Santa Clara High Technology Law Journal

Volume 21 | Issue 2 Article 6

2005

Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in RIAA v. Verizon Internet Services

Trevor A. Dutcher

Recommended Citation

Trevor A. Dutcher, *Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in RIAA v. Verizon Internet Services*, 21 Santa Clara High Tech. L.J. 493 (2005).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol21/iss2/6

COMMENT

A Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in *RIAA v. Verizon Internet Services*

Trevor A. Dutcher†

INTRODUCTION

This comment begins with a brief synthesis of basic theories of copyright infringement and a short history of litigation related to Peer-To-Peer ("P2P") file sharing, which is followed by a general explanation of the safe harbors of the Digital Millennium Copyright Act ("DMCA" or the "Act")[1] and a more detailed explanation of the DMCA subpoena power. It then examines and criticizes the analysis and application of the DMCA subpoena power in *Recording Industry Association of America v. Verizon Internet Services*,[2] and concludes that the holding in *Verizon* was incorrect because (a) the statutory interpretation applied in that case was faulty, (b) the interpretation given was plainly contrary to the stated legislative intent of the DMCA, and (c) the final holding implicitly endorsed an impermissible violation of the equal protection clause (as incorporated into the due process clause) of the Fifth Amendment.

BACKGROUND

The dawn of the Internet has provided substantial benefits to society as a whole through economic globalization, electronic

---

† The author is a student at Santa Clara University School of Law, Editor-in-Chief of the *Santa Clara Computer & High Technology Law Journal*, a student representative on the Advisory Board to the High Tech Law Institute, a Dean's Appointee to the Ingram American Inn of Court, and a J.D. candidate for 2005. He previously earned a B.A. *magna cum laude* in Management with a minor in International Marketing from Menlo College. He would like to thank Professors Tyler Ochoa and Bradley Joondeph for their invaluable insight and commentary during the drafting of this paper, and his family for their tireless patience and support. Copyright © 2004 Trevor A. Dutcher.

[1] 17 U.S.C. § 512 (2004).

[2] 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004).

commerce, online communication, and instantaneous access to a plethora of information. Along the way, however, it has also given rise to substantial legal issues. This article focuses on P2P file sharing technology, its facilitation of copyright infringement, and the battle that the recording industry has faced in trying to enforce its copyrights. The Record Industry easily prevailed over Napster, showing that due to Napster's centralized indexing function, the company was guilty of contributory infringement for the acts of its users.[3] But as distributed architectures became more popular among P2P software vendors, and P2P vendors removed the indexing function from their own servers and pushed it out to the individual users, companies like Grokster and Morpheus were able to escape secondary liability.[4] Such advances in technology left copyright holders without a remedy against the vendors of such applications, and relegated them to lawsuits against the direct infringers, the file traders themselves. The record industry initially pursued these users by use of the DMCA subpoena power, but as is discussed below, plaintiffs are now forced to institute Doe actions against file traders and appear before a judge before any such subpoena may be issued or any subscriber information may be obtained.

I. COPYRIGHT INFRINGEMENT, GENERALLY

To prevail on a claim of copyright infringement, a Plaintiff must show ownership of a valid copyright and that the defendant copied protected expression.[5] Three main theories exist under which a defendant may be liable for copyright infringement: direct infringement, contributory infringement, and vicarious infringement. Direct infringement exists when the defendant himself is engaged in infringing activity.[6] A plaintiff may also sue a party other than the

---

[3] *See* A&M Records Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 920 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) (holding, in essence, that because the Napster file sharing system ran through a central index maintained by the company, the company could be held liable on a theory of secondary liability for the acts that its users engaged in). For an explanation of secondary liability under copyright law see *infra* Part I.

[4] *See* Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1046 (C.D. Cal. 2003), *cert. granted*, 73 U.S.L.W. 3247 (U.S. Dec. 10, 2004) (No. 04-480) (holding that because there was no central function to Grokster's file sharing technology, the company neither had the right and ability to supervise its users, nor did it materially contribute to its users' infringing activity, and it therefore could not be held secondarily liable for copyright infringement). For further explanation of the significance of these findings see *infra* Part I.

[5] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361 (1991).

[6] The statutory definition of copyright infringement is:

direct infringer on theories of contributory or vicarious infringement. To prevail on either of these theories, a plaintiff must first make a threshold showing of direct infringement by someone other than the defendant.[7] Once that threshold is met, a third-party may be liable for contributory infringement when, with knowledge of the direct infringing activity, he "induces, causes, or materially contributes to the infringing conduct of another."[8] A third-party may be liable for vicarious infringement when "he has a right and ability to supervise the [direct] infringing activity and has a direct financial interest in such activities."[9] There is no requirement that a party have knowledge of the infringing activity to be liable on a theory of vicarious infringement.[10] This is equally true for direct infringement.[11] Hence only contributory infringement requires an element of knowledge; direct and vicarious infringement of copyright are strict liability offenses.

> Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122 or of the author as provided in section 106A(a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be. For purposes of this chapter (other than section 506), any reference to copyright shall be deemed to include the rights conferred by section 106A(a). As used in this subsection, the term "anyone" includes any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this title in the same manner and to the same extent as any nongovernmental entity.

17 U.S.C. § 501(a) (2004).

[7] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434 (1984).

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

[9] *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996) (quoting Gershwin Publ'g Corp., 443 F.2d at 1162 (2d Cir. 1971)).

[10] Adobe Sys. Inc. v. Canus Prods., Inc., 173 F. Supp. 2d 1044, 1049 (C.D. Cal. 2001) (citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963)).

[11] The statute provides:

> In a case where the infringer sustains the burden of proving, and the court finds, that such infringer *was not aware and had no reason to believe* that his or her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages to a sum of not less than $200.

17 U.S.C. § 504(c)(2) (2004) (emphasis added). The inverse inference, then, is that even without knowledge or constructive knowledge that his act constitutes infringement, a person can be held directly liable in copyright, albeit to a potentially lesser degree than if he had such knowledge.

II. THE DIGITAL MILLENNIUM COPYRIGHT ACT, GENERALLY

"The DMCA was enacted [in 1998] both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright . . . liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider."[12] "Service providers" are afforded four safe harbors, and the term service provider is defined broadly in the Act. The Act states "[a]s used in subsection [512](a), 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[13] It then says "[a]s used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."[14] The second definition includes providers of more than just Internet connections, but presumably any type of service offered over the Internet.[15]

The first safe harbor, "Transitory Digital Network Communications," excludes service providers from liability for damages and limits the scope of injunctive relief arising from copyright infringement for purely passive transmissions over the service provider's infrastructure, provided that (i) someone other than the service provider initiated the transmission, (ii) the transmission is carried out by automated technical processes without selection of the material being made by the service provider, (iii) the service provider does not actively select the recipients of the transmission, (iv) no copy of the transmission is made for any period longer than necessary to complete the transmission and only the intended recipient may access the transmission, and (v) the content of the transmission is not modified by the service provider.[16]

---

[12] ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) (citing H.R. CONF. REP. NO. 105-796, at 72 (1998), *reprinted in* 1998 U.S.C.C.A.N. 649).

[13] 17 U.S.C. § 512(k)(1)(A) (2004).

[14] *Id.* § 512(k)(1)(B).

[15] By way of illustration, AOL is a traditional provider of Internet connections that meets both definitions of service providers, while a company that offers online file storage only meets the broader definition even if the company does not provide the link that allows customers to connect to the Internet.

[16] *See* 17 U.S.C. § 512(a) (2004).

The second safe harbor, "System Caching," limits, under certain circumstances, liability for the intermediate and temporary storage of transmissions on the service provider's network.[17] This ostensibly addresses the issue of random access memory copies raised by *MAI Systems Corp. v. Peak Computer, Inc.*[18] The third safe harbor, "Information residing on systems or networks at direction of users," limits, under certain circumstances, liability for service providers when infringing files are actually stored on their own physical networks provided they (i) have no actual knowledge of such storage, (ii) no constructive knowledge of such storage, or (iii) upon obtaining knowledge, they act expeditiously to remove or disable access to the files.[19] The fourth safe harbor, "Information location tools," limits, under certain circumstances, liability for service providers who aid their users in locating infringing material by maintaining an index, directory, reference, pointer, or hypertext link, provided that the service provider does not have actual knowledge that the material or activity is infringing, does not have constructive knowledge that the material or activity is infringing, or upon obtaining such knowledge, acts expeditiously to remove access to such infringing material.[20]

To take advantage of any of these safe harbors, the service provider must also satisfy several general requirements. It must first adopt, implement, and inform its users of a policy providing for the termination of repeat infringers.[21] In order to identify and to protect copyrighted works, the provider must also accommodate "standard" technical measures used by copyright owners.[22] Notably, service providers are not required to pro-actively monitor or take any positive action to seek out infringing material.[23] For service providers to moor in the safe harbors provided by § 512(c) and § 512(d), however, there is one final requirement that the service provider not receive a financial benefit directly attributable to the infringing activity where

---

[17] *See id.* § 512(b).

