UNITED STATES DISTRICT COURT

IN RE:

SUBPOENA ENFORCEMENT MATTER

CV No. 0000000000000

MOTION TO QUASH SUBPOENA SERVED PURSUANT TO 17 U.S.C. § 512(H)

Pursuant to 17 U.S.C. § 512, Fed. R. Civ. P. 45, and Article III of, and the First and Fifth Amendments to, the U.S. Constitution, ABC Corporation ("ABC") hereby moves this Court to quash the subpoena served on it by XYZ Corporation ("XYZ"). As explained more fully in ABC's accompanying memorandum filed in conjunction with this motion, this blunderbuss subpoena seeks the names, addresses, telephone numbers, and email addresses of subscribers to ABC's Internet access services based upon XYZ's bald assertion that these subscribers have offered copyrighted material over the Internet. The threat to personal privacy, personal security, reputation, and freedom of expression and association on the Internet posed by this subpoena is obvious. Because this subpoena is issued in violation of both the Copyright Act and the Constitution, it must be quashed.

Respectfully submitted,

By:_____

Counsel for Movant
ABC Corporation

Dated: _____

UNITED STATES DISTRICT COURT

IN RE: **SUBPOENA ENFORCEMENT MATTER**	CV No. 0000000000000

MEMORANDUM OF POINTS AND AUTHORITIIES IN SUPPORT OF MOTION TO QUASH SUBPOENA SERVED PURSUANT TO 17 U.S.C. § 512(H)

Counsel for Movant
ABC Corporation

Date: _____

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

XYZ Corporation ("XYZ") seeks the names, addresses, telephone numbers, and email addresses of subscribers of ABC Corporation ("ABC"). XYZ claims that these Internet users employed peer-to-peer software to offer its allegedly copyrighted material over the Internet from their personal computers. No infringement lawsuit has been filed against these individuals, and the sole basis for issuance of the subpoena is XYZ's bald assertion that it has a "good faith" belief that its copyrights may have been infringed. XYZ apparently believes that its subpoena is authorized by the Digital Millenium Copyright Act ("DMCA") and that ABC must "expeditiously" turn over this confidential information without any substantive or procedural safeguards. ABC hereby moves to quash this subpoena on the grounds that:

- The subpoena is not authorized by the DMCA because the subpoena power contained in 17 U.S.C. § 512(h) is limited to instances where the Internet service provider ("ISP") hosts potentially infringing material on its own network (such as a website). It certainly does not extend to companies like ABC when they are serving as a passive conduit for communications over the Internet. Extension of the subpoena power to material residing on the personal computers of the over 100 million Internet users is contrary to the text, structure, and purpose of this statute.

- The issuance and enforcement of a third-party subpoena outside of any pending case or controversy violates Article III of the Constitution. Supreme Court and other precedent compel the conclusion that compulsory process can only be used in the resolution of a pending case or controversy. *See Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *United States v. Morton Salt Co.*, 338 U.S. 632 (1950); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999).

- The minimal filings required to obtain the subpoena, the lack of notice to the subscriber, and the impermissible shifting of the burden to the ISP to defend presumptively protected speech violate the First Amendment. *See Blount v. Rizzi*, 400 U.S. 410 (1971); *Columbia Ins.*, 185 F.R.D. 573.

- The subpoena provision as applied fails to satisfy the minimum procedural requirements of the Fifth Amendment before depriving Internet users of their liberty interest and ISP's of their property interest in their subscriber lists. *See Connecticut v. Doehr*, 501 U.S. 1 (1991).

- This subpoena is improper in any event, as it bundles multiple subscribers into one subpoena, makes no provision for compensation of ABC, offers no protection for the proprietary data that it purports to require ABC to produce, and fails to comply with the "sworn declaration" requirement of Section 512(h)(2)(C).

The particular subpoena at issue here highlights the harm to privacy and free expression that will result from an unwarranted expansion of Section 512(h).

STATEMENT OF FACTS

Movant ABC is a leading provider of Internet access services. XYZ claims to be the owner of certain copyrighted material. XYZ served a subpoena on ABC demanding that it identify – by name, address, phone number, and email address – numerous subscribers at unique listed Internet Protocol ("IP") addresses at particular dates and times[1] that were assertedly involved in using copyrighted materials without authorization. XYZ's notices accompanying the subpoena only assert a "good faith belief" that the claim is accurate. The notices do not state what, if any, type of inquiry was made to substantiate this "belief." Also, XYZ does not assert that it owns the alleged copyrights but rather that it is the owner's agent. Nor does the statute at issue require proof that the works at issue were registered – a precondition to filing an infringement action.

