

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

In re:

VERIZON INTERNET SERVICES INC.
Subpoena Enforcement Matter

RECORDING INDUSTRY ASSOCIATION OF AMERICA

v.

VERIZON INTERNET SERVICES INC.

**OPPOSITION OF VERIZON INTERNET SERVICES TO
MOTION TO ENFORCE EX PARTE SUBPOENA
ISSUED JULY 24, 2002**

The Recording Industry Association of America ("RIAA") has moved to enforce a subpoena issued to Verizon Internet Services Inc. ("Verizon"). The subpoena does not pertain to any case pending in this or any other court, but rather is based on an ex parte notification of claimed infringement RIAA submitted to the Clerk of the Court under the purported authority of subsection 512(h) of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512. Because the RIAA subpoena relates to conduct outside the limited scope of the extraordinary subpoena authority created by the DMCA, it is invalid and should not be enforced.

INTRODUCTION AND SUMMARY

Section 512, enacted as part of Title II of the DMCA, was the product of extensive, Congressionally supervised negotiations between Internet service providers who provide millions of citizens with access to the Internet and representatives of copyright owners concerned about infringement of their rights in various ways involving the Internet. The goal of Section 512 was to limit the possible liability of Internet service providers for infringing activities in order that "the efficiency of the Internet will continue to improve and that the variety of and quality of services on the Internet will continue to expand." S. Rep. No. 105-190, at 8 (1998).

Reflecting the fact that Internet service providers offer a variety of services using different functions, Congress defined four separate and distinct functions under Section 512. At one end of the spectrum, Congress recognized in subsection 512(a) that Internet service providers acting merely as passive conduits transmitting information from one user to another, with no involvement in the users' possible infringing activities, should not be liable for those activities and should not be required to monitor them. At the other end of the spectrum, Congress specified in subsection 512(c) that service providers who store material on their systems or networks at the direction of users should have greater obligations, including the obligation (as a condition to limited liability) to remove offending material if a copyright holder submits a notification of claimed infringement as specified in subsection (c)(3)(A). Other

subsections address situations somewhat similar to subsection (C), but with different requirements and obligations for those different functions.

Congress also provided for an extraordinary ex parte subpoena power in subsection 512(h), under which copyright owners could obtain a subpoena in certain limited circumstances to compel Internet service providers which have infringing materials on their networks or systems to identify persons asserted to be engaged in infringing activities. An essential condition of a valid subpoena under subsection 512(h) is a notification to the service provider that complies with subsection (c)(3)(A).

RIAA claims to be proceeding under that subpoena power. It asserts that one of Verizon's subscribers who was online one day in mid-July, using what is called "peer-to-peer" software, offered to share various sound files containing music copyrighted by RIAA members. It is clear from RIAA's assertion, however, that Verizon did not store any of the challenged sound files on its system or network. Verizon thus was not involved with the subscriber's activities except, at most, as a passive conduit within the meaning of subsection 512(a).

The subpoena power set forth in subsection 512(h) of the DMCA does not apply when the service provider acts as a passive conduit. The statute strictly confines the subpoena power to circumstances where the assertedly infringing material is stored on the service provider's system or network.

Specifically, subsection 512(h) mandates that a subpoena must be supported by a notification of claimed infringement that "satisfies the requirements of subsection (c)(3)(A)" -- that is, a notification issued under subsection (c) of Section 512, which is limited to service providers who have stored offending material on their own system or network. Subsection (a) -- the provision of Section 512 for Internet service providers acting merely as passive conduit transmitters, as Verizon was here -- contains no provision for any notification of claimed infringers, much less for a notification that "satisfies the requirements of (c)(3)(A)." Because there was no valid 512(c)(3)(A) notification, the DMCA does not authorize the subpoena.