[18] 991 F.2d 511, 518 (9th Cir. 1993) (holding that copies of software loaded into a computer's random access memory, which is necessary for use of the software, constitutes a copy that is fixed for purposes of copyright infringement). For extended discussion of the issue and fallout from *MAI,* see CRAIG JOYCE ET AL., COPYRIGHT LAW 500–01 (6th ed. 2003 & Supp. 2004).

[19] *See* 17 U.S.C. § 512(c) (2004).

[20] *See id.* § 512(d).

[21] *See id.* § 512(i)(1).

[22] *See id.* § 512(i)(2).

[23] *See id.* § 512(m).

the service provider has the right and the ability to control such activity.[24]

III. THE DMCA SUBPOENA POWER

Given the anonymity inherent in Internet communication, copyright holders require cooperation from an Internet Service Provider ("ISP") to obtain the identity of individual infringers before they can effectively sue them. At best, a copyright holder can identify a user of P2P applications by his or her Internet Protocol ("IP") address,[25] and only the ISP is in a position to reveal the true identity of that person so that a complaint may be filed against him.[26] The provisions of § 512(h) of the DMCA allow copyright holders, after providing particularized information, to obtain subpoenas from the clerk of the court.[27] The subpoenas may be presented to the ISP to compel disclosure of the identity of the person behind the IP address so that the copyright holder may then properly bring suit against him.[28]

It is worth noting that these safe harbors are non-exclusive and refer not to types of service providers, but rather activities engaged in or uses made by the service provider's subscribers of the services it provides. A service provider may seek refuge in § 512(a) in a lawsuit alleging passive transport of data by its subscriber, yet the same ISP could nonetheless assert the § 512(c) safe harbor in a separate case alleging that a user stored infringing material on the ISP's server. The choice of which safe harbor should apply is therefore determined not by the form of the ISP, but by the alleged infringing act of the individual subscriber.

---

[24] *See id.* § 512(c)(1)(B), (d)(2). The language in these two clauses seems to state, in essence, that the safe harbors of subsections 512(c) and 512(d) provide no defense to a service provider who is otherwise guilty of vicarious infringement. For the vicarious infringer to seek refuge in the safe harbors of § 512, then, he seemingly would be required to satisfy the requirements of either § 512(a) or (b).

[25] Every computer connected to the Internet is assigned a unique number known as an Internet Protocol ("IP") address. *See* GOOGLE, INC., ADWORDS COMMON TERMS *at* https://adwords.google.com/select/glossary.html#i (last visited Oct. 18, 2004). The IP address, therefore, is the unique identifier of each computer connected to the Internet and is the mechanism by which other computers locate and communicate with it.

[26] The ISP owns the IP address and in a sense "leases" it to its customer so that the customer can connect to the Internet. Given the IP address, the ISP can match the IP address with the subscriber name.

[27] *See* 17 U.S.C. § 512(h) (2004). The actual requirements are discussed at greater length below. *See infra* Part IV.

[28] 17 U.S.C. § 512(h) (2004).

IV. *RIAA V. VERIZON INTERNET SERVICES, INC.*—APPLICATION OF THE SUBPOENA POWER

In a series of highly publicized cases, the record industry has aggressively defended its copyrights. After it became clear that companies like Grokster and Morpheus could escape secondary liability for the acts of their users due to the decentralized nature of their applications, attention was turned to the individuals engaged in direct infringement. Taking advantage of the provisions in § 512(h), the Recording Industry Association of America ("RIAA") began obtaining DMCA subpoenas seeking the identities of individual P2P users from ISPs who provided the users' Internet connections.[29] The first wave of subpoenas was sent to ISPs in July 2003 to identify and contact customers who were alleged copyright infringers.[30] Later that year, the RIAA filed 382 more lawsuits (261 in September, plus 80 in October, plus 41 in December of 2003).[31] While most ISPs complied with the subpoenas, Verizon Internet Services refused to comply with two separate subpoenas.[32] At the enforcement proceedings for the

---

[29] Daphne Eviatar, *Changing It's Tune: If The Music Industry Wants to Survive Online Piracy, In-House Lawyers at the Record Companies Must Adapt*, IP LAW & BUSINESS, Nov. 5, 2003, *available at* http://www.ipww.com/texts/tunes1103.html.

[30] The Impact of Recording Industry Suits Against Music File Swappers, Data Memo from Pew Internet Project and comScore (Jan. 4, 2004), at 5, *available at* http://207.21.232.103/pdfs/PIP_File_Swapping_Memo_0104.pdf.

[31] *Id.*

[32] Section 512(i)(1)(A) provides, as a condition to eligibility for the safe harbor provisions, that a service provider must "adopt[] and reasonably implement[], and inform[] subscribers and account holders of the service provider's system or network of[] a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are *repeat infringers*." 17 U.S.C. § 512(i)(1)(A) (2004) (emphasis added).

Notably, however, the statute does not define the term "repeat infringer." So the question remains as to what constitutes repeat infringement. Would the simple act of sharing a single infringing file with two separate users suffice? What about sharing two separate infringing files with one user? Or are two convictions required? A plain text reading of that section suggests that two infringing distributions of a single file, or the infringing distribution of two separate files should be sufficient to classify the user a "repeat infringer," thereby creating a duty in the ISP to terminate that user's service pursuant to its own policy.

Might it be argued that because Verizon actively defended its subscribers and shielded them from the DMCA subpoenas without terminating the users' service, that it had failed to "reasonably implement" a repeat infringer policy as required by § 512(i)(1)(A), thereby making the safe harbors unavailable, and exposing Verizon to suit for contributory or vicarious infringement for the actions of the users it sought to protect? *See In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 657–59 (N.D. Ill. 2002) (stating that because Aimster's encryption technology prevented identification of infringing users, Aimster could not be adequately informed of "repeat infringers," the policy was not reasonably implemented, and the safe harbors were therefore not available to it); *cf.* Perfect 10, Inc. v. CCBill, LLC, 2004 WL first subpoena, Verizon argued that, based on a prolix interpretation of § 512(h) and its interaction with language in § 512(a)–(d), the DMCA subpoena provision did not apply to Verizon as a mere provider of passive transport of data.[33] Verizon also questioned the constitutionality of § 512(h).[34] The constitutional arguments called into question the court's Article III power to issue the subpoena in the absence of an actual case or controversy, and referred to the First Amendment freedom to engage in anonymous speech. The court declined to discuss the constitutional issues because the issues had not been fully briefed by Verizon, and it disagreed with Verizon's analysis of the general applicability of § 512(h).[35] The motion to enforce the subpoena was granted.

In the enforcement hearings for the second subpoena, Verizon fully developed its constitutional arguments based on Article III and First Amendment grounds, but the court was unmoved. Equally unmoved by Verizon's construction of the statute, which interpreted § 512 as inapplicable to Verizon, the court ordered the second subpoena enforced as well.[36] On appeal, however, Verizon won the day, as the circuit court found that the DMCA subpoena in question was not enforceable against Verizon.[37] Although the victory was touted by Verizon as a win for privacy and safety,[38] the holding in fact turned solely on statutory interpretation.

1798295, at *6 (C.D. Cal. 2004) (suggesting that an infringer is not a repeat infringer—or at least that a repeat infringer policy is not activated—unless the ISP has received *multiple notices* of alleged infringing activity; stating in dicta that, "an Internet service provider who receives repeat notifications that substantially comply with the requirements of § 512(c)(3)(A) about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy"). It seems odd that two *notifications* are required to label a user a "repeat infringer" under this case, and it would seemingly drive copyright holders to send two notices back to back, instead of only one, thereby doubling the amount of paperwork that copyright holders must submit and that ISPs must process, in efforts to ensure that the ISP's "repeat infringer" policy is called into play. Nobody wins under that interpretation.

[33] *See In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 31 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003).

[34] *Id.* at 42 n.17. Verizon did not challenge the section directly, but only alluded to the "questionable nature of its constitutionality" in a footnote.

[35] *Id.* at 42, 44.

[36] *See In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003).

[37] RIAA, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004).

[38] *See* Press Release, Verizon, Inc., Verizon Wins Fight to Protect Internet Safety and Privacy (Dec. 19, 2003) *available at* http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=83104 (last visited Oct. 18, 2004).

The court, applying complex and arguably strained statutory interpretation, found that the DMCA subpoena power did not apply to Verizon as a provider of mere transport services, that the subpoena was improperly issued, and that Verizon need not comply.[39]

In order to obtain a DMCA subpoena, a copyright owner must file with the clerk of the court (i) a copy of a notification described in § 512(c)(3)(A),[40] (ii) a proposed subpoena, and (iii) a sworn declaration that the subpoena is sought to identify an infringer and that the identity will only be used to protect the rights of the copyright owner.[41] "If the notification filed satisfies the provisions of subsection [512](c)(3)(A), the proposed subpoena is in proper form . . . [and] the clerk shall expeditiously issue the . . . subpoena. . . ."[42]

In order for the notice to "be effective under . . . subsection [(c)(3)(A)], a notification of claimed infringement must be a written communication . . . that includes substantially the following:" (i) a physical or electronic signature; (ii) identification of the copyrighted work claimed to have been infringed; (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) contact information of the complaining party; and (v) a statement of a good faith belief that the alleged infringing use is not authorized by the copyright holder.[43]

Both Verizon and the court seized on the third requirement, particularly the phrase "and information reasonably sufficient to permit the service provider to locate the material."[44] Verizon argued, and the court agreed, that because the files were stored on the users' computers or removable storage media, and not on Verizon's network

---

[39] *See Verizon*, 351 F.3d 1229.