Moreover, the notices accompanying the subpoena erroneously assert that ABC subscribers were using "peer-to-peer" applications – *i.e.*, software that allows multiple users to exchange files residing on their personal computers directly with those on the personal computers of others. ABC performed a mere transmission or conduit function for these communications; it does not monitor or maintain any control over its subscribers' email, web browsing, or file-sharing. None of this material is hosted by ABC or resides on its network.

LEGAL BACKGROUND—The Digital Millennium Copyright Act of 1998 ("DMCA")

The 1998 DMCA amended the Copyright Act; it sought to balance copyright owners' interests in protecting their rights with the need to protect and foster the Internet as an important medium of free expression. Title I of the DMCA provided new rights to copyright holders that empowered them to prevent the circumvention of technological "self-help" measures used to protect their copyrights. *See* 17 U.S.C. §§ 1201-1205. Self help was to be copyright owners'

---

[1] Whenever a user is connected to the Internet, the ISP assigns the user a numerical "address." This IP address is not necessarily associated with the user's name and real address, allowing users to browse web sites, read email, and post speech to chat rooms anonymously. Many copyright owners now use electronic robots or "bots" to search the Internet for words or other snippets suggesting the presence of copyrighted material. When they identify such material, they use software to associate the material with an IP address, which they can then use to identify the ISP.

principal new remedy. Title II of the DMCA codified immunities for ISPs, which turn upon the particular role they play in the handling, storage, and dissemination of Internet content. 17 U.S.C. § 512.[2] In both titles, Congress recognized the substantial interest in protecting the privacy and freedom of expression of the over 100 million Internet users in this country. *See, e.g., id.* §§ 512(m), 1205; *see also* S. Rep. No. 105-190, at 18 (1998) ("[T]he committee concluded that it was prudent to rule out any scenario in which section 1201 might be relied upon to make it harder, rather than easier, to protect personal privacy on the Internet.").

Title II drew a sharp distinction between (a) the ISP acting as a passive conduit for communications created, controlled, and stored by others and (b) the ISP "hosting" information on its own network or systems. *Compare* 17 U.S.C. § 512(a) *with id.* § 512(c). The DMCA thus makes clear that ISPs enjoy the same immunities that have traditionally applied to entities that provide a pure "transmission" or "conduit" function. *E.g., E. Microwave, Inc. v. Doubleday Sports, Inc.*, 691 F.2d 125, 128 (2d Cir. 1982). Consistent with this recognition, Section 512(a) *does not impose any specific duties* on ISPs serving as a conduit for transmitting others' content.

By contrast, subsections (b), (c), and (d) of Section 512 impose limited duties to assist copyright owners in protecting their property interests where the ISP has some access to, or control over, the particular material claimed to be infringing. These duties are carefully calibrated depending upon the ISP's involvement with, and control over, the material at issue. Thus, in stark contrast to subsection (a) – which governs ABC's conduct in this case – subsection (c) provides that where a user stores content on the service provider's systems or network (*e.g.*, the provider "hosts" a website) it must respond to a specifically defined "take down" notice that the material is infringing. *Id.* § 512(c)(1)(C).

Title II of the DMCA also contains the unique subpoena provision, codified in Section 512(h), which is at issue here. This provision was designed to require an ISP to identify the owner of particular content stored on the provider's network that is claimed to be infringing in a

[2] A copy of 17 U.S.C. § 512 is attached as an addendum to this memorandum for the convenience of the Court.

valid "take down" notice as provided in subsection (c). *See id.* § 512(h)(4) (take down notice must "satisf[y] the provisions of subsection (c)(3)(A)" for any subpoena to issue). The limitation of this unique subpoena power to the subsection (c) context makes perfect sense in light of the service provider's ability to examine and control the content stored on its own systems and the fact that peer-to-peer file-swapping activity over broadband connections was not even contemplated when the DMCA was enacted in 1998. It also reflects the difference between burdening ISPs with the role of "copyright policeman," requiring them to invade the privacy of their subscribers, and requiring ISPs to exercise narrowly targeted, content-specific functions for material resident on their own facilities.

