISP; and (3) a sworn declaration that the purpose of the subpoena is "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting" rights under the copyright laws of the United States. 17 U.S.C. ss 512(h)(2)(A)-(C). If the copyright owner's request contains all three items, then the Clerk "shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the [ISP]." 17 U.S.C. s 512(h)(4). Upon receipt of the subpoena the ISP is "authorize[d] and order[ed]" to disclose to the copyright owner the identity of the alleged infringer. See 17 U.S.C. ss 512(h)(3), (5).

On July 24, 2002 the RIAA served Verizon with a subpoena issued pursuant to s 512(h), seeking the identity of a subscriber whom the RIAA believed to be engaged in infringing activity. The subpoena was for "information sufficient to identify the alleged infringer of the sound recordings described in the attached notification." The "notification of claimed infringement" identified the IP address of the subscriber and about 800 sound files he offered for trading; expressed the RIAA's "good faith belief" the file sharing activity of Verizon's subscriber constituted infringement of its members' copyrights; and asked for Verizon's "immediate assistance in stopping this unauthorized activity." "Specifically, we request that you remove or disable access to the infringing sound files via your system."

When Verizon refused to disclose the name of its subscriber, the RIAA filed a motion to compel production pursuant to Federal Rule of Civil Procedure 45(c)(2)(B) and s 512(h)(6) of the Act. In opposition to that motion, Verizon argued s 512(h) does not apply to an ISP acting merely as a conduit for an individual using a P2P file sharing program to exchange files. The district court rejected Verizon's argument based upon "the language and structure of the statute, as confirmed by the purpose and history of the legislation," and ordered Verizon to disclose to the RIAA the name of its subscriber. In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 45 (D.D.C. 2003) (Verizon I).

The RIAA then obtained another s 512(h) subpoena directed to Verizon. This time Verizon moved to quash the subpoena, arguing that the district court, acting through the Clerk, lacked jurisdiction under Article III to issue the subpoena and in the alternative that s 512(h) violates the First Amendment. The district court rejected Verizon's constitutional arguments, denied the motion to quash, and again ordered Verizon to disclose the identity of its subscriber. In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 247, 275 (D.D.C. 2003) (Verizon II).

Verizon appealed both orders to this Court and we consolidated the two cases. As it did before the district court, the RIAA defends both the applicability of s 512(h) to an ISP acting as a conduit for P2P file sharing and the constitutionality of s 512(h). The United States has intervened solely to defend the constitutionality of the statute.

## II. Analysis

The court ordinarily reviews a district court's grant of a motion to compel or denial of a motion to quash for abuse of discretion. See, e.g., In re Sealed Case, 121 F.3d 729, 740 (D.C. Cir. 1997). Here, however, Verizon contends the orders of the district court were based upon errors of law, specifically errors regarding the meaning of s 512(h). Our review is therefore plenary. See In re Subpoena Served Upon the Comptroller of the Currency, 967 F.2d 630, 633 (D.C. Cir. 1992).

The issue is whether s 512(h) applies to an ISP acting only as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or, as in this case, sharing P2P files. Verizon contends s 512(h) does not authorize the issuance of a subpoena to an ISP that transmits infringing material but does not store any such material on its servers. The RIAA argues s 512(h) on its face authorizes the issuance of a subpoena to an "[internet] service provider" without regard to whether the ISP is acting as a conduit for user-directed communications. We conclude from both the terms of s 512(h) and the overall structure of s 512 that, as Verizon contends, a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.

### A. Subsection 512(h) by its Terms

We begin our analysis, as always, with the text of the statute. See Barnhart v. Sigmon Coal Co., 534 U.S. 438, 450 (2002). Verizon's statutory arguments address the meaning of and interaction between ss 512(h) and 512(a)-(d). Having already discussed the general requirements of s 512(h), we now introduce ss 512(a)-(d).