[40] In practice, the notification provided in § 512(c)(3)(A) must first be served on the ISP in question. Such notification puts the ISP on notice of the infringing material. In order to avail itself of the safe harbors in § 512 and avoid secondary liability for copyright infringement, the ISP must then take reasonable steps to remove or disable access to the infringing material. This is pursuant to the so-called "notice and takedown" provision. After sending notice to the ISP, the Plaintiff must then attach a copy of that notice to its proposed subpoena to the clerk of the court, in order to have the subpoena issued.

[41] *See* 17 U.S.C. § 512(h)(2)(A)–(C) (2004). The party seeking the subpoena must first notify the ISP of the alleged infringing material, and include a copy of that notification in its request for the subpoena.

[42] *Id.* § 512(h)(4).

[43] *See id.* § 512(c)(3)(A).

[44] *Id.* § 512(c)(3)(A)(iii).

or computers, Verizon was not able to "locate" the material in question. Without an ability to locate the material, notice described in subsection (c)(3)(A) could never be effective, and without effective notice, the subpoena could not issue as per subsection (h)(4).[45] The court's holding, distilled to its essence, is that P2P users are not reachable by the DMCA subpoena process outlined in § 512(h).

The conclusion was based on two basic premises: Service providers who would otherwise qualify for the safe harbor of § 512(a) (those alleged to be engaging in pure transport activity) are always unable to "locate" material that is stored on a user's computer and, in any event, § 512(h) simply does not apply to ISPs who are merely acting as a conduit for transmission activity described in § 512(a). Each of these premises will be rebutted in turn below.

A. Rebutting the Argument That the Files Cannot Be Located

Ignoring momentarily that the five requirements of § 512(c)(3) need only be "substantially"[46] met, this comment will demonstrate that the requirements were completely met. "Locate" simply means to "seek out and determine the location of"[47] or said another way, to ascertain the whereabouts of. By using a copy of the P2P application that the complaining party had used to obtain the IP address in the first place, Verizon could have connected to the alleged infringer's computer by using the IP address supplied by the complaining party in its subpoena. The complaining party could include the name of the particular P2P software it used to find the alleged infringer as part of the "information reasonably sufficient to permit the service provider to locate the material" as required by subsection (c)(3)(A)(iii). Once connected, Verizon could verify that the user is in fact sharing the file at issue. By doing so, Verizon would have effectively "sought out and determined the location of" the offending file—it would be located on the computer using the IP address in question. Notably absent from the language of subsection (c)(3)(A), which describes "effective notice," is a requirement that the ISP locate *and remove the file*, locate *and obtain dominion over the file*, or locate the file *on its own internal servers*. It need only *locate* the file—the text is clear.

It may be argued that expecting Verizon to use a P2P application to navigate a P2P network to locate the file would be unreasonably

---

[45] *See* RIAA, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1236 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004).

[46] *See* 17 U.S.C. § 512(c)(3)(A).

[47] MIRIAM-WEBSTER'S COLLEGIATE DICTIONARY 730 (11th ed. 2003).

burdensome; but navigating a P2P network to find a file on a user's computer is no different than Verizon navigating its own internal network to find the file on an internal server—the exercise is the same, the only difference is which software client is used in the navigation (Refer to the Appendix for an illustration of how this can be accomplished). Therefore, given the IP address of the alleged infringer and the title of the P2P software the user used, Verizon could have "located" the file pursuant to the requirements of § 512(c)(3)(A)(iii).

B. But Don't IP Addresses Change?

In short, the answer is "sometimes." There are two main methods of allocating IP addresses: static and dynamic. A static IP address is a number that is assigned to a computer by an ISP to be its permanent address on the Internet.[48] This is analogous to the street address on your house. The address on your house does not change from day to day and people can always find it with relative ease.

Many IP addresses, however, are assigned dynamically from a pool.[49] Many corporate networks and online services economize on the number of IP addresses they use by sharing a pool of IP addresses among a large number of users.[50] "If you're an America Online user, for example, your IP address [can] vary from one logon session to the next because AOL is assigning it to you from a pool that is much smaller than AOL's [total] base of subscribers."[51]

To use another analogy, dynamic IP addresses are more like hotel rooms than houses, and an ISP that only owns 100 IP addresses can be compared to a hotel that only has 100 rooms. When a user logs on to the ISP using a dynamic IP address, he "checks in" to a "room" which is the IP address that is dynamically assigned to him for the duration of his "stay." When he logs off the service or shuts down his computer, he might "check out" of that "room," making it available for someone else who wants to check in after him. The next time he "checks in" he might get a different "room." This system

---

[48] SEARCHWEBSERVICES.COM DEFINITIONS, STATIC IP ADDRESS/DYNAMIC IP ADDRESS, *at* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci520967,00.html (last visited Oct. 22, 2004).

[49] SEARCHWEBSERVICES.COM DEFINITIONS, IP ADDRESS, *at* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212381,00.html (last visited Oct. 3, 2004).

[50] *Id.*

[51] *Id.*

permits the ISP to serve a gross number of customers that is larger than the actual number of "rooms" available.

A slightly more detailed discussion of the mechanics of dynamic addressing, however, is warranted.[52] When a computer is attempting to enter a network in an environment using Dynamic Host Configuration Protocol ("DHCP"), the computer must first "lease" an IP address so that it may be identified on, and communicate with, the network.[53] To obtain a lease, the DHCP client initiates a conversation with a DHCP server using a series of messages.[54] The DHCP client first makes a request for an IP address.[55] The DHCP server then responds with an "offer."[56] The client will accept the offer, and the server will reply with a finalization of the transaction.[57] The client computer will then be identified by that address until the address is released or the lease expires.[58]

By default, a lease lasts for eight days,[59] but system administrators can configure the leases to last for longer or shorter durations.[60] It is possible that a lease can be set to last indefinitely.[61] Even where the lease is configured to last for less than an infinite duration, it does not necessarily expire after that duration passes. The client will attempt to renew the lease when 50% of the duration has passed.[62] So if the duration of the lease is set to eight days, the client will attempt to contact the DHCP server to renew the lease after four days. If the client successfully contacts the DHCP server and the lease is still available, the lease will be renewed for eight more days.[63]

---

[52] For the sake of simplicity, this section assumes use of DHCP on a Microsoft Windows platform. DHCP stands for Dynamic Host Configuration Protocol and is the mechanism by which dynamic IP addresses are managed within a network.

[53] MICROSOFT, INC., HOW DHCP WORKS, *at* http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Resources/Documentation/windowsserv/2003/all/techref/en-us/w2k3tr_dhcp_how.asp (last visited Oct. 23, 2004).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] MICROSOFT, INC., *supra* note 53.

[60] *Id.*

[61] *Id.* The effect in such a case would be the same as if a static IP address was used.

[62] *Id.*

[63] *Id.* If, for example, the computer is shut down on day three of the eight-day lease, and restarted on day nine, the client will attempt to contact the DHCP server to renew the lease. Technically the lease is expired, but if the address has not yet been reallocated to another computer, renewal is still possible. If the address is not available on the other hand, then a new

Local storage of DHCP information allows the client computer to "remember" its DHCP configuration and IP address even after it shuts down. If the computer is restarted before the lease expires, it will attempt to first renew the lease of its previous IP address before trying to acquire a new one.[64]

Now consider that many high-speed Internet connections such as cable-modem or DSL are "always-on." There is no need to dial-up to an ISP with these types of services; if the computer is on, then it is connected to the Internet. This means that the lease on an IP address, technically, could be renewed in perpetuity, and even a computer using a dynamic IP address could theoretically have the same IP address for weeks or months or more if it is not shut down or otherwise disconnected from the network for such a duration that would allow the lease to expire without a successful renewal. The foregoing discussion illustrates that although IP addresses *can* change, such a possibility does not justify a *per se* conclusion that it would be impossible to "locate" the file. Even if a subpoena containing a given IP address for an alleged infringer is delivered and some time passes before anyone at the ISP attempts to "locate" the file that is complained of, it is still perfectly reasonable that the ISP may be able to locate that file at that IP address after the passage of some time because the user's IP address will not necessarily have changed.

C. Completing the Proof That Effective Notice is Possible

To completely address the notice requirement, § 512(c)(3)(A)(iii), as a whole, requires "[i]dentification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed *or* to which access is to be disabled, and information reasonably sufficient to permit the service provider to locate the material."[65] The disjunctive "or" indicates that the notice is effective if (a) the ISP is able to remove the file, or (b) the ISP is able to disable other people's access to the file. Logically, it must then follow that the ISP may disable access to the file by some method other than by removing it. A contrary reading

---

address will be assigned and the computer will be known by that new address moving forward. *See id.*

[64] MICROSOFT, INC., *supra* note 53. If the renewal is unsuccessful, the computer will then request a new IP address in its place. *Id.*

[65] 17 U.S.C. § 512(c)(3)(A)(iii) (2004) (emphasis added).

would render the phrase "or to which access is to be disabled" mere surplusage.[66]

Having obtained the IP address of the offending host and having already located the file, the ISP could then potentially terminate the host's Internet access. By doing so, the ISP could "disable access to" the file.[67] The ISP is, therefore, able to "locate the offending material . . . to which access is to be disabled"; hence the whole of (c)(3)(A)(iii) would be satisfied. Because the balance of the notice provisions were also satisfied, effective notice was given and the subpoena could have been issued.