ARGUMENT

I. THE NOVEL SECTION 512(h) SUBPOENA POWER APPLIES ONLY TO MATERIAL RESIDING ON AN ISP'S SYSTEM OR NETWORK.

XYZ asks this Court to stretch subsection (h) to reach a problem that did not exist when the law was passed, with dire consequences for Internet functions, such as email and web browsing, that Congress viewed as private and with which it did not wish to interfere. Such a result would violate the Supreme Court's warning that courts should leave for Congress the task of fashioning responses to new technology in the area of copyright law. *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 430-31 (1984) ("Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology."). Peer-to-peer technology did not exist when the DMCA was enacted, and Congress did not have the opportunity to address regulation of that technology or its effect on the rights of ISPs, Internet users, and copyright owners.[3]

[3] *See* David Barkai, *An Introduction to Peer-to-Peer Computing*, Intel Developer Update Magazine, Oct. 2000, at 3, http://cnscenter.future.co.kr/resource/hot-topic/p2p/it02012.pdf) (describing P2P as "a revolution underway that represents a new computing model for the Internet," and contrasting it to "the traditional client/server architecture" in which "the client makes requests of the server with which it is networked").

A. The Text and Structure of Section 512 Compel the Conclusion that Subsection (h) Applies Only to Material Stored on an ISP's System.

A court must make every attempt to interpret a statute "'as a symmetrical and coherent regulatory scheme'" and "'fit, if possible, all parts into an harmonious whole.'" *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (citations omitted)). Section 512 involves a careful calibration of ISP involvement with content on the one hand, and ISP duties in relation to that content, on the other hand. Section 512(n) contains an express rule of construction, directing courts that "[s]ubsections (a), (b), (c) and (d) describe separate and distinct functions for purposes of applying this section." This careful calibration extends to the subpoena provision, which is closely tied to one specific ISP function – storage or hosting addressed in subsection (c).

Subsection (a) addresses the situation where the ISP performs a pure transmission or "conduit" function between its subscribers and myriad opportunities for cultural, commercial, and personal exchange available on the Internet. It includes email, web browsing, and, more recently, peer-to-peer functions, where the user selects the content and destination of the communication. Traditionally, this conduit role for expression of others, such as that performed by a telephone company, has not created any duties or liabilities under the copyright laws.

At the other end of the spectrum is subsection (c), which deals with material residing on the ISP's server at the request of its customer. *See Columbia Ins. Co. v. SeesCandy.com*, 185 F.R.D. 573, 578 n.1 (N.D. Cal. 1999) (drawing distinction between pure "access services" and "domain hosting," where the subscriber maintains material on the ISP's server). In this frequently commercial setting, the ISP is "hosting" an online site on its own servers. Here, Section 512 imposes greater duties on the ISP in exchange for limited immunity, including a duty to "remove" or "disable access to" infringing material upon receiving a valid take-down notice as specified in subsection (c)(3)(A) of the statute.[4] The statute also provides for damages

[4] Under Section 512(g), if a take-down notice is issued to the ISP, the owner of the website receives notice of the allegation of copyright infringement and an opportunity to dispute the issue. The ISP must then reinstate access to the website unless the copyright owner files a lawsuit seeking to enjoin the website owner under the copyright laws. 17 U.S.C. § 512(g)(2)(B).

to be awarded for misrepresentations in a take-down notice that causes the improper removal of the material. *Id.* § 512(f).[5]

Section 512(h), the subpoena provision that is at issue here, contains three separate cross-references to the take-down notice prescribed by subsection (c)(3)(A). In turn, subsection (c)(3)(A) applies exclusively to the particular functions addressed in subsection (c) of the statute. In particular, Section 512(h)(4), entitled "Basis for Granting Subpoena," provides:

> If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

This provision sets up a series of separate statutory *conditions precedent* to the issuance of any subpoena under Section 512(h). A take-down notice drafted and issued in the subsection (a) context cannot, as a matter of law, "satisf[y] the provisions of subsection (c)(3)(A)." The provisions of subsection (c)(3)(A) apply only in the context of subsection (c). *Id.* § 512(c)(3)(A) (providing criteria that must be satisfied for the notification "[t]o be effective under this *subsection*," *i.e.*, subsection (c)). Similarly, the statute requires that a notice described in subsection (c)(3)(A) be filed in requesting the subpoena, *id.* § 512(h)(2)(A), and that a copy of the subsection (c) notice be served with any subpoena, *id.* § 512(h)(5). These repeated references to the required take-down procedure in subsection (c)(3)(A) indicate that the subpoena provision was intended to operate only in the context of an effective take-down notice. Since conduit functions are not subject to take-down notices, and the statute makes no provision for

[5] Subsections (b) and (d) of the statute describe situations that lie between the two poles of the conduit functions described in subsection (a) and the hosting functions described in subsection (c). Subsection (b) applies to caching functions, where the service provider temporarily stores a duplicate of material found elsewhere on the Internet in order to facilitate efficient transmission of the material. Subsection (d) involves information location tools, such as hyperlinks, that might lead a subscriber from a service provider's home page or website to an infringing website. Subsections (b) and (d) provide for their own specific types of take-down notices, distinct from the notice prescribed by subsection (c)(3)(A). *See* 17 U.S.C. § 512(b)(2)(E); *id* § 512(d)(3). Unlike subsections (b), (c), and (d), subsection (a) of the statute, which applies to ABC in this case, does not contain *any* notice or "take-down" procedures.

such a notice in the subsection (a) context, subpoenas are not authorized in the subsection (a) context.

