UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
GREENSBORO DIVISION

Case No. 1:03MC138

IN RE SUBPOENA TO UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL	**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF JOHN DOE'S MOTION TO QUASH THE SUBPOENA ISSUED BY RIAA TO UNC**
RECORDING INDUSTRY ASSOCIATION OF AMERICA, v. UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL	**Hearing Requested**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATE CASES

STATUTES

MISCELLANEOUS

INTRODUCTION

Relying on the novel provisions of Section 512(h) of the Digital Milennium Copyright Act ("Section 512(h)"), the Recording Industry Association of America ("RIAA") has issued a subpoena to the University of North Carolina at Chapel Hill ("UNC") that seeks to uncover the identity of John Doe, an anonymous UNC student using the Internet. John Doe[1] brings this motion to quash that subpoena.

Section 512(h) purportedly authorizes the issuance of this subpoena through a ministerial procedure that does not: (1) require that the subpoena be in support of a case or controversy; (2) provide notice to the affected Internet user of the existence of the request; (3) require the subpoenaing party to detail the specifics of the claim; (4) afford the Internet user an opportunity to be heard; or (5) require a judge to review the legal and constitutional issues presented and make a judicial determination. Instead, all that is needed is a "good faith" assertion by the subpoenaing party. This provision violates Article III's clear mandate that courts may act, and judicial process may be obtained, only in pending cases or controversies.

Section 512(h) is also so devoid of procedural protections that it is an invitation to mistake and misuse. Although it is a relatively new provision, numerous examples of erroneously and abusively issued Section 512(h) subpoenas have already been reported, including the erroneous filing of a lawsuit seeking hundreds of millions of dollars against a 65 year-old grandmother and the improper issuance of subpoenas by companies such as Wal-Mart to suppress legitimate and non-infringing speech about the price of their goods. It is for precisely this reason – to ensure that fundamental rights are not mistakenly or unnecessarily curtailed – that the Due Process Clause of the Fifth Amendment requires adequate procedural safeguards before individuals can be deprived of a protected liberty interest that fundamentally implicates the protection of freedom of expression.

RIAA's subpoena seeks the name, address and telephone number of a UNC student who

[1] John Doe respectfully declines to provide his full name and address in this motion. Through this motion to quash, John Doe seeks to protect his identity from disclosure. Counsel will provide John Doe's identifying information *in camera* to the Court, if so requested.

was using the Internet to communicate anonymously with other Internet users. Quite apart from the important privacy and personal security issues at stake, the right to engage in anonymous speech is guaranteed by the First Amendment. It is also a liberty interest protected by the Due Process Clause. The student's identity cannot, thus, be disclosed absent sufficient procedural protections. That the speech at issue here is alleged to constitute copyright infringement does not matter. Section 512(h) authorizes issuance of a subpoena before any determination has been made that the speech actually constitutes copyright infringement or that it is even reasonably likely to be held to be infringing. Because Section 512(h) lacks adequate safeguards to ensure that vital rights are not curtailed, it violates the Due Process Clause of the Fifth Amendment.

Even if Section 512(h) were constitutional, the subpoena should still be quashed because the subpoena is not authorized by the statute and is procedurally deficient.

FACTUAL BACKGROUND

A. The Procedure For Obtaining A Section 512(h) Subpoena.

Issuance of a Section 512(h) subpoena is a purely ministerial act by the clerk of the court and must be granted – without any questions – upon the mere submission of: (1) a proposed subpoena; (2) a sworn declaration that the subpoena's purpose is to identify an alleged infringer and to protect copyright rights; and (3) a copy of a Section 512(c)(3)(A) notice, identifying some of the copyrighted work(s) at issue and alleging that the copyright holder has a "good faith belief" that such copyrighted material is being used without authorization. 17 U.S.C. § 512(h).

Nothing more is necessary. No notice need be provided to the individual whose identity is being sought. Nor must that individual be given an opportunity to challenge the subpoena. Although the statute requires a "good faith belief" that the conduct in question violates a copyright, the statute imposes no due diligence requirement on the party seeking the subpoena to verify its "belief" in any manner.[2] Nor does the statute require the subpoenaing party to provide specific allegations supporting its claim or to present any evidence supporting its belief. Most

[2] *See Rossi v. Motion Picture Ass'n of Am.*, 2003 U.S. Dist. LEXIS 12864, *8-9 (D. Haw. Apr. 29, 2003) ("good faith" provision in Section 512(c) does not "require[] a copyright holder to conduct an investigation to establish actual infringement prior to sending a notice to an ISP").

importantly, the subpoenas are issued without any judicial oversight or review, rendering the required recitations mere chimerical protection for consumers.

Section 512(h), which is available to anyone claiming to be a copyright holder or an agent of a copyright holder, does not even require the requesting party to show any proof that it is actually the owner of a valid copyright or a true agent. The request for the subpoena need not be signed by a member of the bar. Nor is there any way for the clerk to verify the self-serving assertions in the request. So long as the proper words are recited, the statute requires the clerk to issue the subpoena – without questions.

B. The Potential For Mistake and Misuse of The Section 512(h) Procedure.

Given how easy it is to obtain a Section 512(h) subpoena and how few procedural protections there are, there is a substantial risk that Section 512(h) subpoenas will be both mistakenly issued by legitimate copyright holders and abusively issued by those with improper purposes. This fear is not merely hypothetical. Numerous examples of mistake and misuse have already been reported. Indeed, RIAA has admitted that in one single week, it committed several dozen errors in sending out accusatory notices of copyright infringement under Section 512(c)(3)(A), a sister provision to Section 512(h).[3] *See* McCullagh, *RIAA Apologizes For Erroneous Letters*, CNET News, May 13, 2003, http://news.com.com/2100-1025-1001319.html.