The court rejected a similar argument offered by the RIAA. Pointing to semantic differences between subsections (j)(1)(A)(i) and (j)(1)(A)(ii), the court reasoned that Congress considered disabling an individual's access to the 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[68] and the latter more broadly blocking the

---

[66] "It is an elementary rule of construction that effect must be given, if possible, to every word, clause, and sentence of a statute." 2A NORMAN J. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 46:06 (6th ed. 2002) (citing United States v. Menasche, 348 U.S. 528 (1955)). "A statute should be construed so that effect is given to all its provisions, so that no part will be . . . superfluous. . . ." *Id.* (citing Office of Consumers' Counsel v. F.E.R.C., 783 F.2d 206 (D.C. Cir. 1986)). "No clause [or] sentence or word shall be construed as superfluous . . . if the construction can be found which will give force to and preserve all the words of the statute." *Id.* (citing Tax Appeal of County of Maui v. KM Hawaii, Inc., 915 P.2d 1349 (Haw. 1996)). "The legislature is presumed to have intended to avoid surplusage in the words and sentences and therefore it is permissible to interpret the statute to avoid such a pitfall." *Id.* at § 46:07 (citing Commonwealth v. Scott, 546 A.2d 96 (Pa. Super. Ct. 1988)).

[67] Critics may view this as a Draconian proposition, that is, that terminating a user's Internet access for "allegedly" sharing a copyrighted work is an unjust solution. To be clear, that is not what I am suggesting. I am merely illustrating that the ISP is able to "locate" the material "to which access is to be disabled." Because the ISP can "locate" the material, and because it is capable of "disabling access to it," then notice can be properly served. Whether it *actually* disables access or not is only relevant to analyzing whether its termination policy is reasonably implemented and whether it has complied with the notice and takedown provisions in order to avail itself of the safe harbors generally. That issue is separate from the issuance of subpoenas. The statute does not require the ISP to remove the file in order for notice to be effective.

[68] This premise seems to create an inconsistency. In the court's own words, "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." RIAA, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004) (citing *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003) (internal quotations omitted)).

If Congress had not conceived of P2P technology, why would it need to "block access to infringing material on the offender's computer" as the court asserts is the rationale behind the offender's access to the Internet.[69] These distinct statutory remedies satisfied the court 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.[70] The court stated, "[w]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms [to] have different meanings."[71] This statement, however, proves too much; it only answers the question of "*must* access be disabled by termination of the user's Internet connection; that is, is termination of the users connection the *only* way to disable access to the file?" Clearly the answer is "no" in the larger context of § 512 as a whole. It does not, however, compel an answer in the negative to the question of "*may* access be disabled by termination of the user's Internet connection?" Certainly it may.

Two terms can have different meanings without being, of necessity, incompatible. They might mean different things, yet one can be a means while the other an end. It is unclear to this author why the termination of one user's Internet access cannot be a perfectly effective method of disabling other users' access to the infringing files he hosts. The court's view in this respect seems to be somewhat myopic, unnecessarily focusing on the single computer, and that particular user's access to his own file. It does not take into account that disabling the host from the network does in fact "disable access" to that file by all the millions of other users who are downloading it. It no longer exists anywhere on ISP's network or at any point accessible using their network, and for users searching for the file to download it, their access has been disabled.

"disabling access remedy?" A more reasonable assumption is that disabling Internet access was thought of as a remedy to keep the user from using his Internet access to post, upload, or broadcast infringing material in the future. *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231 (N.D. Cal. 1995) (enjoining defendant from posting unauthorized copies of L. Ron Hubbard's copyrighted works on an Internet bulletin board). Disabling Internet access of P2P file traders would be entirely consistent with such intent because it disables access by others, and it keeps the subscriber from broadcasting/distributing files over the network just as it would keep him from uploading the files to a bulletin board service.

[69] *Verizon*, 351 F.3d at 1235 (comparing "§ 512(j)(1)(A)(i) (authorizing injunction restraining ISP from providing access to infringing material [on its servers]) with . . . § 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)" (internal quotations omitted)).

[70] *Id.*

[71] *Id.* (quoting Transbrasil S.A. Linhas Aereas v. Dep't of Transp., 791 F.2d 202, 205 (D.C. Cir. 1986)).

More importantly, however, the court's discussion of § 512(j)(1)(A) seems entirely misplaced. Subsection (j)(1)(A) applies to service providers who qualify for the safe harbors of § 512(b)–(d).[72] Verizon, in this instance, clearly belonged under the auspices of the safe harbor provided by § 512(a). Section 512(j)(1)(B), which specifically addresses remedies against ISPs for § 512(a)-type activity, provides two possible orders for injunctive relief. Section 512(j)(1)(B) states:

> If the service provider qualifies for the limitation on remedies described in subsection (a), the court may *only* grant injunctive relief in one or both of the following forms: (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, *by terminating the accounts of the subscriber or account holder that are specified in the order*, or (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.[73]

So, in fact, the *only* remedy a court could order against a service provider who qualifies under the provisions of § 512(a), like Verizon, is in fact an order to terminate Internet access *by* a United States user, or prevent access *to* a foreign user via the conduit that it provides. Verizon could have "located" the infringing files, it could have disabled other users' access to the files, and it could have done so in a manner entirely consistent with the remedy expressly available against it; therefore the notice provisions of § 512(c)(3)(A), and hence § 512(h) were satisfied in their entirety.[74]

The court, however, went one step further to conclude that the § 512(h) subpoena power simply does not extend to Service Providers who do not engage in storage activities.[75] It reasoned that subsections 512(b) and (d) are storage functions.[76] As such, they are, like the ISP

---

[72] *See* 17 U.S.C. § 512(j)(1)(A) (2004). This subsection begins with "With respect to conduct *other than that which qualifies for the limitation on remedies set forth in subsection (a)*. . . ." *Id.* (emphasis added).

[73] *Id.* § 512(j)(1)(B) (emphasis added).

[74] Such a reading would also be consistent with the "termination policy" that is required by the DMCA as a prerequisite to an ISP's eligibility for the safe harbors to begin with. *See supra* text accompanying note 32.

[75] *Verizon*, 351 F.3d at 1237.

[76] *Id.*

activities described in § 512(c) and unlike the transmission functions listed in § 512(a), susceptible to the notice and take down regime of § 512(b)–(d), of which the subpoena power of § 512(h) is an integral part.[77] At this time, the reader might ask himself if the subpoena power of § 512(h) *really is* an *integral* part of the "notice and takedown regime"[78] of the safe harbors.

The safe harbors are concerned with providing shelter for ISPs from secondary liability arising from the acts of their subscribers. The subpoena power, on the other hand, gives plaintiffs a mechanism to identify and seek a remedy against direct infringers. These are separate tools. An ISP may very well receive notice of an allegedly infringing use that is sufficient for a subpoena to issue; but whether the ISP actually acts upon that notice by "taking down" the material in order to avail itself of the safe harbor is a wholly separate issue and should have no bearing on the subpoena analysis. As will be discussed momentarily, the immunity of the safe harbor provisions was granted *in exchange for* compliance with the subpoena process. This further suggests that the safe harbors and the subpoena power are completely discrete and separable concepts and not one inextricably intertwined all-or-nothing "regime." The court went on to say:

> [w]e think it clear, therefore, that the cross-references to § 512(c)(3) in §§ 512(b)-(d) demonstrate that § 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 § 512(b), as a web site stored on the ISP's server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d) –

---

[77] *Id.*

[78] Four separate elements of § 512 seem to be conflated into one "thing" by use of the colloquial phrase "notice and take down regime" as the term has gained popularity in common parlance. There is "*notice*," defined in detail at §512(c)(3), which serves two functions: (i) to put ISPs on notice so that they might take action to avail themselves of the safe harbors or else risk a lawsuit for secondary infringement, and separately, (ii) to satisfy an element of the burden placed upon plaintiffs in pursuit of a subpoena as described in § 512(h) to initiate an action for direct infringement. There is also "*takedown*" which is a second element that requires the ISP to remove or disable access to the purportedly infringing material it has been given "notice" of if it wishes to moor in the safe harbors of § 512(b)–(d) and avoid secondary liability; there is the "*immunity*" provided by the safe harbor if both "notice" and "take down" are satisfied; and there is the "*subpoena*" power itself, described in § 512(h) which compels the ISP to identify the direct infringer. "Notice and takedown," if it is a regime at all, would seem only to govern whether an ISP can moor in a safe harbor, by showing that after obtaining notice, it took down the offending material. It seems that the subpoena power is not integral to this process at all, which is discussed at further length below.