RIAA is seeking to expand the subsection 512(h) subpoena power to reach all Internet users, not just those who store infringing material on a service provider's system or network. RIAA proposes a dazzlingly broad subpoena power that would allow any person -- without filing a complaint, to invoke the coercive power of a federal court to force disclosure of the identity of any user of the Internet, based on a mere assertion in a form submitted to the court's clerk that the user is engaged in infringing activity. Such a broad-ranging invocation of federal judicial authority, as a pure investigative tool outside the context of a pending case, raises substantial questions as to whether it exceeds the power of an Article III Court.¹ Further, a procedure that would give private parties unfettered authority to force disclosure of the identities of persons using the Internet, not tied to any infringing material residing on the service provider's system or network, raises substantial First Amendment concerns in light of the well-established freedom to engage in anonymous speech -- a general principle² that has been specifically applied to protect anonymous speech over the Internet.³ These substantial constitutional questions are yet a further reason for rejecting RIAA's overly expansive reading of the DMCA subpoena power, under the settled principle that statutes should be construed, if possible, in a manner that avoids or minimizes constitutional concerns.

Contrary to RIAA's suggestion, a proper construction of the subsection 512(h) subpoena power -- which avoids or minimizes these substantial constitutional concerns -- would not leave copyright owners powerless to pursue infringement claims on the Internet. For example, if RIM believes that the Internet user who was online at the IP address at the specified time identified in its subpoena is a serious infringer, it can initiate a "John Doe" lawsuit against the person described in its present ex parte subpoena, and issue an orthodox Rule 45 subpoena to Verizon for information sufficient to identify the asserted infringer. A judge presiding over that action (or a judge in the court where the subpoena was issued) could carefully weigh the 5 constitutional implications and determine the propriety of such a subpoena.

Verizon proposed this alternative to RIAA here, but RIAA rejected it and chose instead to file this motion as a test case. But the filing of an Article III lawsuit, as an alternative to the approach RIAA has chosen, is more than a formality or technicality. The filing of a complaint ensures that the allegations "have evidentiary support" or "are likely to have evidentiary support" Fed. R. Civ. P. 11(b)(3). Permitting forced disclosure of the identities of Internet users, without a "case or controversy" in the form of a filed lawsuit, would pose a grave threat of widespread abuse of this Court's subpoena power including by marketers, pornographers, based on flimsy assertions of copyright infringement and others who could invoke the DMCA procedures under the unfettered subpoena authority posited by RIAA. ~ Part 2 below). That is not what the statute says, and it cannot be what Congress intended.

STATEMENT OF THE FACTS

The RIAA Subpoena and "Notification"

On July 24, 2002, RIM served a subpoena issued under the purported authority of subsection 512(h) of the DMCA, 17 U.S.C. § 512(h), directing Verizon to disclose the identity of a subscriber to Verizon's Internet access service who was online at the "IP address: 141.158.104.94 on 7/15/02 at 5:26 p.m. (EDT)." (Attachment A to RIM Motion). The subpoena was accompanied by a July 24, 2002 letter from RIM to Verizon stating that the subscriber was believed to be "offering for download [by other Internet users] files containing copyrighted sound recordings through a peer to peer application" without the authorization of the copyright owners represented by RIAA. (Attachment B to RIAA Motion). Attachments to the letter make it appear that the peer-to-peer file-sharing was being done through software provided by KaZaA, a popular provider of such applications. The letter also demanded that Verizon "remove or disable access" to the files "via your system" although RIAA did not assert -- and could not assert -- that the files reside on Verizon's system. (Attachment C to RIAA Motion).

Verizon's Internet Access Service

Verizon is an Internet service provider that provides Internet access to over one million subscribers. With respect to the subscriber described by the RIAA subpoena, Verizon served solely as the subscriber's service provider and in that capacity provided only transmission services to the subscriber in connection with transmitting assertedly offending material that the subscriber may have received from or sent to other Internet users. There is no business relationship between Verizon and KaZaA. Any transmission of the material to and from the subscriber was initiated by and at the direction of the subscriber. Verizon carried out the requested transmission through an automatic technical process in which Verizon neither selected the material that was sent nor selected the recipients of the material. During the transmission of any material to or from the subscriber, no copy of the material was maintained on Verizon's system or network. Further, in transmitting the assertedly offending material to and from the subscriber, Verizon did not modify its content. (Declaration of Scott E. Lebrede in Support of Opposition by Verizon Internet Services to Motion to Enforce Ex Parte Subpoena Issued July 24, 2002, at 5) ("Lebrede Decl.").