The following examples of mistaken and erroneous uses of Section 512 – honest mistakes that would not have occurred if adequate safeguards were in place – are illustrative:

- RIAA issued a Section 512(h) subpoena, obtained the identity of an anonymous individual, and filed a federal copyright infringement action seeking damages of up to $150,000 per song, based on its sworn "good faith" belief that the defendant had downloaded over 2,000 copyrighted songs, including the song, "I'm a Thug," by the rapper Trick Daddy. As it turned out, the defendant whose anonymity was breached is a 65 year-old grandmother who has never downloaded songs and does not own a computer capable of running the software allegedly used. *See* Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sep. 24, 2003, C1.

- RIAA obtained the identity of a Los Angeles resident through a Section 512(h) subpoena and filed a lawsuit against him, seeking millions of dollars in damages for the defendant's alleged downloading of music. As it turns out, the IP address

[3] Errors and misuse of the 512(c)(3)(A) notice provisions are directly relevant to Section 512(h) subpoenas because those 512(c)(3)(A) notices are a prerequisite for obtaining a Section 512(h) subpoena.

allegedly used for the downloading is not defendant's, and the defendant did not have the file sharing software allegedly used. In addition, the allegedly infringed songs are primarily Spanish-language songs; the accused individual does not understand Spanish and does not listen to songs in Spanish. *See* Menn, *Group Contends Record Labels Have Wrong Guy*, Los Angeles Times, Oct. 14, 2003.

- Warner Brothers sent a notice to an ISP that alleged that an illegal copy of the film "Harry Potter and the Sorcerer's Stone" was being made available on the Internet. The notice stated that the requesting party had the requisite "good faith belief" that copyright infringement had taken place over the ISP's connection at a specific date and time, and demanded that the ISP terminate the anonymous user's account. As it turned out, the material in question was a child's book report.

- RIAA sent a notice to Penn State's Department of Astronomy and Astrophysics, accusing the university of unlawfully distributing songs by the pop singer Usher. In fact, RIAA mistakenly identified the combination of the word "Usher" – identifying faculty member Peter Usher – and an *a capella* song performed by astronomers about a gamma ray as an instance of copyright infringement. RIAA blamed a "temporary employee" for the error and admitted that it does not routinely require its "Internet copyright enforcers" to listen to the song that is allegedly infringing. *See* McCullagh, *RIAA Apologizes for Threatening Letter*, CNET News, May 12, 2003, http://news.com.com/2100-1025_3-1001095.html.

- A purported copyright owner sent a notice of copyright infringement to the Internet Archive, a well-known website containing numerous public domain films, in connection with two films, listed on the website as 19571.mpg and 20571a.mpg. As it turned out, the sender had mistaken the two public domain films for the popular copyrighted movie about a submarine, "U-571." *See* <http://www.chillingeffects.org/notice.cgi?NoticeID=595>.

Mistaken use of Section 512 is bad enough. Even worse is that many companies and individuals will try to take advantage of the easily invoked provisions of Section 512(h) for improper purposes. Several instances of deliberate misuse of Section 512 have been reported:

- Wal-Mart sent a Section 512(h) subpoena to a comparison-shopping website that allows consumers to post prices of items sold in stores. The subpoena sought the identity of a consumer who had anonymously posted price information. Wal-Mart claimed that its prices were copyrighted; in fact, prices are not copyrightable facts. K-Mart, Jo-Ann Stores, OfficeMax, Best Buy and Staples have also improperly served Section 512(c) notices on the same theory. *See* McCullagh, *Wal-Mart Backs Away from DMCA Claim*, CNET News, Dec. 5, 2002, <http://news.com.com/2100-1023-976296.html>.

- An electronic voting machine company has flooded ISPs with Section 512 notices claiming copyright infringement in an effort to remove thousands of embarrassing internal e-mails from websites critical of the company. The documents are covered by the fair use doctrine, yet the notices have been successful in scaring ISPs into removing the material, thus effectively censoring the public debate. Roberts, *Diebold Voting Case Tests DMCA*, PC World News, Nov. 4, 2003, http://www.pcworld.com/news/article/0,aid,113273,00.asp.

- The Church of Scientology has long been accused of using copyright law to harass and silence its critics. It has apparently begun to use the provisions of Section 512, making DMCA claims against the search engine Google in an attempt to cause it to stop including any information about certain websites critical of the Church. *See* Loney and Hansen, *Google pulls Anti-Scientology Links*, News.com, CNET, March 21, 2002, http://news.com.com/2100-1023-865936.html; *see also* http://www.chillingeffects.org/notice.cgi?NoticeID=232.

- Several owners of trademarks – who have no rights under Section 512 – have asserted DMCA violations in an improper attempt to take advantage of Section 512. *See* http://www.chillingeffects.org/notice.cgi?NoticeID=310.

- A DMCA claim was made – despite the clear existence of a right to fair use – against an individual who posted public court records that contained copyrighted material. *See* http://www.chillingeffects.org/notice.cgi?NoticeID=348.