> and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.[79]

While the inference is articulated with precision and force, saying that something is clear, no matter how emphatically you say it, does not necessarily make it so. The plain language of § 512(h) requires only that *notice* be given to the *service provider* (not just the service provider who stores users' data). Moreover, a revisitation of the text of § 512(k) is informative—it defines "service provider" in terms of "transmission," "routing," "connections for digital online communication," "online services" and "network access." While "online services," arguably, could mean "storage," applying the maxim of *ejusdem generis*, it ought to be interpreted as a telecommunications-type service in order to give it a meaning consistent with the terms that surround it. This would suggest that the safe harbors created in § 512(a)–(d) were aimed *primarily* at protecting transport providers (conduits) against liability arising from the use made by their subscribers of the infrastructure that they provide, including pure transport or varying and increasing degrees of storage arising from such use—be it incidental caching, permanent web storage, or location by search tools such as the Google™ search engine or P2P applications.

Moreover, the cavernous breadth with which the definitions of service provider were written suggests liberal application of their provisions. The plain reference in § 512(h) to "service provider" betrays no limitation as to which type of service provider it should apply. It is important not to lose sight of the fact that § 512 was intended from the outset to protect transport providers like Verizon, who might otherwise be liable under copyright for incidental copying; not to protect storage providers who engage in incidental transport services.

Accepting that as a first principle, it follows that the proximity of § 512(c) to § 512(h) suggests, temporally speaking, that § 512(c), which appears first in the document, was drafted first in order to attain the primary goal of creating safe harbors for "service providers," and the reference back to § 512(c)(3)(A) contained later in § 512(h) is a simple shorthand reference, for clarity and simplicity's sake, to the notice procedure that had already been drafted earlier in the document.[80] To conclude that the reference back to the notice

---

[79] *Verizon*, 351 F.3d at 1237.

[80] *See* 1A NORMAN J. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 21:13 (6th ed. 2002) stating:

provision creates a limitation as to which type of service provider is subject to compliance with the subpoena process would be to rewrite the text of the statute. Additionally, the fact that the two subsections are so far apart, with so much text between them, belies the proposition that the subsections (512(c)(3)(A) and 512(h)), with the addition of subsections 512(b) and 512(d) should be treated as inexplicably intertwined, to the exclusion of § 512(a).

A more plausible conclusion is that, in Congress' attempt to ensure that individuals received adequate protections against unconstitutional invasions, the added component that the ISP must be able to locate the file in question, was added as a procedural safeguard before a subpoena could issue; if the ISP, looking to the user's shared files, was unable to locate the file in question, or any shared files at all for that matter, it could, on the user's behalf, challenge the subpoena as suspect, or on the grounds that notice was not properly given.[81] Such an interpretation seems to be more consistent with a plain text reading of the statute, practicality and common sense, and, as discussed below, Congress' stated intent that the Act be flexible enough to meet the challenges presented by new technology.

Therefore, as previously stated, effective notice was given and Verizon was a service provider; hence, there was no need to engage in the tortured interpretation that weakened the efficacy of § 512(h) by reading into it a limitation that simply does not exist in its text. The statute can be read to reach users engaged in § 512(a)-type activity,

---

> There are, however, occasions where reference is necessary. This is particularly true of long statutes. To avoid repetition, reference may need to be made to procedures . . . set forth in the same . . . statute. . . . This incorporation of one section into another tends toward simplicity of expression and directness of language, which fosters clarity and incisive style.

Id. I think few would dispute that § 512 is a long statute that derives benefits in the form of clarity and simplicity from reference back, rather than repetition of a notice procedure in multiple locations.

[81] *See, e.g.*, *In re* Verizon Internet Servs., 240 F. Supp. 2d 24, 40–41 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003) (describing the notice requirements of § 512(h)(2)(C) as procedural safeguards that

> provide substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas. Indeed, they provide greater threshold protection against issuance of an unsupported subpoena than is available in the context of a John Doe action. And, of course, nothing in the DMCA precludes a service provider from raising non-compliance or other objections to a subsection (h) subpoena).

See also In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 260–63 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003).

and if the files cannot be located as described above (perhaps because they have been removed before the ISP checks, or the user is offline or not running his P2P application when the ISP attempts to check), then notice is not properly served *in that particular instance* and the subpoena would not have to be honored. This would be no different than the case where a § 512(c)-type user storing files on his ISP's "web storage" deletes the files after he is discovered by the copyright holder, but before the subpoena is served upon the ISP. In that case, the ISP would once again be unable to "locate" the infringing material and the subpoena would simply be unenforceable, for a failure to provide proper notice under § 512(c)(3)(A)(iii); but certainly nobody would argue that the subpoena power simply does not apply to a situation covered by § 512(c) because the risk of being unable to locate the files exists.

A more narrow holding that comports with the interpretation I have suggested would have been preferable to the result reached in *Verizon* because it would address the same concern—inability to locate the file—on a case-by-case basis, empowering copyright holders in all instances, and leaving the text of the statute intact.

D. Legislative Intent

As to legislative intent, the court opined that Congress had no reason to foresee the application of § 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along.[82] It stated "[h]ad the Congress been aware of P2P technology, or anticipated its development, § 512(h) might have been drafted more generally."[83] Notwithstanding Congress' inability to specifically foresee P2P technology, however, "[a] word is not a crystal, transparent and unchanged, it is the skin of a living thought and may vary greatly in color and content according to the circumstances and the time in which it is used."[84] Congress, in enacting the DMCA, was concerned that "owners [would] hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."[85] A reading of the statute that is consistent with this concern would

---

[82] *See* RIAA, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004).

[83] *Id.*

[84] Towne v. Eisner, 245 U.S. 418, 425 (1918) (citing Lamar v. United States, 240 U.S. 60, 65 (1916)).

[85] S. REP. NO. 105-190, at 8 (1998).

require that § 512(h) be applied to protect copyright owners against the single greatest current threat of such piracy—P2P file sharing.

Courts have explicitly recognized compromises embodied in the DMCA, giving service providers protection against copyright liability in exchange for assisting copyright owners to identify parties infringing their works.[86] Congress' intent that the DMCA be flexible enough to embrace and be applied to new technology is clear in Senator Leahy's statement that "[t]he DMCA is a product of the Senate Judiciary Committee's recognition that ours is a time of unprecedented challenge to copyright protection. . . . This bill is a well-balanced package of proposals that address the needs of creators, consumers and commerce in the digital age and well into the next century."[87] A straightforward, plain text interpretation of the DMCA that reads § 512(h) as reaching P2P users who connect through ISPs like Verizon fully embraces Congress' intent.

---

[86] *See In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 274 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003) (stating in dicta:

> It would not be in the public interest to alter the trade-offs Congress carefully crafted in the DMCA. As this Court has stated, "in exchange for complying with subpoenas under subsection (h), service providers receive liability protection from any copyright infringement. . . . Hence, any additional burden [on service providers] is offset by that [liability] protection, which, of course, is exactly the contemplation reflected in the structure of the DMCA).

See also id. n.35 ("Other courts have recognized the trade-offs embodied in the DMCA, giving service providers copyright liability protection in exchange for assisting copyright owners to identify infringers.") (citing ALS Scan v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1124 (N.D. Cal. 2002).

For a discussion of the history of the DMCA and ISP lobbying efforts to obtain the protections offered by the safe harbor provisions, see Tyler T. Ochoa, *1984 And Beyond: Two Decades of Copyright Law*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 167, 179 (2003) (citing Irina Y. Dmitrieva, *I Know It When I See It: Should Internet Providers Recognize Copyright Violation When They See It?*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 233, 244–53 (2000)). *See also* H.R. CONF. REP. NO. 105-796, at 72 (1998) (describing the then-new liability standard for ISPs as being designed to preserve "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").

The notion underlying this reasoning, that such compromises should only be required of ISPs who physically store infringing material, leaving other ISPs, who only provide transport, privy to the safe harbor of § 512(a) free from the same obligation, seems inequitable.

[87] S. REP. NO. 105-190, at 69 (1998); *see also id.* at 8 (stating:

> Copyright laws have struggled through the years to keep pace with emerging technology from the struggle over music played on a player piano roll in the 1900's to the introduction of the VCR in the 1980's. With this constant evolution in technology, *the law must adapt in order to make digital networks safe places to disseminate and exploit copyrighted materials*. . .)

(emphasis added).

To summarize, because Verizon could have located the material described in the subpoena, and because there is no reason to conclude that an ISP, as a third-party, must first store something on its servers before it can be compelled by § 512(h) to provide the identity of a customer engaged in copyright infringement, and because such a conclusion is consistent with Congress' intent as well as the clear text of the statute, the subpoena could have properly issued, and the court should have ordered its enforcement.

E. Equal Protection

Even if one were to completely accept the court's interpretation, and agree that Congress intended to treat subscribers of ISPs who engage in activity described by § 512(a) differently than subscribers of ISPs engaged in activity described in § 512(b)–(d), the decision by its own holding cannot stand, as it implicitly endorses a violation of the equal protection clause of the Fifth Amendment. Although the words "equal protection" do not appear in the text of the Fifth Amendment, they have been read in as a component of the due process clause.[88]

An equal protection problem can arise when a law facially discriminates between two classes of people and by its express terms treats them differently. Traditional equal protection principles require that only those who are similarly situated should be treated alike.[89] Differences in treatment can be justified when they correspond to relevant differences.[90] Courts should review classifications that are not based on either suspect[91] or quasi-suspect[92] classifiers under the minimal scrutiny standard, or rational basis review. Rational basis review requires that the discrimination serve a legitimate state interest

---

[88] *See* Bolling v. Sharpe, 347 U.S. 497, 499 (1954).