As a passive provider of transmission services to the subscriber, Verizon did not store, cache or otherwise make any intermediate or temporary copy of material the subscriber received from or transmitted to other locations on the Internet. (M. at 1 6). Nor did Verizon store any material on its system or network at the direction of the subscriber. (M. at 7). With regard to the activities of the subscriber at issue, Verizon also did not refer or provide a link to any online location through the use of any information location tools. (M. at 1 8).

Peer-to-Peer Applications

Millions of Internet users communicate with each other on the Internet through peer-to-peer file-sharing software programs that allow a group of computer users to share information stored on each other's computers. Peer-to-peer file-sharing has many presumptively lawful

applications. Such software allows users to locate and share files containing, for example speeches by various American presidents and political activists. In other uses, some companies employ peer-to-peer file sharing as a way for employees to share files without the expense of a centralized server or as an inexpensive way for companies to exchange information with other companies. Many individuals use peer-to-peer file-sharing to exchange information (e.g., photographs taken with digital cameras) with others who share like interests. (Lebrede Decl. at 19).

A variety of entities provide specialized peer-to-peer file-sharing software. This software allows an Internet user to share files with other users of the software by permitting each user to review a list of available files maintained by other users or to request files of a particular description maintained by other users. The software then attempts to identify other users of the software who are also online and who have the requested files available to share. Once the requested file is located on another computer, the software allows the files to be transferred between the two computers. (id. at 10).

KaZaA provides a popular version of this specialized software for peer-to-peer file-sharing. According to KaZaA's Internet homepage, more than 100 million copies of its peer-to-peer file-sharing software have been downloaded, and more than two million of its users are commonly online at any given time. (id. at 11).

The Process of Identifying Subscribers on the Basis of IP Addresses

The RIAA Motion to Enforce asserts without explanation or evidentiary support that Verizon could comply with the subpoena by identifying the subscriber "in a matter of seconds" and that compliance with such subpoenas "will require only a simple and ministerial act by Verizon, putting virtually no burden on them." (RIAA Motion II, 12). This is incorrect.

As set forth in the Declaration of Scott E. Lebrede accompanying this Opposition, substantial time and effort is required for Verizon to determine the identity of even one of its subscribers based only on information that the subscriber was operating at a particular IP address at a particular time on a particular day (most Verizon subscribers normally receive a different IP address frequently or each time they access the Verizon service). To determine a subscriber's identity based on this information, Verizon must employ a software tool to search its records and then go through a second process to verify the identity of the subscriber.

While the amount of time necessary to identify a subscriber varies, on average it takes between 15 and 25 minutes to identify a single subscriber. Thus, if Verizon were asked to identify five subscribers, the process could take a Verizon employee over two hours. If Verizon were asked to identify 1,000 subscribers, the process of identifying the subscribers could take Verizon employees more than 400 hours. (Lebrede Decl. at 12). The task of responding to requests to provide this information to third-parties such as RIM would take substantial time and effort over and above the 15 to 25 minutes per request described above. RIAA has not said how frequently it intends to issue subpoena requests if its interpretation of Section 512(h) is adopted, but Verizon understands that RIM uses Internet robots, or "bots," to search for possible infringements. These "bots" are capable of automatically generating an unlimited number of subpoena requests.

ARGUMENT

I. THE DMCA DOES NOT AUTHORIZE A SUBPOENA WHEN THE OFFENDING MATERIAL IS NOT STORED ON THE SERVICE PROVIDER'S SYSTEM BUT IS MERELY PASSIVELY TRANSMITTED BY THE PROVIDER

A. Title II Of The DMCA Was Carefully Negotiated Legislation Intended To Protect Service Providers From Liability And From Unreasonable Burdens, Particularly When Acting As A Passive Conduit Transmitter of Materials.

Title II of the DMCA was enacted to ensure the continued growth of Internet services by, among other things, providing assurance to Internet service providers that they would not be held liable for copyright infringement as a result of the conduct of third parties, including their subscribers. As the legislative history explains, "by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand." S. Rep. No. 105-190, at 8 (1998).⁶

Title II also ensures that Internet service providers are not subjected to unreasonable burdens related to the enforcement of copyrights by their owners. Thus, Section 512 makes clear that service providers are not obligated to monitor their services or seek facts that may indicate infringing activity. 17 U.S.C. § 512(m). The scope of injunctive relief available against service providers is specifically limited, and before an injunction is issued a court must consider whether the injunction (either alone or in combination with other injunctions issued under subsection 512(j)) "would significantly burden either the provider or the operation of the provider's system or network." 17 U.S.C. § 512(j)(1) & (2).