It is a well-established principle of statutory construction that a statutory cross-reference must be given effect, and where it places substantive or procedural limitations on the referring provision, those limitations are incorporated into the referring provision. *Estate of Joseph Leder v. Comm'r of Internal Revenue*, 893 F.2d 237, 241 (10th Cir. 1989) (noting the "only inference" that can be drawn from an "express cross reference" is that Congress meant for the two linked subsections to be interpreted "*in para materia*"); *Overseas Educ. Ass'n v. FLRA*, 824 F.2d 61, 65 (D.C. Cir. 1987) ("highly specific cross reference" must be read to limit scope of more general statutory provision). The three express cross-references in subsection (h) to an actual (c)(3)(A) notification make clear that that subsection applies only to the subsection (c) context.

Nor can the statutory requirements for the issuance of a Section 512(h) subpoena be coherently applied to the subsection (a) context. The substantive requirements of the notice provision in subsection (c)(3)(A) cannot be satisfied in the subsection (a) conduit context. For example, the notice can be "effective under this subsection" only if it contains "[i]dentification of the material that is claimed to be infringing ... and that is to be removed or access to which is to be disabled." 17 U.S.C. § 512(c)(3)(A)(iii). This requirement necessarily presumes the ability of the ISP to remove or disable access to material and thus requires *control* over the particular material at issue. ABC does not have such control over material stored on the personal computers of its millions of Internet access subscribers. *See* S. Rep. No. 105-190 at 50 (expressly tying use of terms "disabling access to" or "removing" material to subsection (c)(1) take-down duties). By contrast it does have control over material that resides on its own system or network and can selectively disable access to or remove material that is claimed to be infringing.

The notice also must contain "information reasonably sufficient to permit the service provider to locate the material." 17 U.S.C. § 512(c)(3)(A)(iii). "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). But this is simply impossible in the subsection (a) context. ABC cannot find, much less examine, material residing on personal computers or other third-party storage devices to examine a claim of infringement. Thus, a take-down notice drafted and issued in the subsection (a) context cannot, as a matter of law, be deemed to "satisf[y] the provisions of subsection (c)(3)(A)." Application of subsection (h) to conduit functions renders the cross-references to subsection (c)(3)(A) meaningless and requires the filing and service of a take-down notice that has no purpose or effect. This reading violates the cardinal rule of construction that no provision may be read to be without operation or effect. *Bennett v. Spear*, 520 U.S. 154, 173 (1997).

B. The Legislative History and Purpose of the Statute Support Limiting Section 512(h) Subpoenas to the Subsection (c) Context.

Peer-to-peer file sharing software, such as KaZaA, did not exist in 1998. The vast majority of Internet connections operated at speeds that precluded the uploading of large digital files, such as video files, from a home computer. The central concern when the DMCA was debated and enacted was infringement through online websites, hosted by ISPs, with the capacity to store and disseminate large amounts of data. The response was take-down duties and a subpoena provision limited to ISP-hosted "online sites." *See, e.g.*, H. Rep. No. 105-551, at 53 (referring to "wrongful activity that is occurring at the site on the provider's system or network at which the material resides" as an example of infringing activity at an "online site"); S. Rep. No. 105-190, at 44 (same).

The conduit functions Congress was aware of and referenced in the legislative history of the DMCA were email and web browsing. *See* H. Rep. No. 105-551 at 42 (referring to both "email" and "storage of a web page in the course of transmission to a specific user" as conduit functions). These subsection (a) functions were not seen as presenting infringement problems and, in fact, were viewed by Congress as qualitatively different from hosted websites in terms of

the privacy and free expression interests of Internet users. Congress embodied substantial protections for the privacy of Internet users in the DMCA, and it is incredible to *assume* that without the peer-to-peer issue before it, Congress wished to place a highly intrusive unsupervised subpoena power in private hands for every type of Internet communication.