The instances of mistake and misuse can only be expected to increase. RIAA itself has apparently used Section 512(h) to obtain over 2,200 subpoenas in the past few months alone.[4]

The consequences of Section 512(h)'s lack of protections are far from trivial. In addition to depriving Internet users of their constitutional right to privacy and anonymity, there is nothing to stop a vindictive business from claiming copyright to acquire the identity of an anonymous critic who has posted information on an Internet message board. Even worse, there are no safeguards to stop individuals like batterers, cyberstalkers or pedophiles from using Section 512(h) to obtain – without any questions – an intended victim's name, address and telephone number. This danger is, unfortunately, not far-fetched. In connection with another proceeding, representatives of organizations devoted to online safety and protecting battered women submitted declarations explaining their concerns about how the lack of procedural protections will enable pedophiles and abusive husbands to obtain the identity and physical location of their targets. *See* Declaration of Parry Aftab, WiredSafety.org, available at http://www.eff.org/Cases/RIAA_v_Verizon/20030318_aftab_declaration.pdf; Declaration of Juley Fulcher, National Coalition Against Domestic Violence, available at

[4] The risk of mistake and misuse is magnified – and made even more probable – by the widespread use by companies of automated software robots ("bots") to monitor Internet activity. *See* Ahrens, *Ranger vs. the Movie Pirates*, Wash. Post, June 19, 2002, at H01. When these bots find a possibly suspicious file, they note its location, the date and time, and automatically generate lists – sometimes, even boilerplate Section 512(c) notices – that are sent to the relevant ISPs. These bot-generated notices seem to get little, or no, human review, let alone a meaningful analysis of whether a valid infringement claim or fair use defense exists.

http://www.eff.org/Cases/RIAA_v_Verizon/20030318_fulcher_declaration.pdf. For example, a pedophile who has been talking with another Internet user in an Internet chat room could easily claim copyright in his online postings to obtain – without questions – the identity, telephone number and address of the other participant through a Section 512(h) subpoena.[5]

The need for adequate procedural protections is particularly important for college students, such as John Doe, who are required to use the Internet for their classes, to, among other things, obtain homework assignments and complete their assignments. Under UNC's official Computing Policy, a student's network access through a personal computer is automatically suspended upon the mere receipt of a Section 512 complaint. *See* University Procedure on Dealing with Possible Infringement of Intellectual Property Rights, available at http://www.unc.edu/policy/copyinfringe.html. Indeed, based solely on RIAA's unproven allegation, UNC has suspended John Doe's ability to access the Internet from his computer. Almost two months later, with finals looming, John Doe is still unable to access the Internet on his computer. The only way to restore service is to file a written counter-complaint contesting the termination. Unfortunately, under UNC's policy, that challenge must contain John Doe's name and must get sent to the copyright holder. *Id.*

C. The Subject Matter Of Section 512(h) Subpoenas.

Section 512(h) can be used in a variety of different contexts, to affect any form of speech allegedly constituting copyright infringement, including emails, word documents and web postings. In this particular case, the Section 512(h) subpoena seeks disclosure of the identity of a UNC student using "peer-to-peer technology" on the Internet. Peer-to-peer technology enables users to create networks to connect directly to peers to search for and share information in text, audio or video files. Although it is possible to use these networks to exchange copyrighted material without authorization, many users also share a broad range of material that is either in the public domain – such as the works of Shakespeare, Mozart or the Bible – or whose copyright

[5] The potential for such a scenario should not, unfortunately, be in doubt. *See Greensboro Man Pleads to Kidnap, Rape of Teen He Met Online*, AP, Nov. 13, 2003, available at http://www.wfmynews2.com/news/news.asp?ID=19713.

holders have consented to reproduction and distribution among network users – such as up-and-coming musicians looking to gain a following. *See* Nelson, *Upstart Labels See File Sharing as Ally, Not Foe,* N.Y. Times, Sept. 22, 2003, at C1.[6]

D. Procedural Background.

RIAA first obtained a subpoena to UNC from the district court in Washington, D.C. on October 6, 2003. Because that subpoena was invalid, *see Boston College v. RIAA*, Misc. Act. No. 1:03-MC-10210-JLT (D. Mass. Aug. 7, 2003) (granting motion to quash a RIAA subpoena improperly issued from the D.C. court), RIAA withdrew the subpoena.

RIAA served this second subpoena on UNC on November 12, 2003.[7] The subpoena requires UNC, in its capacity as an Internet Service Provider ("ISP"), to provide the name, address, telephone number and email address of John Doe. The subpoena was accompanied by an undated and unaddressed form letter labeled "Notice to Service Provider," a letter to UNC's copyright agent, and a "Declaration Pursuant to 17 U.S.C. § 512(h)." Neither the subpoena, the letters, nor the Declaration identifies the actual owner(s) of the allegedly infringed copyrights or the specific peer-to-peer files placed on the Internet that are claimed to contain the copyrighted songs allegedly infringed by John Doe.

The question raised by this Motion is whether this subpoena should be quashed because it is not authorized by Section 512(h) and because it is constitutionally deficient.

ARGUMENT

I. THE SUBPOENA IS NOT AUTHORIZED BECAUSE SECTION 512(h) AUTHORIZES A SUBPOENA ONLY WHEN THE INFORMATION AT ISSUE IS STORED ON THE ISP'S SYSTEM.

Section 512 recognizes that ISPs may encounter copyrighted content on their systems in various ways. The statute thus imposes different obligations on ISPs based on their level of

---

[6] Even well-known artists use peer-to-peer technology for commercial purposes. *See* Strauss, *File-Sharing Battle Leaves Musicians Caught in Middle*, N.Y. Times, Sept. 14, 2003, at A1. Peer-to-peer file sharing is also increasingly used in countries where, due to government monitoring and censorship of the Internet, anonymous file sharing is the only safe way to exchange or receive valuable news and cultural materials. *See, e.g.*, *New Technology May Foil PRC Attempts at Censorship Efforts*, The China Post, March 12, 2003, available at 2003 WL 4136640.