Section 512 is based throughout on a careful delineation of four different, specifically defined functions performed by service providers, each of which is subject to different liability limitations, procedures, and obligations. As the Senate Report explains, "[I]n the beginning, the Committee identified the following activities (1) digital network communications, (2) system caching, (3) information stored on services providers, and (4) information location tools." S. Rep. No. 105-190, at 19. These activities are the subject of subsections 512(a), (b), (c) and (d), respectively. As Section 512 itself makes clear, "Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section." 17 U.S.C. § 512(n) (emphasis added)!

The conduit function at issue here is the subject of subsection 512(a), captioned "Transitory Digital Network Communications," which applies where the service provider is simply "transmitting, routing, or providing connections for" material through its system or network. Congress recognized that service providers cannot reasonably be held responsible for the conduct of their users when they perform such conduit functions, and provided them the greatest scope of virtually unconditional protection, with no obligations. Thus, contrary to RIAA's implication (RIAA Motion 6 & n.2, 9, 14), under subsection (a) the knowledge of the service provider is irrelevant, the financial interest of the service provider in the transaction is irrelevant, and there is no "takedown" obligation "to remove, or disable access to" offending material. Compare 17 U.S.C. § 512(a) ~ 17 U.S.C. § 512(c). Similarly, subsection 512(a) has no provision for a copyright owner to provide a notification of claimed infringement to a service provider acting within the conduit function. ~ 17 U.S.C. § 512(a).

At the other end of the spectrum is subsection 512(c), captioned "Information Residing on Systems or Networks at Direction of Users." The limitation of liability provided by this subsection applies only where the provider does not have actual knowledge of infringing activity, and does not receive a financial benefit from infringing activity that it can control. Further, subsection (c) creates an elaborately defined "notice and takedown" process, by which a copyright owner can submit a notification of claimed infringement to the service provider requesting the provider to remove or disable access to infringing material residing on the system or network of the service provider. Subsection 512(c)(3), on which RIAA bases its argument, defines the elements of a notification necessary to trigger the takedown process under subsection 512(c).

Subsection 512(b), captioned "System Caching," provides specific rules governing the temporary caching by a service provider of material on its system or network in certain circumstances. The subsection includes a specific description of the caching function and affords service providers an intermediate level of liability protection between the high level of

protection for the conduit function and the more limited protection for material "residing" on the service provider's system or network. For example, subsection (b) conditions protection from liability upon several requirements, but does not include the provisions of subsection (c) that the provider must not have actual knowledge of infringing activity nor receive any financial benefit from it. Subsection (b) contains a form of notice and takedown process, "modeled on the procedure under subsection (c)." S. Rep. No. 105-190, at 43. However, the caching service provider's takedown obligation is more limited and applies only if the copyright owner notifies the service provider that cached material was removed from the originating location (or is subject to a court order of removal).

Finally, subsection 512(d), captioned "Information Location Tools," addresses the function of the service provider using or hosting "information location tools" such as directories, indexes, or hyperlinks on its system or network. This subsection includes a knowledge and financial benefit standard. It also contains notice and takedown processes based on the procedures described in subsection (c), but modifies the required notification of claimed infringement to conform with subsection (d) by requiring an identification of the "reference or link" to be removed from the service provider's system.

This carefully articulated statutory framework was the product of extensive negotiation and collaboration between industry groups and Congress, a process aimed at devising fair solutions and compromises in an area of competing and potentially divergent interests.⁹ In such circumstances, the language of the statute should be closely followed and given a strict construction. ~ *United States v. Sisson*, 399 U.S. 267, 291 (1970) (the "compromise origins" of an act "justify the principle of strict construction"); *Rodriguez v. ComRass ShiDDing Co.*, 451 U.S. 596, 617 (1981) (where a legislative compromise has occurred "the wisest course is to adhere closely to what Congress has written").