C. The Scope of Section 512(h)'s Subpoena Power Presents an Issue of First Impression in this Court.

The issues raised herein, regarding the scope and constitutionality of Section 512(h) of the DMCA, are issues of first impression in this Court. Most of these issues are also currently the subject of an expedited appeal before the D.C. Circuit, *In re Verizon Internet Services, Inc.*, Nos. 03-7015 & 03-7053 (argument scheduled September 16, 2003). The D.C. Circuit will be reviewing decisions of a district court that held that subsection (h) does apply to conduit functions and is constitutional. *In re Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24 (*Verizon I*) & 257 F. Supp. 2d 244 (*Verizon II*) (D.D.C. 2003). *Verizon I*, which addressed the statutory interpretation issue, is wholly unpersuasive in its analysis of the statute and should not be followed by this Court. The *Verizon I* court ignored the explicit cross-references that limit the scope of Section 512(h) and instead focused on the generic definition of "service provider," 17 U.S.C. § 512(k)(1). 240 F. Supp. 2d at 30-32. But the term "service provider" is used throughout Section 512 in numerous provisions, like Section 512(h), that by context or cross-reference are limited to one or more of the particular functions described in subsections (a) through (d). *E.g.*, 17 U.S.C. §§ 512(b)-(g). The definition of "service provider" addresses the question of *who* is covered by the statute, but not the question of *what duties* they must undertake in the context of particular functions. As the Supreme Court has held, a statutory definition cannot be given controlling effect where the substantive provisions of the statute point to a different result. *Robinson v. Shell Oil Co.*, 519 U.S. 337, 343-44 (1997) ("[E]ach section must

be analyzed to determine whether the context gives the term a further meaning that would resolve the issue in dispute.").

Moreover, the *Verizon I* court failed to explain how the take-down notice required by subsection (c)(3)(A), which is an essential prerequisite for the issuance and service of a subpoena, could have any meaning in the context of subsection (a). 240 F. Supp. 2d at 33-34 & n.5. Even if the statute could be read to extend the subpoena power to any situation where a take-down notice is authorized (*i.e.* subsections (b), (c) & (d)), the *Verizon I* court clearly erred in extending the subpoena power to subsection (a), where no take-down notices or take-down duties are provided for and such notices cannot serve their statutory purpose. Based upon the sensitive and private nature of conduit functions, ISPs' lack of control over content when performing those functions, and ISPs' inability literally to "take-down" any material alleged to be infringing in the conduit context, Congress made a conscious decision to omit any take-down notices or duties from subsection (a). The omission must be given effect in applying Section 512(h), which depends upon the filing and service of take-down notices for its operation. *See United States v. Male Juvenile,* 280 F.3d 1008, 1015 (9th Cir. 2002) (citing *Russello v. United States,* 464 U.S. 16, 23 (1983)). This Court has the opportunity to correct these errors of statutory construction and to give Section 512(h) the more limited scope that the statutory language and structure command and that Congress clearly intended.

II. A JUDICIAL SUBPOENA CANNOT BE ISSUED OR ENFORCED OUTSIDE A PENDING CASE OR CONTROVERSY.

In disregard of Article III, Section 512(h) authorizes the issuance of judicial process absent a pending case and without any requirement that any elements of a legal cause of action even be *alleged*. Further, the statute supposedly foists upon the judiciary the distinctly non-judicial role of serving as private investigator for a non-litigant on an *ex parte* basis. The

machinery of the federal courts simply cannot be used to investigate *possible civil wrongdoing* or to identify *possible* defendants outside the context of an actual "case" or "controversy."

A. Courts May Act Only in Cases or Controversies.

Article III of the Constitution limits the exercise of federal judicial power to specifically enumerated "cases" and "controversies." U.S. Const. Article III, sec. 2. A "case" in the constitutional sense has consistently been defined as "a suit instituted according to the regular course of judicial procedure." *Muskrat v. United States*, 219 U.S. 346, 356 (1911) (citation omitted). As the Ninth Circuit recently has held, "[t]he requirement that a case or controversy anchor our jurisdiction as a threshold matter spring[s] from the nature and limits of the judicial power of the United States and is inflexible and without exception." *United States v. Larson*, 302 F.3d 1016, 1019 (9th Cir. 2002) (internal quotations omitted) (alteration in original).

From the earliest days of the Republic, this requirement has been understood to entail, at a minimum, an adversarial proceeding that involves at least two parties, a cause of action within the jurisdiction of the federal courts, and a prayer for judicial relief that is determinative of some set of rights or obligations as between those parties. *Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *Osborn v. Bank of United States*, 22 U.S. (9 Wheat.) 738, 819 (1824); *United States v. Ferreira*, 54 U.S. (13 How.) 40 (1851); *Gordon v. United States*, 117 U.S. Appx. 697, 699-706 (1864); *Muskrat*, 219 U.S. at 353-63. "A justiciable controversy is definite, concrete, real, and substantial; it is subject to specific relief. A controversy is not justiciable if it is hypothetical, abstract, academic, or moot." *Campbell v. Wood*, 18 F.3d 662, 680 (9th Cir. 1994). In the absence of such a case or controversy, a federal court is without authority to take *any* judicial action, except dismissal of the proceeding. *Ex parte McCardle*, 74 U.S. (7 Wall.) 506, 514 (1868); *Mansfield, C. & L.M. Ry. Co. v. Swan*, 111 U.S. 379, 382 (1884); *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998).