> "The Fifth Amendment . . . does not contain an equal protection clause. . . . But the concepts of equal protection and due process, both stemming from our American ideal of fairness, are not mutually exclusive. The 'equal protection of the laws' is a more explicit safeguard of prohibited unfairness than 'due process of law,' and, therefore, we do not imply that the two are always interchangeable phrases. But, as this Court has recognized, discrimination may be so unjustifiable as to be violative of due process." *Id.*

[89] KATHLEEN M. SULLIVAN & GERALD GUNTHER, CONSTITUTIONAL LAW 671 (14th ed. 2003).

[90] *Id.*

[91] "Suspect" classifications include race, alienage, and national origin, and are reviewed under strict scrutiny.

[92] "Quasi-suspect" classifications include gender and legitimacy, and are reviewed under intermediate scrutiny.

and that the discrimination be rationally related to the attainment of that interest.[93] If the statute fails rational basis review, it cannot be allowed to stand as so written, applied or interpreted.[94]

The court's interpretation of § 512 facially creates two classes of people: People who store content on their personal computer and people who store content on the computers owned and run by their ISPs. The two classes are similarly situated in the sense that they both store infringing material in digital form. The difference between the classes, where they store their infringing files, should not be treated as a "relevant" difference for purposes of equal protection analysis. The difference between the two classes that results from the court's reading is that the former subscribers must be accorded notice and opportunity to be heard, with an opportunity to contest the issuance of the subpoenas, while the latter subscribers are guaranteed no such protection.[95] The law, therefore, is read as facially treating the two classes differently. Because the distinction—the location of where the user stores his files—is not a suspect or quasi-suspect classification, a court should review the holding under a rational basis standard. Under rational basis review, there must be a legitimate (not arbitrary) interest to be served by such a facially discriminatory law,

---

[93]

> The first step in determining whether legislation survives rational-basis scrutiny is identifying a legitimate government purpose—a goal—which the enacting government body could have been pursuing. The actual motivations of the enacting governmental body are entirely irrelevant. . . . The second step of rational-basis scrutiny asks whether a rational basis exists for the enacting governmental body to believe that the legislation would further the hypothesized purpose. The proper inquiry is concerned with the existence of a conceivably rational basis, not whether that basis was actually considered by the legislative body. As long as reasons for the legislative classification may have been considered to be true, and the relationship between the classification and the goal is not so attenuated as to render the distinction arbitrary or irrational, the legislation survives rational-basis scrutiny.

Joel v. City of Orlando, 232 F.3d 1353, 1358 (11th Cir. 2000) (quoting Haves v. City of Miami, 52 F.3d 918, 921–22 (11th Cir. 1995) (internal quotations and citations omitted)).

[94] *See, e.g.*, Horizon House Developmental Servs., Inc. v. Township of Upper Southampton, 804 F. Supp. 683 (E.D. Pa. 1992) (finding that requirement of 1,000 foot spacing between group homes for retarded adults, while no such restrictions applied to homes for other types of families, had no rational basis to support its facial discrimination, and was thus held to be facially invalid and its enforcement was enjoined).

[95] Critics who might argue that my reading of the statute affords *none* of the subscribers notice and opportunity to be heard, thereby creating a violation of the due process clause or of the users' privacy rights, are referred to *infra* note 98 and accompanying text.

and the discrimination must be rationally related to the attainment of that interest.[96]

Ignoring for a moment that Congress has neither articulated an intent to so discriminate, nor a purportedly legitimate interest in doing so, leaving commentators to their own imaginations, the only possible interest this author can conceive of for imposing such a distinction is the wish to not impose upon an ISP a statutory requirement with which it cannot comply. This interest might be argued to arise from the belief that ISPs cannot "locate" the infringing material in a situation covered by § 512(a). But as has already been discussed, that interest simply does not arise on these facts, because the ISPs *can* locate the material in question.

It is difficult to conceive of another state interest that might be at play here. It certainly cannot be one of privacy, due process, protecting a disadvantaged class, or remediation because such an interest ought naturally extend to § 512(b)–(d)-type subscribers as well; not just to § 512(a)-type subscribers. Because there is really no other conceivable legitimate state interest at play here, the discrimination would have to fail rational basis review. Therefore, the Court's discriminatory reading of § 512 does not even rise to the challenge of minimal scrutiny, and the statute must instead be read and applied in a facially neutral fashion. As such § 512(h) has to be read as reaching all ISP subscribers, or none of them. And to say that it reaches none of them would be a plainly contrary, hence unacceptable, reading of the text of the statute. This analysis therefore lends further support to the argument that the Court should have read the statute to apply to subscribers of ISPs engaged in activity described by § 512(a).

V. CONCLUSION

Alas, the Court saw things differently. So where does that leave us in the grand scheme of P2P litigation? P2P vendors who are wise enough to employ distributed architectures and decentralization of all indexing and file transfer functionality cannot be held vicariously or contributorily liable for the copyright infringement that their applications facilitate. Moreover, ISPs acting only as a conduit for communications who do not store any semblance of the communication on their own physical networks are not subject to the DMCA subpoena provisions of § 512(h). In effect, the DMCA is

---

[96] *See supra* text accompanying note 93.

flaccid as regards copyright infringement over P2P networks and Plaintiffs against P2P file traders have been relegated to a state of the law that existed before § 512 was even passed, at least in the D.C. Circuit. Certainly this is not consistent with what the drafters of the DMCA had intended.

Does that mean that file-traders win and users are untouchable? Not at all. The industry can still file John Doe actions against individual P2P infringers and obtain Doe Subpoenas under Federal Rule of Civil Procedure 45.[97] The process, however, is more arduous than the DMCA subpoena process: The Plaintiff must file a John Doe action ahead of the subpoena; the Doe defendant must be given notice of the subpoena request and must be allowed to contest the issuance of the subpoena; the process will require the plaintiff to brief the court and give oral argument before the judge decides whether to issue the subpoena.[98] The process will be far more time-consuming, expensive, and burdensome for both the copyright holders and the courts than the more streamlined filing prescribed in § 512(h), which can still be used in situations covered by § 512(b)–(d). The result is that copyright holders will be hobbled in their efforts to enforce their statutory rights as against P2P file traders, the process will become more expensive

---

[97] *See generally* FED. R. CIV. P. 45.

[98] *See In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 254 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003). Some constitutional scholars might argue that this is good because the DMCA as a whole violates users' Constitutional due process or privacy rights. While the notion is not expressly rejected, extended discussion is outside the scope of this article. *But see* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (stating that the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (holding that when an Internet subscriber "entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. . ." and as such had no reasonable expectation of privacy in the information so provided); *see also* Sony Music Entm't, Inc. v. Does 1–40, 326 F. Supp. 2d 556, 562–64 (S.D.N.Y. 2004) (stating that individuals using the Internet to download or distribute copyrighted music are engaged in anonymous "speech" entitled to First Amendment protection, but motion to quash subpoena to identify alleged individual infringers is denied where prima facie case of infringement is pleaded).

For more in-depth examination of the issues, however, see Matthew Amedeo, Comment, *Shifting the Burden: The Constitutionality of Section 512(h) of the Digital Millenium Copyright Act and Its Impact on Internet Service Providers*, 11 COMMLAW CONSPECTUS 311 (2003), suggesting that § 512(h) is unconstitutional on First, Fourth, and Fifth Amendment grounds. Compare the reasoning in *Verizon*, 257 F. Supp. 2d at 248–68, concluding that § 512(h) does not violate Article III or the First Amendment, and expressly stating at pages 259–60 that the speech involved in P2P file trading is not the type of speech protected by the First Amendment to which a right to privacy or anonymity might attach. Neither of these analyses, however, addresses the possible equal protection issues raised by the court's holding.

for them, and in some cases cost-prohibitive, leading some smaller copyright owners to acquiesce in such infringement. In the alternative, courts may be flooded with hearings contesting the enforcement of such subpoenas where larger plaintiffs like the RIAA do choose to move forward.