B. A Subpoena Under Subsection 512(h) Is Not Available In Connection With The Passive Conduit Function Of A Service Provider; It Is Limited By The Express Terms Of The Statute To Infringing Material Stored On A Service Provider's System Or Network.

Although RIAA argues that the plain language of Section 512 must govern this case (RIAA Motion 9-10), it asks this Court to ignore an express condition imposed by Congress on the issuance of a subpoena under subsection 512(h). Specifically, subsection 512(h) requires that the subpoena request be accompanied by a "copy of a notification described in subsection (c)(3)(A)" ~, a "notice and takedown" request) and provides that the subpoena may only be issued "[i]f the notification filed satisfies the provisions of subsection (c)(3)(A)." 17 V.S.C. § 512(h)(2)(A) & (h)(4).

Subparagraph (c)(3)(A) of Section 512 specifically defines the requirements for a notification of claimed infringement "[t]o be effective under this subsection." 17 V.S.C. § 512(c)(3)(A). The reference to "this subsection" means subsection (c), which addresses only material residing on a service provider's system or network. A notification such as that submitted by RIAA, which addresses peer-to-peer file activities where the service provider acts as a passive conduit under subsection 512(a) transmitting material that does not reside on its system or network, simply cannot be "effective" under subsection (c). RIAA's notice therefore cannot "satisf[y] the provisions of subsection (c)(3)(A)" as required by subsection 512(h)(4) for the issuance of a valid subpoena. Indeed, as noted earlier, there is no provision for any form of notification of claimed infringement in subsection 512(a), which governs the conduit function at issue here. Thus, there is no such thing as a meaningful or "effective" notice with respect to the conduit function.

RIAA asserts that paragraph (3)(A) of subsection (c) should be viewed as a "freestanding" provision of Section 512. (RIAA Motion 4, 17). But it is not. It is an integral

part of subsection (c). Had Congress intended the notification requirement to be "freestanding" it could easily have made it so, as a separate subsection. Instead, Congress included the notification requirement in subsection (c) and emphasized the importance of that placement by expressly instructing courts that "Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section." 17 U.S.C. § 512(n).

The subsection (c)(3)(A) notification required by subsection (h) expressly must include identification of the material "to be removed or access to which is to be disabled" and information allowing the service provider "to locate the material." 17 U.S.C. § 512(c)(3)(A)(iii). These requirements can only refer to material residing on the service provider's system or network. Verizon cannot "locate" infringing material within the meaning of subsection (c)(3)(A) if the material is not stored on Verizon's system or network. Presumably, the sound files that RIAA asserts the subscriber shared with other KaZaA users are located on the subscriber's personal computer, but Verizon does not know that and has no ability to reach into its subscriber's personal computer to check. Nor can Verizon disable or remove "the material" if it is not stored on Verizon's computers. The only way Verizon could "disable access" to material stored on a subscriber's computer would be by terminating the subscriber's entire Internet access account (including applications having nothing to do with the alleged infringement, such as the user's email). However, that is not the way Congress used the term "remove, or disable access to, the material" in subsection (c)(1)(C), where the reference is plainly to specific infringing "material" on the service provider's system or network. Congress was not speaking of requiring the service provider to terminate a subscriber's entire access to the Internet merely on the basis of a copyright owner's assertion of infringement.

When Congress wanted to speak of requiring a service provider to cease providing "access to a subscriber" (emphasis added) by "terminating the accounts of the subscriber," it plainly knew how to do so, as it did in describing possible forms of injunctive relief -- which could only be awarded if the copyright owner filed an actual case in court - under subsections 512(j)(1)(A)(i) and (B)(i) (preventing the issuance of "an order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network. . . by terminating the accounts of the subscriber or account holder that are specified in Congress did not use such language in describing the required content of a valid the order"). subsection (c)(3)(A) notification identifying the "material" on the service provider's system "that is to be removed or access to which is to be disabled."

It would be a severe remedy, and a severe burden on free speech, to allow a copyright owner to bar an individual from any access to the Internet based merely on an assertion of copyright infringement. The language of the statute does not support this outcome, and Congress could not have intended it.