The Supreme Court consistently has rejected legislative and executive attempts to expand federal courts' "case or controversy" jurisdiction by converting them into free floating investigative bodies to discover facts unconnected to the adjudication of actual disputes. *See*

Hayburn's Case, 2 U.S. at 410 (concluding that a law assigning judges the task of taking pension applications and making recommendations to the Secretary of War unconstitutionally imposed duties "not of a judicial nature"); *United States v. Ferreira*, 54 U.S. (13 How.) 40, 46-47 (1851) (striking down a law assigning Florida judges the task of adjusting claims by Spanish inhabitants under the Treaty of 1819 in *ex parte* proceedings based "upon such evidence as he may have before him, or be able himself to obtain").

In *United States v. Morton Salt Co.*, the Supreme Court again confirmed that "[f]ederal 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." 338 U.S. 632, 641-42 (1950). In upholding the ability of a federal agency to monitor compliance with a previously entered judicial decree, the Court drew a sharp distinction between these "investigative and accusatory duties," properly lodged in an executive agency, and the more limited role of the Article III courts. *Id.* at 643. While the agency could engage in a "fishing expedition" for evidence of civil or criminal wrongs, "[c]ourts have often disapproved the employment of the judicial process in such an enterprise." *Id.* at 641-42; *see also Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 171-72 (1803); *Yale Todd's Case*, *printed at* 54 U.S. (13 How.) 52 (1851); *Gordon*, 117 U.S. Appx. at 699-706; *United States Catholic Conf. v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988).[6]

[6] Assigning the clerk of the court the non-judicial role of issuing subpoenas for private parties outside of any pending case will also interfere with operations of the Judicial Branch itself by diverting resources from their proper adjudicative role. Indeed, the clerk's office of the district court in Washington, D.C. has already been flooded with subpoena requests and has been forced to reassign personnel from other tasks. *See RIAA Nearing 1,000 Subpoenas Against File-Sharing Suspects*, SiliconValley.com, July 18, 2003, *at* http://www.siliconvalley.com/mld/siliconvalley/6335275.htm (visited July 21, 2003). The *Verizon II* court alluded to this possibility as a substantial separation of powers concern, 257 F.Supp. 2d at 256, but held that the concern was "speculative" because "no barrage of requests has occurred." *Id.* What the district court deemed to be speculation at the time *Verizon II* was decided has now clearly come to pass.

B. Issuance and Enforcement of Subpoenas, Like All Other Judicial Acts, Must Occur Within the Context of a Case or Controversy.

The issuance and enforcement of subpoenas are no exception to Article III's requirement that judicial acts must occur within the context of a case or controversy properly pending before a federal court. A subpoena is a form of *judicial process* – a tool to assist the court in the resolution of some other actual case or controversy. Thus, Fed. R. Civ. P. 45(a)(2) requires that "[e]very subpoena shall ... state the title of the action, the name of the court in which it is pending, and its civil action number." *See* Black's Law Dictionary 1426 (6th ed. 1990) ("subpoena *duces tecum*" is "[a] court process, initiated by a party in litigation, compelling production of certain specific documents ... material and relevant to facts in issue in a pending judicial proceeding").

In *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, the Supreme Court affirmed the right of the recipient of a third-party subpoena to challenge the underlying jurisdiction of the court in whose name the subpoena issued – even in the posture of a civil contemnor. The Court reasoned that:

> Federal Rule Civil Procedure 45 grants a district court the power to issue subpoenas as to witnesses and documents, *but the subpoena power of a court cannot be more extensive than its jurisdiction.* It follows that if a district court *does not have subject-matter jurisdiction over the underlying action, and the 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.