For proponents of the reasoning in *Verizon*, some rhetorical questions are offered: If, as discussed above, compliance with § 512(h) represents a tradeoff for the immunity provided by the safe harbors, what precisely are ISPs seeking refuge in § 512(a) offering in exchange?[99] Have we incentivized ISPs to offer fewer services to consumers and to act only as passive conduits thereby stifling innovation and the expansion of useful services? Is that consistent with the purpose and policy of the Intellectual Property Clause of the Constitution? Why, exactly, should the subpoena process to reach an infringer who shares an MP3 file with the masses, by offering it for download from a website, be different than the process required to reach the infringer who shares the same MP3 file with the same masses by offering it for download on a P2P network? Why should the latter have a greater expectation of due process, privacy or equal protection than the former? Why should the *situs* of the file change the rules as between the copyright holder and the infringer? If the answer to any of these is in the negative, then perhaps *Verizon* deserves a second look.[100]

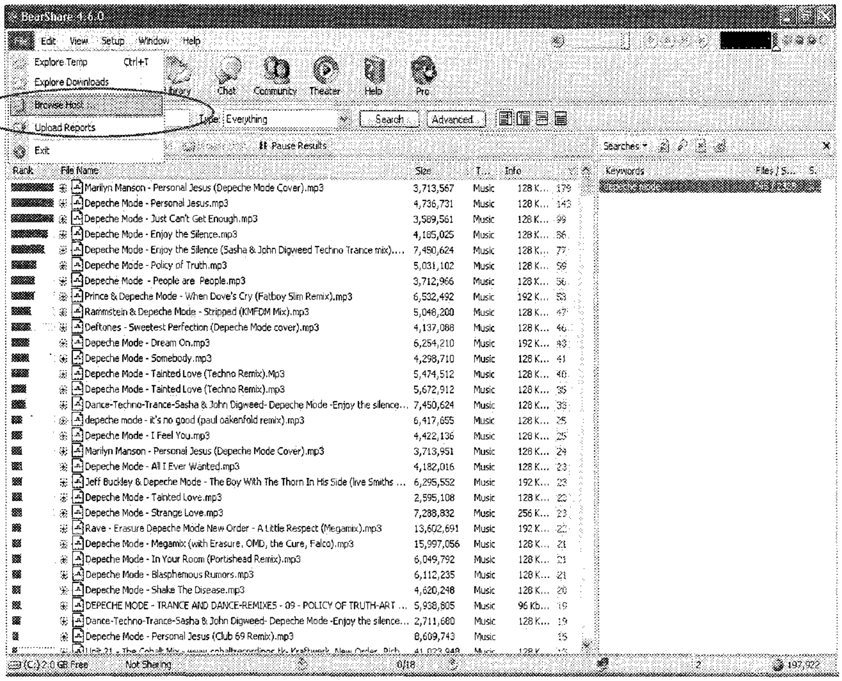
---

[99] For a discussion of the history of the DMCA and ISP lobbying efforts to obtain the protections offered by the safe harbor provisions, see Ochoa, *supra* note 86 at 178. *See also* H.R. CONF. REP. NO. 105-796, at 72 (1998) (describing the then-new liability standard for ISPs as being designed to preserve "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").

[100] The RIAA has since instituted 477 additional Doe actions, 69 of which targeted users on University networks. *See New Wave of Illegal File Sharing Lawsuits Brought By RIAA*, *available at* http://www.riaa.com/news/newsletter/042804.asp (Oct. 22, 2004).

APPENDIX

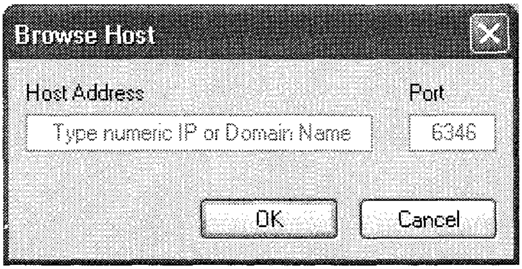
Fig. 1



File Name	Size	T...	Info	
Marilyn Manson - Personal Jesus (Depeche Mode Cover).mp3	3,713,567	Music	128 K...	179
Depeche Mode - Personal Jesus.mp3	4,736,731	Music	128 K...	143
Depeche Mode - Just Can't Get Enough.mp3	3,589,561	Music	128 K...	99
Depeche Mode - Enjoy the Silence.mp3	4,185,025	Music	128 K...	86
Depeche Mode - Enjoy the Silence (Sasha & John Digweed Techno Trance mix)....	7,450,624	Music	128 K...	77
Depeche Mode - Policy of Truth.mp3	5,031,102	Music	128 K...	59
Depeche Mode - People are People.mp3	3,712,966	Music	128 K...	56
Prince & Depeche Mode - When Dove's Cry (Fatboy Slim Remix).mp3	6,532,492	Music	192 K...	53
Rammstein & Depeche Mode - Stripped (KMFDM Mix).mp3	5,048,200	Music	128 K...	47
Deftones - Sweetest Perfection (Depeche Mode cover).mp3	4,137,088	Music	128 K...	46
Depeche Mode - Dream On.mp3	6,254,210	Music	192 K...	43
Depeche Mode - Somebody.mp3	4,298,710	Music	128 K...	41
Depeche Mode - Tainted Love (Techno Remix).Mp3	5,474,512	Music	128 K...	40
Depeche Mode - Tainted Love (Techno Remix).mp3	5,672,912	Music	128 K...	35
Dance-Techno-Trance-Sasha & John Digweed- Depeche Mode -Enjoy the silence...	7,450,624	Music	128 K...	33
depeche mode - it's no good (paul oakenfold remix).mp3	6,417,655	Music	128 K...	25
Depeche Mode - I Feel You.mp3	4,422,136	Music	128 K...	25
Marilyn Manson - Personal Jesus (Depeche Mode Cover).mp3	3,713,951	Music	128 K...	24
Depeche Mode - All I Ever Wanted.mp3	4,182,016	Music	128 K...	23
Jeff Buckley & Depeche Mode - The Boy With The Thorn In His Side (live Smiths ...	6,295,552	Music	192 K...	23
Depeche Mode - Tainted Love.mp3	2,595,108	Music	128 K...	23
Depeche Mode - Strange Love.mp3	7,288,832	Music	256 K...	23
Rave - Erasure Depeche Mode New Order - A Little Respect (Megamix).mp3	13,602,691	Music	192 K...	22
Depeche Mode - Megamix (with Erasure, OMD, the Cure, Falco).mp3	15,997,056	Music	128 K...	21
Depeche Mode - In Your Room (Portishead Remix).mp3	6,049,792	Music	128 K...	21
Depeche Mode - Blasphemous Rumors.mp3	6,112,235	Music	128 K...	21
Depeche Mode - Shake The Disease.mp3	4,620,248	Music	128 K...	20
DEPECHE MODE - TRANCE AND DANCE-REMIXES - 09 - POLICY OF TRUTH-ART ...	5,938,805	Music	96 Kb...	19
Dance-Techno-Trance-Sasha & John Digweed- Depeche Mode -Enjoy the silence...	2,711,680	Music	128 K...	19
Depeche Mode - Personal Jesus (Club 69 Remix).mp3	8,609,743	Music		15

Suppose an ISP is served with a subpoena alleging that one of its subscribers at the IP address 67.115.178.246 is using BearShare software to share copyrighted works by the artist Yngwie Malmstein, and in particular, a file called "Classical Guitar Solo." Rather than opening up windows explorer to browse its own internal network to find the file, it can instead open up BearShare to browse the P2P network. As will be demonstrated in the images that follow, the ISP has been given information that amounts to "*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*" as required by § 512(c)(3)(a)(iii). From the file menu, the ISP can select "Browse Host."

Fig. 2

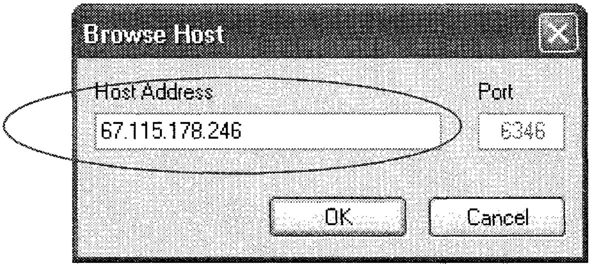


Host Address

Port: 6346

A window will pop up asking for the IP address of the host it would like to connect to.

Fig. 3

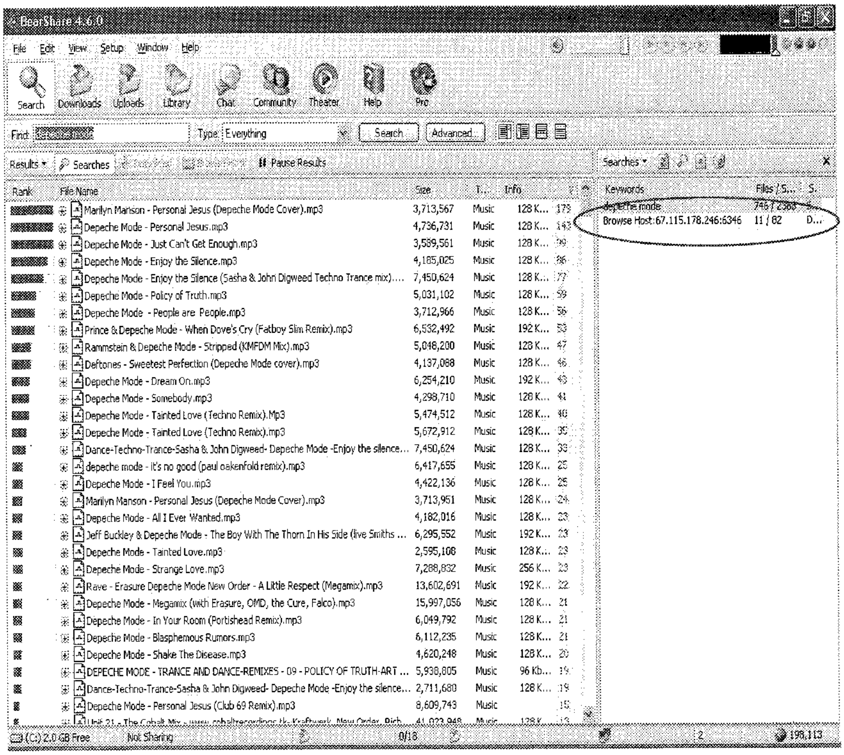


Host Address: 67.115.178.246

Port: 6346

The ISP can then enter the IP address it has been given in the subpoena and press OK.