Section 512 creates four safe harbors, each of which immunizes ISPs from liability for copyright infringement under certain highly specified conditions. Subsection 512(a), entitled "Transitory digital network communications," provides a safe harbor "for infringement of copyright by reason of the [ISP's] transmitting, routing, or providing connections for" infringing material, subject to certain conditions, including that the transmission is initiated and directed by an internet user. See 17 U.S.C. ss 512(a)(1)-(5). Subsection 512(b), "System caching," provides immunity from liability "for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the [ISP]," s 512(b)(1), as long as certain conditions regarding the transmission and retrieval of the material created by the ISP are met. See 17 U.S.C. ss 512(b)(2)(A)-(E). Subsection 512(c), "Information residing

on systems or networks at the direction of users," creates a safe harbor from liability "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider," as long as the ISP meets certain conditions regarding its lack of knowledge concerning, financial benefit from, and expeditious efforts to remove or deny access to, material that is infringing or that is claimed to be the subject of infringing activity. See 17 U.S.C. ss 512(c)(1)(A)-(C). Finally, s 512(d), "Information location tools," provides a safe harbor from liability "for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools" such as "a directory, index, reference, pointer, or hypertext link," subject to the same conditions as in ss 512(c)(1)(A)-(C). See 17 U.S.C. ss 512(d)(1)-(3).

Notably present in ss 512(b)-(d), and notably absent from s 512(a), is the so-called notice and take-down provision. It makes a condition of the ISP's protection from liability for copyright infringement that "upon notification of claimed infringement as described in [s 512](c)(3)," the ISP "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing." See 17 U.S.C. ss 512(b)(2)(E), 512(c)(1)(C), and 512(d)(3).

Verizon argues that s 512(h) by its terms precludes the Clerk of Court from issuing a subpoena to an ISP acting as a conduit for P2P communications because a s 512(h) subpoena request cannot meet the requirement in s 512(h)(2)(A) that a proposed subpoena contain "a copy of a notification [of claimed infringement, as] described in [s 512](c)(3)(A)."* In particular, Verizon maintains the two subpoenas obtained by the RIAA fail to meet the requirements of s 512(c)(3)(A)(iii) in that they do not - because Verizon is not storing the infringing material on its server - and can not, identify material "to be removed or access to which is to be disabled" by Verizon. Here Verizon points out that s 512(h)(4) makes satisfaction of the notification requirement of s 512(c)(3)(A) a condition precedent to issuance of a subpoena: "If the notification filed satisfies the provisions of [s 512](c)(3)(A)" and the other content requirements of s 512(h)(2) are met, then "the clerk shall expeditiously issue and sign the proposed subpoena ... for delivery" to the ISP.

Infringing material obtained or distributed via P2P file sharing is located in the computer (or in an off-line storage

---

* Subsection 512(c)(3)(A) provides that "[t]o be effective under this subsection, a notification of claimed infringement must be a written communication ... that includes substantially the following":

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information

> reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
>
> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

17 U.S.C. s 512(c)(3)(A).

device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the ISP can neither "remove" nor "disable access to" the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers.

The RIAA contends an ISP can indeed "disable access" to infringing material by terminating the offending subscriber's internet account. This argument is undone by the terms of the Act, however. As Verizon notes, the Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies for the protection of copyright owners, the former blocking access to the infringing material on the offender's computer and the latter more broadly blocking the offender's access to the internet (at least via his chosen ISP). Compare 17 U.S.C. s 512(j)(1)(A)(i) (authorizing injunction restraining ISP "from providing access to infringing material") with 17 U.S.C. s 512(j)(1)(A)(ii) (authorizing injunction restraining ISP "from providing access to a subscriber or account holder ... who is engaging in infringing activity ... by terminating the accounts of the subscriber or account holder"). "[W]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings." Transbrasil S.A. Linhas Aereas v. Dep't of Transp., 791 F.2d 202, 205 (D.C. Cir. 1986). These distinct statutory remedies establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer.

The RIAA points out that even if, with respect to an ISP functioning as a conduit for user-directed communications, a copyright owner cannot satisfy the requirement of s 512(c)(3)(A)(iii) by identifying material to be removed by the ISP, a notification is effective under s 512(c)(3)(A) if it "includes substantially" the required information; that standard is satisfied, the RIAA maintains, because the ISP can

identify the infringer based upon the information provided by the copyright owner pursuant to ss 512(c)(3)(A)(i)-(ii) and (iv)-(vi). According to the RIAA, the purpose of s 512(h) being to identify infringers, a notice should be deemed sufficient so long as the ISP can identify the infringer from the IP address in the subpoena.