[7] A copy of the subpoena is attached as Exhibit A to the LR 7.2 Appendix, filed herewith. Copies of all decisions and materials not appearing in certain published reports cited in this brief are included in the Appendix.

involvement with the content. Here, the alleged infringing files are not stored on UNC's system; they are purportedly on the user's computer. This case is thus controlled by subsection (a), where the ISP performs a pure transmission or "conduit" function. 17 U.S.C. § 512(a). Subsection (c), in contrast, addresses circumstances where material is stored on an ISP's servers at a user's request. 17 U.S.C. § 512(c). In that context, the ISP has access to the allegedly infringing material, and the DMCA thus places certain obligations on the ISP in exchange for immunity, including the duty to "remove" or "disable access to" infringing material upon receipt of a "take down notice" sent by a copyright owner. 17 U.S.C. § 512(c)(3)(A).

Subsection (h), the subpoena provision at issue here, contains numerous cross-references to the take down notice of subsection (c)(3)(A). *See* 17 U.S.C. § 512(h)(2)(A) (the subpoena request must be filed with a "copy of a [take down] notification described in subsection (c)(3)(A)"); *id.* at § 512(h)(5) (an ISP must comply with the subpoena only if there is a (c)(3) notice); *id.* at § 512 (h)(4) (clerk shall not issue a subpoena without a (c)(3) notice). These repeated cross-references demonstrate that the issuance of a Section 512(h) subpoena is dependent upon a proper 512(c)(3)(A) take down notice. Subsection (a), by contrast, contains no such take down provision. As a result, a subpoena sought under subsection (h), which is conditioned on a proper (c)(3)(A) notice, cannot logically apply in the subsection (a) context.

The language of subsection (c)(3)(A) also establishes that Section 512(h) subpoenas are only available when allegedly infringing content is stored on an ISP's system. Subsection (c)(3)(A) requires a take down notice to contain "information reasonably sufficient to permit the service provider to *locate* the material." 17 U.S.C. § 512(c)(3)(A)(iii) (emphasis added). "The goal of this provision is to provide the service provider with adequate information to *find* and *examine* the allegedly infringing material expeditiously." H. Rep. No. 105-551, at 55 (emphasis added). This provision, thus, presumes the ability of the ISP to *locate*, *find* and *examine* the allegedly infringing material so that it can remove or disable access to it. In the subsection (a) conduit context, such as here, those tasks are impossible. UNC cannot *locate* or *find*, let alone *examine*, information stored on a student's personal computer over which it has no control.

The availability of Section 512(h) subpoenas in the subsection (a) context was addressed by a district court in the District of Columbia. *In re Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24 (D.D.C. 2003) ("*Verizon I*"), *appeal pending*, No. 03-7015 (D.C. Cir. argued Sep. 16, 2003). That court found, in part, that limiting the DMCA's subpoena power to the subsection (c) context would "create a huge loophole in Congress's effort to prevent copyright infringement on the internet." *Id.* at 31. If so, the "loophole" was created by Congress, and should be honored by this Court. *See Sony Corp. v. Universal City Studios*, 464 U.S. 417, 431, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984) ("Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials.").

II. THE SUBPOENA IS INVALID BECAUSE IT IS PROCEDURALLY DEFICIENT.

Even if Section 512(h) does authorize this subpoena, the subpoena should still be quashed because it is procedurally deficient. First, the subpoena fails to identify the copyright owner(s) on whose behalf the subpoena is sought. Section 512(h) states that only a "copyright owner or a person authorized to act on the owner's behalf" may obtain a subpoena. Absent any indication of who the copyright owner is, it is impossible to determine if this requirement has been met.

Second, the subpoena is overbroad because it improperly requests John Doe's email address. Section 512(h)(3) states that a subpoena can only require production of "information sufficient to identify the alleged infringer." A name and address are clearly sufficient to identify John Doe. Indeed, most email addresses contain little, if any, identifying information.

III. THE SUBPOENA IS INVALID BECAUSE IT VIOLATES ARTICLE III'S MANDATE THAT COURTS MAY ACT, AND JUDICIAL PROCESS MAY BE OBTAINED, ONLY IN PENDING CASES OR CONTROVERSIES.

Article III of the Constitution limits the exercise of judicial power to "cases" or "controversies." U.S. Const., Article III, § 2. The case or controversy requirement of Article III has been zealously guarded since the earliest days of our country. *See, e.g., Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *Muskrat v. United States*, 219 U.S. 346, 353-63, 31 S.Ct. 250, 55 L. Ed. 246 (1911); *United States v. Morton Salt*, 338 U.S. 632, 641-42, 70 S.Ct. 357, 94 L.Ed. 401 (1950). Where, as here, there is no case or controversy, a federal court cannot take any judicial

action, except dismissal of the proceeding. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94, 718 S.Ct. 2199, L.Ed.2d 874 (1998); *Ex parte McCardle*, 74 U.S. (7 Wall.) 506, 514, (1868). Section 512(h), which purports to authorize issuance of a judicial subpoena absent a pending case and with no requirement that a future case be contemplated, is in violation of Article III.