RIAA attempts to argue that subsections (b) and (d) provide for takedown notifications, and that this must mean that Congress intended the subpoena power to apply where the service provider was not storing materials on its system or network. (RIAA Motion 18). But contrary to RIAA's arguments, those subsections only apply to situations where the service provider is storing offending material on its system or network-- cached materials that the provider has placed in "intermediate and temporary storage... on [its] system or network" in subsection (b), and information location tools including an actual "reference or link" on the system or network in subsection (d). II

More fundamentally, there is no need here to decide whether a notification under subsection (b) or (d) could be regarded as a "(c)(3)(A)" notification justifying a subpoena under subsection (h). The decisive point for purposes of this motion is that there is no provision at all for any takedown notification with respect to the conduit function described in subsection (a), which is the situation at issue here. There is indeed no reference whatever in subsection (a) to any material that is to be "removed" or "access to which is to be disabled" by a passive conduit service provider.

In addition, the reason why Congress required that an "effective" subsection (c)(3)(A) notification must include an "identification of the material. . . that is to be removed or access to which is to be disabled" does not apply to passive conduit activity under subsection (a). The "goal of this provision" requiring "information reasonably sufficient to permit the service provider to identify and locate the allegedly infringing material" is to allow the service provider "to find and examine the allegedly infringing material expeditiously" if it chooses to determine whether the requested action is appropriate. H.R. Rep. No. 105-551, pt. 2, at 55 (1998). A purported notification directed to a passive conduit service provider under subsection (a) does not accomplish this goal of allowing the provider "to find and examine the allegedly infringing material" on its system or network, since the infringing material is not on the service provider's network or system and cannot be examined by the service provider.

The requirement in subsection (c)(3)(A)(iii) that a valid notification must include information sufficient to allow the service provider to "locate the material" in order to be able to examine it thus underscores that the subsection (c)(3)(A) notification required for a subpoena applies only to allegedly infringing material residing on a service provider's network or system under subsection (c), and not to a provider acting merely as a passive conduit under subsection (a).

C. RIAA's Attempt To Read The Requirement For An Effective Subsection 52(c)(3)(A) Notification Out Of Subsection 512(h) Is Unavailing.

RIAA argues that Verizon "confuses two totally different things" (RIAA Motion 9) when Verizon points out that subsection 512(h) explicitly provides that a subpoena can only be issued if the subpoena request is accompanied by a notification of claimed infringement that "satisfies the provisions of subsection (c)(3)(A)." 17 U.S.C. § 512(h)(4). RIAA asserts that a notification of claimed infringement relates only to a service provider's duty to remove infringing material upon notice "in order to maintain limitations on its own liability," while the subsection 512(h) subpoena power supposedly addresses the separate matter of the service provider's "obligation to provide the information that copyright owners need to address infringement being committed by others." (RIAA Motion 9).

The difficulty with this argument is that Congress wrote the statute differently. It made the requirement for a valid and effective notification satisfying the requirements of subsection (c)(3)(A) an explicit precondition for the issuance of a subpoena. Indeed, Congress referenced the need for a subsection (c)(3)(A) notice not once but three separate times in defining the exercise of subpoena power in subsection 512(h). 17 U.S.C. § 512(h)(2)(A), (4) and (5).

RIAA also suggests that the decision in *ALS Scan, Inc. v. Rembert Communities, Inc.*, 239 F.3d 619, 620 (4th Cir. 2001), which concluded that a DMCA notification of infringement was properly drafted, is somehow controlling here. But *ALS Scan* arose under subsection 512(c) of the statute, as the court explicitly noted. 14. at 623. *ALS Scan* involved "an online Internet service provider that provide[d] access to its subscribing members. . . to over 30,000 newsgroups which cover thousands of subjects," m. at 620, comprising material that was actually residing on the service provider's system or network. *ALS Scan* therefore simply does not address the propriety of a subpoena involving passive conduit activity described by subsection 512(a), the issue here.