Nothing in the Act itself says how we should determine whether a notification "includes substantially" all the required

information; both the Senate and House Reports, however, state the term means only that "technical errors ... such as misspelling a name" or "supplying an outdated area code" will not render ineffective an otherwise complete s 512(c)(3)(A) notification. S. Rep. No. 105-190, at 47 (1998); H.R. Rep. No. 105-551 (II), at 56 (1998). Clearly, however, the defect in the RIAA's notification is not a mere technical error; nor could it be thought "insubstantial" even under a more forgiving standard. The RIAA's notification identifies absolutely no material Verizon could remove or access to which it could disable, which indicates to us that s 512(c)(3)(A) concerns means of infringement other than P2P file sharing.

Finally, the RIAA argues the definition of "[internet] service provider" in s 512(k)(1)(B) makes s 512(h) applicable to an ISP regardless what function it performs with respect to infringing material - transmitting it per s 512(a), caching it per s 512(b), hosting it per s 512(c), or locating it per s 512(d).

This argument borders upon the silly. The details of this argument need not burden the Federal Reporter, for the specific provisions of s 512(h), which we have just rehearsed, make clear that however broadly "[internet] service provider" is defined in s 512(k)(1)(B), a subpoena may issue to an ISP only under the prescribed conditions regarding notification. Define all the world as an ISP if you like, the validity of a s 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under s 512(c)(3)(A). And as we have seen, any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of s 512(c)(3)(A)(iii) and is therefore ineffective.

In sum, we agree with Verizon that s 512(h) does not by its terms authorize the subpoenas issued here. A s 512(h) subpoena simply cannot meet the notice requirement of s 512(c)(3)(A)(iii).

B. Structure

Verizon also argues the subpoena provision, s 512(h), relates uniquely to the safe harbor in s 512(c) for ISPs engaged in storing copyrighted material and does not apply to the transmitting function addressed by the safe harbor in s 512(a). Verizon's claim is based upon the "three separate cross-references" in s 512(h) to the notification described in s 512(c)(3)(A). First, as we have seen, s 512(h)(2)(A) requires the copyright owner to file, along with its request for a subpoena, the notification described in s 512(c)(3)(A). Second, and again as we have seen, s 512(h)(4) requires that the notification satisfy "the provisions of [s 512](c)(3)(A)" as a condition precedent to the Clerk's issuing the requested subpoena. Third, s 512(h)(5) conditions the ISP's obligation to identify the alleged infringer upon "receipt of a notification described in [s 512](c)(3)(A)." We agree that the presence in s 512(h) of three separate references to s 512(c) and the absence of any reference to s 512(a) suggests the subpoena power of s 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.

As the RIAA points out in response, however, because ss 512(b) and (d) also require a copyright owner to provide a "notification ... as described in [s 512](c)(3)," the cross-references to s 512(c)(3)(A) in s 512(h) can not confine the operation of s 512(h) solely to the functions described in s 512(c), but must also include, at a minimum, the functions described in ss 512(b) and (d). Therefore, according to the RIAA, because Verizon is mistaken in stating that "the take-down notice described in [s 512](c)(3)(A) ... applies exclusively to the particular functions described in [s 512](c) of the

statute," the subpoena power in s 512(h) is not linked exclusively to s 512(c) but rather applies to all the ISP functions, wherever they may be described in ss 512(a)-(d).

Although the RIAA's conclusion is a non-sequitur with respect to s 512(a), we agree with the RIAA that Verizon overreaches by claiming the notification described in s 512(c)(3)(A) applies only to the functions identified in s 512(c). As Verizon correctly notes, however, the ISP activities described in ss 512(b) and (d) are storage functions. As such, they are, like the ISP activities described in s 512(c) and unlike the transmission functions listed in s 512(a), susceptible to the notice and take down regime of ss 512(b)-(d), of which the subpoena power of s 512(h) is an integral part. We think it clear, therefore, that the cross-references to s 512(c)(3) in ss 512(b)-(d) demonstrate that s 512(h) applies to an ISP storing infringing material on its servers in any capacity - whether as a temporary cache of a web page created by the ISP per s 512(b), as a web site stored on the ISP's server per s 512(c), or as an information locating tool hosted by the ISP per s 512(d) - and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.