Issuance and enforcement of a subpoena does not fall outside the strictures of Article III. A subpoena is a form of judicial process. *See, e.g.*, Black's Law Dictionary 1426 (6th ed. 1990) (a "subpoena duces tecum" is a "court process"); 9 Charles A. Wright, et al., *Federal Practice and Procedure* § 2451 (1971). As a result, "[t]he judicial subpoena power not only is subject to specific constitutional limitations . . . but also is subject to those limitations inherent in the body that issues them because of the provisions of the Judiciary Article of the Constitution." *Morton Salt*, 338 U.S. at 642. A court can, thus, only issue a subpoena when it has jurisdiction over an existing matter. *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76, 108 S.Ct. 2268, 101 L.Ed.2d. 69 (1988) ("if a district court does not have subject matter jurisdiction over the underlying action, and the [subpoena] process was not issued in aid of determining that jurisdiction, then the process is void and an order of civil contempt based on refusal to honor it must be reversed") (citation omitted).

This Article III issue was considered by the same D.C. district court judge in a second decision, *In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d 244 (D.D.C. 2003), *appeal pending*, No. 03-7053 (D.C. Cir. argued Sep. 16, 2003) ("*Verizon II*"). The *Verizon II* court asserted that Article III is not triggered because the clerk issuing a Section 512(h) subpoena performs a "quintessentially ministerial act" that is not an "act of 'the court.'" *Id.* at 249. Issuance of a judicial subpoena, however, is an exercise of judicial power. *See, e.g., In re Simon*, 297 F. 942, 944 (2d Cir. 1924) ("The fact that a writ of subpoena is actually signed in writing by the clerk of the court . . . makes it none the less the court's order."); *see also Fisher v. Marubeni Cotton Corp.*, 526 F.2d 1338, 1340 (8th Cir. 1975) ("A subpoena is a lawfully issued mandate of the court issued by the clerk thereof."). Were it otherwise, a court clerk could perform a function when a judge (without jurisdiction) could not. *See, e.g., Lloyd v. Lawrence*, 60 F.R.D. 116, 118

(S.D. Tex. 1973) ("Obviously, the Clerk may not take action which the Court itself may not take."). In addition, the subpoena is issued in the name of the district court and carries with it the enforcement authority of the court.

The Supreme Court has repeatedly rejected attempts by the legislative and executive branches to relax Article III's case or controversy requirement. *See, e.g., United Food Commercial Workers Union Local 751 v. Brown Group, Inc.*, 517 U.S. 544, 551, 116 S.Ct. 1529, 134 L.Ed.2d 758 (1996) (requirement of Article III standing is "absolute" and not "malleable by Congress"); *Morton Salt*, 338 U.S. at 641-42 ("Federal judicial power itself extends only to adjudication of cases and controversies and it is natural that its investigative powers should be jealously confined to these ends."). Any attempt to require court clerks to perform judicial duties in the absence of a case or controversy should likewise be rejected. *See Lloyd*, 60 F.R.D. at 118.

The *Verizon II* court also attempted to avoid the strictures of Article III by relying on Federal Rule of Civil Procedure 27, which authorizes the taking of depositions before litigation is commenced to preserve testimony necessary to an imminent lawsuit. Rule 27 is far different from Section 512(h). First, a party requesting discovery under Rule 27 must file a verified petition stating that it expects to bring a lawsuit in federal court relating to the requested discovery, but that it is presently unable to do so. Fed. R. Civ. Proc. 27(a)(1). Section 512(h) does not even require a subpoenaing party to assert that it is *contemplating* the filing of a lawsuit, let alone to *confirm* that it will file such a lawsuit when possible. Indeed, RIAA, which does not own the copyrights at issue, could not make such a promise because it has no standing to bring a lawsuit. *See* 17 U.S.C. § 501(b) (infringement action can only be brought by copyright owner).

Second, unlike Section 512(h), Rule 27 can only be used in limited circumstances: when necessary to perpetuate testimony that will otherwise be lost. Fed. R. Civ. Proc. 27(a)(1), (a)(3).

Third, Rule 27 requires notice to be provided, an evidentiary showing to be made, and, of critical importance, a pre-discovery hearing before a judge to determine if the discovery should be permitted. A Rule 27 request is, in other words, a "suit" for the perpetuation of testimony, with all elements of the promised claim specified in the petition. *See Arizona v. California*, 292

U.S. 341, 347, 54 S.Ct. 735, 78 L.Ed. 1298 (1934) ("The sole purpose of such a [Rule 27] suit is to perpetuate the testimony."). As discussed below, Section 512(h) subpoenas, by contrast, are issued on an *ex parte* basis, with no requirement of notice, no requirement that any evidentiary showing or specification of claim be made, and no judicial determination.[8]

IV. SECTION 512(H) VIOLATES THE DUE PROCESS CLAUSE BECAUSE IT DOES NOT CONTAIN ADEQUATE PROCEDURAL PROTECTIONS AGAINST THE CURTAILMENT OF CONSTITUTIONALLY PROTECTED EXPRESSION.

The Fifth Amendment requires adequate procedural protections before a person can be deprived of liberty to ensure that fundamental rights are not unnecessarily curtailed. *Mathews v. Eldridge*, 424 U.S. 319, 332, 96 S.Ct. 893, 47 L.Ed.2d 18 (1976). Sufficient safeguards are especially critical where, as here, the liberty interest is the freedom of speech guaranteed by the First Amendment. *See, e.g.*, *Blount v. Rizzi*, 400 U.S. 410, 416, 91 S.Ct. 423, 27 L.Ed.2d 498 (1971) ("Government 'is not free to adopt whatever procedures it pleases for dealing with [illicit content] without regard to the possible consequences for constitutionally protected speech'") (citation omitted); *NAACP v. Alabama*, 357 U.S. 449, 460-61, 78 S.Ct. 1163, 2 L.Ed.2d (1958). Heightened protections are necessary because "the line between speech unconditionally guaranteed and speech which may legitimately be regulated, suppressed, or punished is finely drawn." *Speiser v. Randall*, 357 U.S. 513, 525, 78 S.Ct. 1332, 2 L.Ed.2d 1460 (1958).