487 U.S. 72, 76 (1988) (emphases added); *see Morton Salt*, 338 U.S. at 642 ("The *judicial* subpoena power ... is subject to those *limitations inherent in the body that issues them* because of the provisions of the Judiciary Article of the Constitution." (emphases added)). Thus, a subpoena would be void *ab initio* where an attempt had been made to plead the elements of a federal action but that attempt was unsuccessful. *United States Catholic Conf.*, 487 U.S. at 76. *A fortiori,* such process is void where there has never been an attempt to properly invoke the subject matter jurisdiction of any federal court.[7]

[7] The *Verizon II* court suggested, without analysis, that Section 512(h) was analogous to other federal statutes. 257 F. Supp. 2d at 251. But none of these statutes involves the issuance and enforcement of a *judicial* subpoena simply to gather facts that are deemed useful to a private party. They all involve either judicial enforcement of administrative process where a live

The U.S. District Court for the Northern District of California also has confirmed that attempts to force the identification of otherwise anonymous individuals must be made in the context of a justiciable case or controversy. In *Columbia Insurance*, the Court was reluctant to require the identification of an individual *even where a complaint already had been filed* against that individual where it had not also been served. 185 F.R.D. at 577 (observing that "[a]s a general rule, discovery proceedings take place only after the defendant has been served" but that "in rare cases, courts have made exceptions").[8] The Court ultimately allowed the plaintiff to seek the identity of the defendant from third parties, but only after establishing several prerequisites for seeking that discovery, including that the plaintiff "establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." *Id.* at 579. These requirements were designed, *inter alia*, to "ensure that federal requirements of jurisdiction and justiciability can be satisfied," "to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant." *Id.* at 578-79. Significantly, the Court held that the "plaintiff must make some showing that an act giving rise to civil liability actually occurred" before forcing disclosure of the defendant's identity and that "[a] conclusory pleading will never be sufficient to satisfy this element." *Id.* at 579-80.[9]

(Continued . . .)
controversy arising under federal law is presented, *see* 35 U.S.C § 24; 45 U.S.C. § 157(h); 7 U.S.C. § 2354(a), or inherent powers, such as that of the judiciary to offer international comity to tribunals in foreign nations. *See* 28 U.S.C. § 1782(a).

[8] *See also Rancho Publ'ns v. Superior Court*, 68 Cal. App. 4th 1538, 1547-48, 1551 (Ct. App. 1999) (recognizing that "there is a … qualified immunity, grounded in the free speech and privacy provisions of the United States and California Constitutions, that limits what courts can compel through civil discovery," and refusing to permit discovery of speakers' identities where information was not "directly relevant to the [pending] defamation lawsuit").

[9] In *Verizon II*, the district court conceded that Section 512(h)'s subpoena provision is an "innovation," 257 F. Supp. 2d at 249, but found that it did not violate Article III. It relied almost entirely on its theory that a clerk issuing a subpoena under Section 512(h) performs a purely "ministerial act," and therefore Article III is not implicated at all in the issuance of the subpoena. *Id.* at 249-251. However, the effect of a subsection (h) subpoena is anything but "ministerial." The subpoena is issued *in the name of the district court* and carries with it *on the day of its issuance* the enforcement authority that federal courts derive from Article III of the Constitution. *See, e.g.*, Advisory Committee Notes to Rule 45 (1937) ("This rule applies to subpoenas ad

C. The Subpoena at Issue Here Was Issued Outside of any "Case or Controversy" and Is Therefore Unenforceable Under Article III.

XYZ's *ex parte* request for a subpoena is not itself a "case or controversy" within the meaning of Article III. Such a request does not present the elements of any civil action within the jurisdiction of the federal courts. Although the requestor must recite that the subpoena's "purpose" is to identify an alleged infringer and that information obtained will be used for "protecting rights" under the copyright laws, no suit need ever be brought, or even contemplated, for a subpoena to issue. 17 U.S.C. § 512(h)(2)(C). Indeed, the notice that accompanies the subpoena requires only the assertion of "a good faith belief" – but not even necessarily a reasonable one – that infringement has occurred. *See id.* § 512(c)(3)(A)(v); Order, *Rossi v. MPAA*, No. 02-00239BMK, at *7 (D. Haw. Apr. 29, 2003) (stating that "good faith" provision in subsection (c) does not even "require[] a copyright holder to conduct an investigation to establish actual infringement prior to sending a notice to an ISP"). That is, the showing necessary to obtain a Section 512(h) subpoena would not even pass the Rule 11 sanctions test for filing a lawsuit.[10]

In sum, at the time this subpoena was issued no case or controversy existed within the subject matter jurisdiction of the federal courts. The facts XYZ seeks to uncover are not placed before this Court or any other body in aid of adjudication of any issue of federal law. They are simply handed over to XYZ for any use it deems necessary in protecting its asserted copyright

---

(Continued . . .)
testificandum and duces tecum issued by the district courts."); *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."). Indeed, the very cases relied upon by the district court flatly contradict its ultimate conclusion, 257 F. Supp. 2d at 250-51. *See, e.g.*, *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.").