2. A'S ATTEMPT TO RADICALLY EXPAND THE EX PARTE SUBPOENA POWER OF SUBSECTION 512(h) WOULD HAVE DRAMATIC IMPLICATIONS.

RIAA characterizes this case as "a straightforward subpoena enforcement action." (RIAA Motion 2). By downplaying the issue presented, however, RIAA masks the dramatic

impact that its expansive interpretation of the subsection 512(h) subpoena power would have on service providers and, even more importantly, the Internet user community. If service providers were forced to comply with subsection 512(h) subpoenas whenever a copyright holder asserts a "good faith belief that infringement is occurring" (RIAA Motion 3), the predictable result would be to uncork a tidal wave of subpoenas in every instance where a copyright owner suspected that a subscriber had infringing material on his or her personal computer, or had transmitted infringing material.

RIAA argues that the language of subsection 512(h)(1) is exceptionally broad, and can be read in isolation from the requirement for a valid subsection 512(c)(3)(A) notification and the other provisions of Section 512. If read in this fashion, subsection 512(h)(1) might be argued to command a service provider to provide any available information regarding any user whom a copyright owner believed it had reason to suspect of any form of copyright infringement that somehow involves the Internet. Even if only users of the KaZaA peer-to-peer file-sharing software are considered, RIM's proposed construction of subsection 512(h) would allow RIM to obtain subpoenas requiring service providers to identify any or all of the more than 100 million users who have downloaded KaZaA software, one million of whom are Verizon subscribers. And KaZaA is, of course, only one of a number of popular peer-to-peer file-sharing software programs.

In bringing this as a test case to establish a precedent, RIAA has issued a subpoena asking for the identity of only a single Verizon subscriber. But identifying a single subscriber out of, apparently, tens of millions of KaZaA users would be meaningless for RIAA. Nothing could be more certain than that future subpoenas would demand the identity of subscribers for much longer lists of IP addresses. Contrary to RIM's suggestions (RIAA Motion 11, 12), identifying users on the basis of an IP address in use at some date in the past is time-consuming ~ Lebrede Declaration 1 12), and could impose a crushing burden on service providers, depending on the number of IP addresses RIAA or other copyright owners or their representatives decided to include in future subpoenas. There is nothing under RIM's interpretation of the subpoena power to limit those numbers or the potentially overwhelming burdens on service providers.

Even more importantly, there is nothing under RIAA's interpretation of the subpoena power to limit such subpoenas to attempts to obtain the identity of suspected users of peer-to-peer file-sharing software such as KaZaA. If all that is required is an assertion of suspected infringement and a "freestanding" notification of infringement (RIAA Motion 4, 17), any copyright owner could issue such a subpoena. The extraordinary scope of RIAA's desired construction can only be appreciated when it is understood that (i) everyone can be a copyright owner; and (ii) every transmission on the Internet implicates activities within the scope of the exclusive rights of copyright owners.

A copyright subsists automatically in any "work of authorship" fixed in any tangible medium of expression. 17 U.S.C. § 102. If someone writes an article, a letter, or even an e-mail, the author owns a copyright; if someone creates a commercial or personal web page, there is also a copyright. Essentially everyone is or can easily be a copyright owner. The required element of "originality" is met by only a "minimal degree of creativity." *Feist Publications, Inc. v. RYrn Telephone Service Co.*, 499 U.S. 340,345 (1991). There is no obligation to register a copyright or to include any notice in order to own a copyright. 17U.S.C. §§ 401, 405, 408. A copyright grants the owner a broad range of exclusive rights, including the rights to authorize the making of copies of the work, the public distribution of the work, the public performance of the work, and the public display of the work. 17 U.S.C. § 106. In virtually every instance when a work is transmitted over the Internet, a copy is made, and often stored, in the receiving computer. In addition, although the law is not settled, copyright owners argue that many Internet transmissions implicate rights to control the public distribution, public performance, and public display of copyrighted work.

Service providers act as passive conduits for much more, of course, than the transmission of files at the request of persons using peer-to-peer file-sharing software. A service provider acts as a conduit whenever a user sends or receives e-mail, or downloads material from a web site. Nothing in RIAA's proposed construction of the subsection 512(h) ex parte subpoena power would limit such subpoenas to the situation of peer-to-peer file-sharing.