As detailed earlier, Section 512(h) permits an alleged copyright holder to obtain an Internet speaker's identity without providing anything more than a self-serving assertion of "good faith." The following factors should be examined to determine if these "protections" of Section 512(h) are sufficient to pass constitutional scrutiny: (1) the private interest affected by enforcement of the law; (2) the risk of erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional safeguards; (3) the government's

[8] The *Verizon II* court also erroneously suggested that Section 512(h) subpoenas are similar to subpoenas authorized by a few other federal statutes. *Verizon II*, 257 F. Supp. 2d at 251-52. None of those statutes, like Section 512(h), authorizes the issuance and enforcement of judicial subpoenas to private parties merely seeking to gather information unrelated to a pending or promised federal lawsuit. Nor do those statutes authorize issuance of subpoenas without judicial review or a judicial determination.

interest; and (4) the interest of the private party seeking to bring about the deprivation. *Mathews*, 424 U.S. at 335; *see also Connecticut v. Doehr*, 501 U.S. 1, 11, 111 S.Ct. 2105, 115 L.Ed.2d 1 (1991). These factors demonstrate that Section 512(h) falls far short of the procedural protections required by the Due Process Clause.

A. Internet Users Have A Substantial And Constitutionally Protected Liberty Interest In Privacy And Anonymous Expression.

Freedom of speech is one of the liberty interests protected by the Due Process Clause. *See, e.g., Procunier v. Martinez*, 416 U.S. 396, 418, 94 S.Ct. 1800, 40 L.Ed.2d 224 (1974), *overruled on other grounds by Thornburgh v. Abbott*, 490 U.S. 401, 109 S.Ct. 1874, 104 L.Ed.2d 459 (1989); *NAACP*, 357 U.S. at 460.

It is well-established that the First Amendment protects the right to anonymity. *See, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995) ("anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent"). This right to anonymity is more than just a form of protected speech; it is part of "our national heritage and tradition." *Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166, 122 S.Ct. 2080, 153 L.Ed.2d 205 (2002).

The Supreme Court has explained the importance of the right to anonymity:

> Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.

McIntyre, 514 U.S. at 357 (citations omitted).

This long-standing right to anonymity is especially critical to a thoroughly modern medium of expression: the Internet. The rise of the Internet has created an opportunity for dialogue and expression on a scale and in a manner previously unimaginable. *See Reno v. ACLU*, 521 U.S. 844, 870, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997) (noting that the Internet is a

new and powerful democratic forum in which anyone can become a "pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox").

The unique nature of the Internet makes the right to speak on the Internet anonymously especially important. Unlike traditional media speakers, Internet speakers typically do not have professional training to evaluate the nuances of copyright law as it might affect the information they post, editors to peruse their posts for problems, or lawyers to advise them of the complexities of the laws possibly implicated by their statements. Faced with the threat of having to defend against costly litigation arising out of an erroneously or maliciously issued – but easily obtained – Section 512(h) subpoena, many legitimate users may simply decide that using the Internet as a forum for their communications is not worth the risk. In addition, for many online speakers, such as critics of a company, the protection of anonymity is essential to their willingness to speak. *See, e.g., Doe v. 2theMart.com,* 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously.").

Recognizing the speech-enhancing and equalizing features of the Internet, the Supreme Court has accorded it the highest degree of constitutional protection. *Reno,* 521 U.S. at 870 (concluding that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium"). This rigorous protection extends to speech conducted anonymously on the Internet. *See, e.g., 2theMart.com,* 140 F. Supp. 2d at 1093 ("the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded"); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (recognizing the "legitimate and valuable right to participate in online forums anonymously or pseudonymously").[9]

Several courts that have considered similar discovery requests to uncover the identity of anonymous Internet speakers have recognized the substantial interest in maintaining online

[9] *See also ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D. N.M. 1998), *aff'd* 194 F.3d 1149 (10th Cir. 1999) (striking down law "that prevents people from communicating and accessing information anonymously"); *ACLU v. Miller,* 977 F. Supp. 1228 (N.D. Ga. 1997) (striking down law prohibiting anonymous Internet speech).

anonymity. In *Columbia Insurance Company v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999), a subpoena sought the identity of the defendant, an alleged trademark infringer. The court ruled that the party seeking the subpoena needed to satisfy certain standards of proof at a pre-disclosure hearing, explaining that:

> This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.

Id. at 578. The court in *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001), reached a similar conclusion: "If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment Rights." *See also Dendrite, Int'l, Inc. v. Doe No. 3,* 775 A.2d 756, 771 (N.J. Super. A.D. 2001) (strict procedural safeguards must be imposed "as a means of ensuring that plaintiffs do not use discovery procedures to ascertain the identities of unknown defendants in order to harass, intimidate or silence critics in the public forum opportunities presented by the Internet").