The storage activities described in the safe harbors of ss 512(b)-(d) are subject to s 512(c)(3), including the notification described in s 512(c)(3)(A). By contrast, as we have already seen, an ISP performing a function described in s 512(a), such as transmitting e-mails, instant messages, or files sent by an internet user from his computer to that of another internet user, cannot be sent an effective s 512(c)(3)(A) notification. Therefore, the references to s 512(c)(3) in ss 512(b) and (d) lead inexorably to the conclusion that s 512(h) is structurally linked to the storage functions of an ISP and not to its transmission functions, such as those listed in s 512(a).

C. Legislative History

In support of its claim that s 512(h) can - and should - be read to reach P2P technology, the RIAA points to congressional testimony and news articles available to the Congress prior to passage of the DMCA. These sources document the threat to copyright owners posed by bulletin board services (BBSs) and file transfer protocol (FTP) sites, which the RIAA says were precursors to P2P programs.

We need not, however, resort to investigating what the 105th Congress may have known because the text of s 512(h) and the overall structure of s 512 clearly establish, as we have seen, that s 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others. Legislative history can serve to inform the court's reading of an otherwise ambiguous text; it cannot lead the court to contradict the legislation itself. See Ratzlaf v. United States, 510 U.S. 135, 147-48 (1994) ("[W]e do not resort to legislative history to cloud a statutory text that is clear").

In any event, not only is the statute clear (albeit complex), the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. That is not surprising; P2P software was "not even a glimmer in anyone's eye when the DMCA was enacted." In re Verizon I, 240 F. Supp. 2d at 38. Furthermore, such testimony as was available to the Congress prior to passage of the DMCA concerned "hackers" who established unauthorized FTP or BBS sites on the servers of ISPs, see Balance of Responsibil-

ities on the Internet and the Online Copyright Liability Limitation Act: Hearing on H.R. 2180 Before the House Subcomm. on Courts and Intellectual Property, Comm. on the Judiciary, 105th Cong. (1997) (statement of Ken Wasch, President, Software Publishers Ass'n); rogue ISPs that posted FTP sites on their servers, thereby making files of copyrighted musical works available for download, see Complaint, Geffen Records, Inc. v. Arizona Bizness Network, No. CIV. 98-0794, at p 1 (D. Ariz. May 5, 1998) available at http://www.riaa.com/news/newsletter/pdf/geffencomplaint.pdf, (last visited December 2, 2003); and BBS subscribers using dial-up technology to connect to a BBS hosted by an ISP. The Congress had no reason to foresee the application of s 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along. Had the Congress been aware of P2P technology, or anticipated its development, s 512(h) might have been drafted more generally. Be that as it may, contrary to the RIAA's claim, nothing in the legislative history supports the issuance of a s 512(h) subpoena to an ISP acting as a conduit for P2P file sharing.

D. Purpose of the DMCA

Finally, the RIAA argues Verizon's interpretation of the statute "would defeat the core objectives" of the Act. More specifically, according to the RIAA there is no policy justification for limiting the reach of s 512(h) to situations in which the ISP stores infringing material on its system, considering that many more acts of copyright infringement are committed in the P2P realm, in which the ISP merely transmits the material for others, and that the burden upon an ISP required to identify an infringing subscriber is minimal.

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforseen internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." See Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).

The stakes are large for the music, motion picture, and software industries and their role in fostering technological innovation and our popular culture. It is not surprising, therefore, that even as this case was being argued, committees of the Congress were considering how best to deal with the threat to copyrights posed by P2P file sharing schemes. See, e.g., Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Comm. On Governmental Affairs, 108th Congress (Sept. 30, 2003); Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Comm. on the Judiciary, 108th Congress (Sept. 9, 2003).

## III. Conclusion

For the foregoing reasons, we remand this case to the district court to vacate its order enforcing the February 4

subpoena and to grant Verizon's motion to quash the July 24 subpoena.

So ordered.