Fig. 4

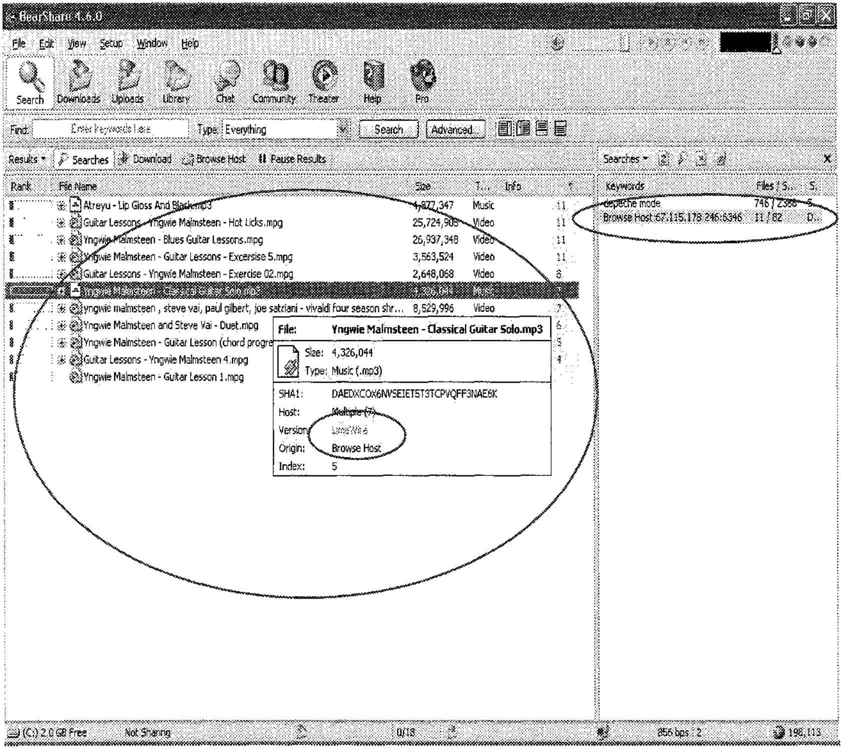


Rank	File Name	Size	T...	Info	
	Marilyn Manson - Personal Jesus (Depeche Mode Cover).mp3	3,713,567	Music	128 K...	179
	Depeche Mode - Personal Jesus.mp3	4,736,731	Music	128 K...	143
	Depeche Mode - Just Can't Get Enough.mp3	3,589,561	Music	128 K...	99
	Depeche Mode - Enjoy the Silence.mp3	4,185,025	Music	128 K...	86
	Depeche Mode - Enjoy the Silence (Sasha & John Digweed Techno Trance mix)....	7,450,624	Music	128 K...	77
	Depeche Mode - Policy of Truth.mp3	5,031,102	Music	128 K...	59
	Depeche Mode - People are People.mp3	3,712,966	Music	128 K...	56
	Prince & Depeche Mode - When Dove's Cry (Fatboy Slim Remix).mp3	6,532,492	Music	192 K...	53
	Rammstein & Depeche Mode - Stripped (KMFDM Mix).mp3	5,048,200	Music	128 K...	47
	Deftones - Sweetest Perfection (Depeche Mode cover).mp3	4,137,088	Music	128 K...	46
	Depeche Mode - Dream On.mp3	6,254,210	Music	192 K...	43
	Depeche Mode - Somebody.mp3	4,298,710	Music	128 K...	41
	Depeche Mode - Tainted Love (Techno Remix).Mp3	5,474,512	Music	128 K...	40
	Depeche Mode - Tainted Love (Techno Remix).mp3	5,672,912	Music	128 K...	35
	Dance-Techno-Trance-Sasha & John Digweed- Depeche Mode -Enjoy the silence...	7,450,624	Music	128 K...	33
	depeche mode - it's no good (paul oakenfold remix).mp3	6,417,655	Music	128 K...	25
	Depeche Mode - I Feel You.mp3	4,422,136	Music	128 K...	25
	Marilyn Manson - Personal Jesus (Depeche Mode Cover).mp3	3,713,951	Music	128 K...	24
	Depeche Mode - All I Ever Wanted.mp3	4,182,016	Music	128 K...	23
	Jeff Buckley & Depeche Mode - The Boy With The Thorn In His Side (live Smiths ...	6,295,552	Music	192 K...	23
	Depeche Mode - Tainted Love.mp3	2,595,108	Music	128 K...	23
	Depeche Mode - Strange Love.mp3	7,288,832	Music	256 K...	23
	Rave - Erasure Depeche Mode New Order - A Little Respect (Megamix).mp3	13,602,691	Music	192 K...	22
	Depeche Mode - Megamix (with Erasure, OMD, the Cure, Falco).mp3	15,997,056	Music	128 K...	21
	Depeche Mode - In Your Room (Portishead Remix).mp3	6,049,792	Music	128 K...	21
	Depeche Mode - Blasphemous Rumors.mp3	6,112,235	Music	128 K...	21
	Depeche Mode - Shake The Disease.mp3	4,620,248	Music	128 K...	20
	DEPECHE MODE - TRANCE AND DANCE-REMIXES - 09 - POLICY OF TRUTH-ART ...	5,938,805	Music	96 Kb...	19
	Dance-Techno-Trance-Sasha & John Digweed- Depeche Mode -Enjoy the silence...	2,711,680	Music	128 K...	19
	Depeche Mode - Personal Jesus (Club 69 Remix).mp3	8,609,743	Music		15

Keywords	Files / S...	S.
depeche mode	746 / 2568	S...
Browse Host:67.115.178.246:6346	11 / 82	D...

The ISP's BearShare application will connect to the computer that sits at the IP address provided and query the files it has available. When the query is done, the ISP can click on the Host.

Fig. 5



Rank	File Name	Size	T...	Info	
	Atreyu - Lip Gloss And Black.mp3	4,877,347	Music		11
	Guitar Lessons - Yngwie Malmsteen - Hot Licks.mpg	25,724,905	Video		11
	Yngwie Malmsteen - Blues Guitar Lessons.mpg	26,937,348	Video		11
	Yngwie Malmsteen - Guitar Lessons - Excersise 5.mpg	3,563,524	Video		11
	Guitar Lessons - Yngwie Malmsteen - Exercise 02.mpg	2,648,068	Video		8
	[illegible]	[illegible]	[illegible]		[illegible]
	yngwie malmsteen , steve vai, paul gilbert, joe satriani - vivaldi four season shr...	8,529,996	Video		7
	Yngwie Malmsteen and Steve Vai - Duet.mpg				6
	Yngwie Malmsteen - Guitar Lesson (chord progre				5
	Guitar Lessons - Yngwie Malmsteen 4.mpg				4
	Yngwie Malmsteen - Guitar Lesson 1.mpg				

File: **Yngwie Malmsteen - Classical Guitar Solo.mp3**
Size: 4,326,044
Type: Music (.mp3)
SHA1: DAEDXCOX6NVSEIET5T3TCPVQFF3NAE6K
Host: Multiple (7)
Version: LimeWire
Origin: Browse Host
Index: 5

Keywords	Files / S...	S.
depeche mode	746 / 2388	S.
Browse Host 67.115.178.246:6346	11 / 82	D...

When the host is selected, the window on the left displays all of the files that the computer at the stated IP address is offering for download. The ISP has now located the allegedly infringing files on the computer using the IP address provided by the complaining party. If the ISP so chooses, it can download the file and listen to it, just to make sure it is what it purports to be. It is that easy.

Because the ISP *is able to* terminate the user's Internet access, thereby disabling access to the file, the requirements of § 512(c)(3) can be satisfied.

Notably, the file information in the yellow-tinted box indicates that the user offering this file for download is actually using LimeWire software, and not BearShare, at the other end. This is significant because BearShare communicates not only with BearShare clients, but also with other software clients that operate on the

Gnutella network.[101] Popular examples include LimeWire, Morpheus, Mutella, Shareza, and others. This would tend to rebut the argument that that it would be too much trouble to maintain a copy of each of these clients in order to "locate" files, depending on which client the alleged infringer is said to be using. Doing so is not required.

---

[101] According to the software vendor "Bearshare lets you search for, download, and share files with everyone on the global Gnutella peer-to-peer information network." *See BearShare 4.6.0, Software Publisher's Description*, CNET Download.com, *at* http://www.download.com/BearShare/3000-2166_4-10295159.html?tag=lst-0-1 (last visited Oct. 16, 2004) (copy on file with author).