In spite of these cases, the *Verizon II* court concluded that the anonymous online speakers in that case had only a minimal right to anonymity because the speech at issue was "alleged copyright infringement." *Verizon II*, 257 F. Supp. 2d at 260. The fundamental flaw in the *Verizon II* court's analysis is that at the time a Section 512(h) subpoena is issued – *i.e.*, when the right to anonymity will be lost – no determination has yet been made as to whether the anonymous speech at issue is protected or not. The First Amendment does not protect speech constituting proven copyright infringement, just as it does not shelter obscene or libelous speech. The First Amendment does, however, provide full protection to speech allegedly constituting copyright infringement, just as it protects allegedly obscene or libelous speech. *See*, *e.g.*, *New York Times Co. v. Sullivan*, 376 U.S. 254, 268-69, 84 S.Ct. 710, L.Ed.2d 686 (1964) ("Like insurrection, contempt, advocacy of unlawful acts, breach of the peace, obscenity, solicitation of

legal business, and the various other formulae for the repression of expression that have been challenged in this Court, libel can claim no talismanic immunity from constitutional limitations."); *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58, 66, 83 S.Ct. 631, 9 L.Ed.2d 584 (1963). That is why, as discussed below, procedural safeguards must be put in place to ensure that legitimate expression is not suppressed merely because it may not be protected speech.

B. The Minimal Procedural Protections of Section 512(h) Give Rise To A Substantial Risk of Erroneous Deprivation Of Constitutional Rights That Could Be Diminished By the Use of Adequate Procedural Safeguards.

Section 512(h) was designed to provide an expeditious way for copyright holders to protect their works in the digital age. That goal is legitimate, and understandable. The failure of the statute to provide even the most minimal procedural safeguards, however, creates an invitation to mistake and misuse. As detailed earlier, numerous examples of both erroneous and abusive use of Section 512(h) have already been reported. *See supra*, pp. 3-5.

The substantial risk of mistake and misuse exists because Section 512(h) requires little more than an *ex parte* assertion of "good faith." In *Connecticut v. Doehr,* 501 U.S. 1, 111 S.Ct. 2105, 115 L.Ed.2d 1 (1991), the Supreme Court invalidated a Connecticut statute authorizing pre-judgment attachment of real estate based, as here, solely on the submission of a "good faith" affidavit and without any showing of extraordinary circumstances. The Court held that the statute violated due process because it permitted an *ex parte* attachment without affording the property owner prior notice or an opportunity to be heard and thus created "too great a risk of erroneous deprivation." *Id.* at 13-14. Similarly, in *Fuentes v. Shevin*, 407 U.S. 67, 92 S.Ct. 1983, L.Ed.2d 556 (1972), the Court also found that an individual's self-interested statement of "belief in his [own] rights" was insufficient to satisfy the requirements of due process. *Id*. at 83. Section 512(h)'s "good faith" requirement is likewise not sufficient.

Recognizing the need to protect the right to anonymity, several courts that have been faced with discovery requests seeking to uncover the identity of online speakers have imposed strict procedural safeguards before permitting the right to anonymity to be overridden. *See*

Seescandy, 185 F.R.D. at 578-80 (procedural safeguards, including an attempt to notify the anonymous speaker and a showing to "establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss," must be imposed to "prevent use of [civil discovery mechanisms] to harass or intimidate" anonymous Internet speakers); *In re Subpoena Duces Tecum to America Online, Inc.*, 2000 WL 1210372, *8 (Va. Cir. Ct. 2000), *rev'd on other grounds sub nom. American Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001) ("before a court abridges the First Amendment right of a person to communicate anonymously on the Internet, a showing, sufficient to enable that court to determine that a true, rather than perceived, cause of action may exist, must be made"); *Dendrite*, 775 A.2d at 760-61 (requiring notice, identification of the precise statements alleged to be infringing, production of evidence to the Court sufficient to demonstrate each element of the cause of action and a judicial determination as to whether the need for the identity outweighs the right to anonymity); *2themart.com,* 140 F. Supp. 2d at 1095 (judicial determination must be made, based on evidence produced by subpoenaing party, that, *inter alia*, information sought is materially relevant to claim). Those cases all involved subpoenas issued in the context of a pending lawsuit. In the context of a Section 512(h) subpoena, where no lawsuit has been filed and no lawsuit need even be contemplated by the subpoenaing party, the necessity of procedural safeguards is even more paramount.

Adequate procedural protections would minimize the possibility of mistake and misuse of Section 512(h); their absence renders Section 512(h) in violation of the Due Process Clause. First, notice must be given to the anonymous user that the subpoenaing party is seeking its identity. Section 512(h)'s failure to require this notice is a violation of a basic, yet critical, due process protection. *See, e.g.*, *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314, 70 S.Ct. 652, 94 L.Ed. 865 (1950) ("An elementary and fundamental requirement of due process . . . is notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.").

Second, the anonymous Internet user must be given an opportunity to challenge the request to disclose his or her identity. *See, e.g.*, *Mathews*, 424 U.S. at 333 ("The fundamental requirement of due process is the opportunity to be heard 'at a meaningful time and in a meaningful manner.'") (citation omitted); *see also* Fed. R. Civ. Proc. 26(d), 26(f) (discovery not permitted absent court order until after service of the complaint).

Third, a complaint or other pleading must be filed that identifies with specificity and with factual support the nature of the infringement, the identity of the copyright holder, and each item alleged to be infringing. *See Seescandy*, 185 F.R.D. at 579-80; *Dendrite*, 775 A.2d at 760. Without these basic details, an Internet user has no real notice of the claims and no real opportunity to challenge the subpoena or defend his or her rights. *Mathews*, 424 U.S. at 333.

Finally, a judge must make a determination as to whether the pleading and evidence presented establishes a *prima facie* claim for infringement that justifies stripping the speaker's anonymity. *Seescandy*, 185 F.R.D. at 579-80; *In re Subpoena to America Online*, 2000 WL 1210372, *8; *Dendrite*, 775 A.2d at 760-61; *2themart.com*, 140 F. Supp. 2d at 1095. Absent such a showing, there is no compelling reason to overcome the fundamental right to anonymity.