If RIAA were correct in its construction of subsection 512(h), the potential for uncontrollable abuse would be enormous. It would not be difficult for any copyright owner (~, virtually anyone) to contrive asserted copyright infringements in order to obtain identifying information about private citizens using the Internet. To offer but a few examples, a marketer could create a web site, include an "agreement" prohibiting downloading by any web user that did not voluntarily provide their name and address, and then demand from a service provider the identification of every subscriber that used the service to access the web site and download copyrighted material without providing the requested information. A blackmailer could demand the identification of any subscriber that accessed a "copyrighted" pornographic site or a site with "copyrighted" material dealing with a socially-sensitive disease, and then threaten the person with public disclosure. A person seeking the identity of Internet users for improper purposes (such as a stalker, pedophile or private detective) could demand the identity of a user who exchanges e-mails with that person and stores copies of those "copyrighted" messages on her/his computer. RIM is, of course, a bona fide organization pursuing business ends it believes are legitimate, but its construction of the statute would open up these opportunities for abuse of the subpoena power.

Requiring service providers who are merely acting as passive conduits under subsection 512(a) to respond to any and all such subpoenas would at best turn the service providers into an Internet police force (and in the process impose a compliance burden stretching far beyond what Congress contemplated when it enacted subsection 512(h)'s ex parte subpoena power). And at worst, it would force the disclosure of identifying information that would expose private citizens using the Internet to harassment or more. Such a broad-ranging power to force disclosure of the identities of Internet users would pose grave threats to their legitimate First Amendment interests in privacy and anonymity. ~ pages 3-5 and notes 2 and 3, ~.

But, as the preceding discussion has shown, the requirement for a valid subsection (c)(3)(A) notification confines and limits the subpoena power to those situations in fact contemplated by Congress, and minimizes the potential for such abusive subpoenas. An application for a subsection 512(h) subpoena must be supported by "(A) a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an asserted infringer and that such information will only be used for the purpose of protecting rights under this title." Requirements (B) and (C) can be satisfied perfunctorily in any case of asserted copyright infringement. But clause (A) of subsection 512(h)(2), mandating a notification authorized by the statute and in compliance with subsection 512(c)(3)(A), prevents the subpoena power from being extended to every suspected occurrence of copyright infringement involving the Internet.

RIAA argues that its unboundedly expansive reading of the subpoena power is justified because it has no other way to obtain the identities of persons who it believes are infringing its members' copyrights. But, as discussed at the outset of this Opposition, that is simply not so. RIAA has the alternative of filing an actual lawsuit, which it has declined Verizon's invitation to do, and to seek the identity of asserted infringers through an orthodox Rule 45 subpoena under the supervision of a court that can assess RIAA's need and justification for such private information.

The filing of a lawsuit, as the means for RIAA or other copyright owners to determine the identity of Internet users with allegedly infringing materials on their personal computers, is far more than a technical distinction in comparison to the vast-ranging subpoena authority urged by

RIAA. First, such a lawsuit avoids the severe Article III concerns that are presented by allowing a private party to invoke the coercive power of the federal judiciary for purely investigatory purposes outside the context of a pending lawsuit. ~ page 4 & note 1,~. Further, any such lawsuit is subject to the protections of Rule 11, ensuring that the allegations of copyright infringement "have evidentiary support" or "are likely to have evidentiary support" after a "reasonable opportunity for further investigation," and that sanctions are available for violation of these standards. Fed. R. Civ. P. 11(b)(3) & (c). The DMCA has no comparable provisions to ensure evidentiary support for assertions of copyright infringement, or to impose sanctions if such assertions are not well-founded. 14 To the contrary, RIAA's proposed construction would allow for robot-generated notices of infringement whenever a computer detects Internet activity involving peer-to-peer file-sharing of music files, or other automatic processes that would flood service providers with subpoenas, without any sanctions for robot-generated errors. Without any requirement of evidentiary support, or any power to impose sanctions for ill-founded assertions of copyright infringement, the potential for widespread abuse of the coercive subpoena powers of the federal courts is apparent.

CONCLUSION

For the foregoing reasons, the motion by RIM to enforce the ex parte subpoena issued to Verizon on July 24, 2002 should be denied. In view of the significant legal issues presented, Verizon respectfully requests oral argument.

Dated: August 30, 2002