The *Verizon II* court declined to require any such procedural safeguards.[10] Instead, that court concluded that procedural safeguards were not necessary because (1) the subpoenaing party has to assert that it has a "good faith belief" that an unauthorized use has occurred, (2) the declaration accompanying the subpoena must be submitted under penalty of perjury, (3) Section 512(f) provides a remedy against issuance of erroneous subpoenas, and (4) the Rules of Civil Procedure can be used to object to a subpoena. *Verizon II*, 257 F. Supp. 2d at 262-63. These "safeguards" hardly provide sufficient constitutional protection.

First, as just discussed, a subpoenaing party's assertion that it has a "good faith" claim is not sufficient to satisfy due process standards. *Fuentes*, 407 U.S. at 83.

Second, a subpoenaing party need only state under oath that its purpose is to use the

[10] The *Verizon II* court addressed the adequacy of procedural safeguards in considering whether Section 512(h) violates the First Amendment. That court did not address or render a decision on the issue presented in this motion: whether Section 512(h)'s procedural safeguards satisfy the Fifth Amendment requirements of due process.

information to protect copyrighted material; it need not swear that copyright infringement has occurred. *See* 17 U.S.C. § 512(h)(2)(C). Indeed, there is not even a requirement that the subpoenaing party conduct any due diligence, such as actual review of the suspicious files, to determine if the files are truly improper or if their use is protected by the fair use doctrine.

Third, the loss of anonymity created by an improperly obtained subpoena is exactly the type of irreparable damage that a subsequent recovery of monetary damages under Section 512(f) cannot cure. *See Rancho Publications v. Superior Court*, 68 Cal.App.4th 1538, 1541 (Cal. App. 1999) ("anonymity, once lost, cannot be regained"); *see also Elrod v. Burns*, 427 U.S. 347, 373-74, 96 S.Ct. 2673, 49 L.Ed.2d 547 (1976) ("The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable harm"). In addition, Section 512(f) only applies when the subpoenaing party "knowingly materially misrepresents" that infringement has occurred. 17 U.S.C. § 512(f). Where, as in the mistaken lawsuits discussed earlier, the subpoenaing party simply fails to conduct any due diligence or to consider whether the speech is protected by the fair use doctrine, Section 512(f) may provide no remedy.

Finally, the Federal Rules are of little value to an anonymous speaker where, as under Section 512(h), there is no requirement that the speaker receive any notice or an opportunity to challenge the subpoena. Although ISPs have the ability to provide such notice to their subscribers, there is no guarantee (or requirement) that they will do so – especially given the multitude of subpoenas RIAA has been serving and the incredibly short time frame for compliance. Without a notice requirement, the theoretical ability to challenge a Section 512(h) subpoena is meaningless.[11]

C. The Legitimate Interests Of the Government and Copyright Holders Will Not Be Substantially Affected By The Use of Adequate Protections.

The government – like copyright holders – has a strong interest in ensuring that copyright

[11] That UNC – the ISP here – chose to provide such notice to John Doe in this case does not mean that other ISPs, or even UNC, will do so in the future. In addition, an ISP will not always challenge the subpoena on behalf of its subscriber or raise all of the arguments that would be brought by the subscriber, particularly because the ISP may not have access to all of the relevant facts. Indeed, UNC has chosen not to challenge this subpoena.

owners can protect against infringement of their works. The government also has a substantial interest in ensuring that its laws are not used to suppress the speech and privacy rights of anonymous Internet users, and that the discovery processes of the courts are not abused. The additional procedural protections strike an appropriate balance between these interests, ensuring that each will be furthered. If a proper showing is made, a copyright holder will be entitled – and should be entitled – to learn the identity of the anonymous speaker. Absent such a showing, to guard against the potentially erroneous disclosure of identity and to preserve a vital constitutional right, the subpoena should be rejected.

Requiring these procedural protections – protections required in all other civil contexts where anonymity is at stake – would be no more onerous than the rules applicable to all other legal claims. Claims of copyright infringement should be treated no differently – especially in view of the constitutional rights at stake.

CONCLUSION

For the foregoing reasons, the subpoena served by RIAA should be quashed.

Respectfully submitted, this the ____ day of November, 2003.

_____
SETH JAFFE,
N.C. Bar Number 27261
American Civil Liberties Union of
North Carolina Legal Foundation
P.O. Box 28004
Raleigh, NC 27611
(919) 834-3466

CHRISTOPHER A. HANSEN
ADEN J. FINE,
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500

CERTIFICATE OF SERVICE

I certify that I have served the foregoing **MEMORANDUM OF POINTS OF AUTHORITIES IN SUPPORT OF JOHN DOE'S MOTION TO QUASH** on the parties' counsel by placing a copy thereof enclosed in a first-class, postage-prepaid, properly-addressed wrapper in a post office or official depository under the exclusive care and custody of the United States Postal Service, addressed to:

Mr. Mark Prak, Esq.
Brooks Pierce McLendon Humphrey & Leonard
Wachovia Capitol Center, Suite 1600
150 Fayetteville Street Mall
Raleigh, N.C. 27601

Mr. David Parker, Esq.
Campus Box 9105
Suite 300B, Bank of America Building
137 East Franklin Street
Chapel Hill, N.C. 27599-9105

This, the 21st day of November 2003.

_____
SETH JAFFE