[10] Section 512(h) does not require the pleading of the elements of an infringement cause of action. While an action for copyright infringement can be brought only by the owner of the exclusive rights, 17 U.S.C. § 501(b); *Gardner v. Nike, Inc.*, 279 F.3d 774, 781 (9th Cir. 2002), Section 512(h) allows agents of copyright owners to obtain subpoenas. And while registration of the copyright with the U.S. Copyright Office is a *jurisdictional* prerequisite to an infringement lawsuit, 17 U.S.C. § 411, Section 512(h) requires no such proof of registration.

interests. Offering assistance to private parties to further their business interests or to investigate possible civil claims is simply not an activity that Article III courts can or should engage in.[11]

III. THIS SUBPOENA VIOLATES THE FIRST AMENDMENT RIGHTS OF ABC'S SUBSCRIBERS.

Section 512(h) creates a novel legal device that purports to grant a private party the right to invoke the court's coercive power to strip away another's core First Amendment expressive and associational rights based only upon an *ex parte* declaration, without providing the other party notice or an opportunity to be heard. Because the statute provides insufficient procedural protection for these rights and because it is vastly overbroad, it violates the First Amendment.

A. Internet Users Have a First Amendment Right To Speak, Listen, and Associate Anonymously.

As the Supreme Court repeatedly has recognized, individuals have a right to speak, listen, and associate anonymously. *See, e.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995); *see Talley v. California*, 362 U.S. 60, 64 (1960). The right to speak and associate anonymously takes on particular importance in the Internet context, where courts have confirmed the importance of "the legitimate and valuable right to participate in online forums anonymously or pseudonymously." *Columbia Ins.*, 185 F.R.D. at 578. In a case establishing important procedural safeguards before allowing a plaintiff to discover the identity of a defendant in a pending lawsuit, the U.S. District Court for the Northern District of California observed 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.

[11] The district court in *Verizon II* also ignored its duty to construe Section 512(h) narrowly in light of substantial Article III concerns. *See Ashwander v. Tennessee Valley Auth.*, 297 U.S. 288, 348 (1936) (Brandeis, J., concurring). Because the provision for expedited issuance of Rule 45 subpoena can be given effect in a pending infringement action (it relaxes the limitations on pre-conference discovery contained in Fed. R. Civ. P. 26(d)), it should be construed narrowly to apply only in pending actions. *See Columbia Ins.*, 185 F.R.D. at 579-80 (holding that a complaint that can withstand a motion to dismiss is a pre-requisite to any pre-service discovery).

Id.

B. Section 512(h) Violates the First Amendment.

Although there is obviously no First Amendment right to engage in copyright infringement, no judicial determination of copyright infringement is made at the time Section 512(h) is invoked. No speech is safe if courts simply assume a violation of law based upon unsubstantiated allegations that the complaining party is not required to prove, or even assert, in formal litigation. As discussed in detail in Part II, *supra*, the filings required by Section 512(h) fall far short of meeting even the notice pleading requirements for *alleging* a case of copyright infringement. Such minimal allegations, made in an *ex parte* context, are simply not sufficient to shift the burden to ABC to defend the First Amendment rights of its subscribers.

Because Section 512(h) is a procedure designed to strip Internet speakers of their presumptively protected anonymity, "those procedures violate the First Amendment unless they include built-in safeguards against curtailment of constitutionally protected expression, for 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.'" *Blount v. Rizzi*, 400 U.S. 410, 416 (1971) (citation omitted); *see FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 220 (1990) (plurality opinion) (noting need for First Amendment "procedural safeguards"). Because the Supreme Court has "recognized that 'the line between speech unconditionally guaranteed and speech which may legitimately be regulated . . . is finely drawn,'" "'[t]he separation of legitimate from illegitimate speech calls for sensitive tools.'" *Blount*, 400 U.S. at 417 (citation omitted). Section 512(h) is not a sensitive tool but a blunt instrument. It may be wielded by trade associations, private individuals, or bounty hunters who use automatic "infringement detection" robot software and who are compensated in proportion to the number of potential infringers identified. It inevitably will lead to the irreparable loss of anonymity without even the allegation of a valid cause of action that might justify a restriction on free expression. *See id.* at 410.

First, on its face, Section 512(h) permits the employment of a federal court's power to strip Internet users of their anonymity upon no more than an *ex parte* "good faith" allegation by anyone willing to allege he or she is a copyright owner, or authorized to act on behalf of a copyright owner, that copyright infringement *might* be occurring. 17 U.S.C. § 512(c)(3)(A)(v). Such a cursory showing is not constitutionally sufficient to destroy presumptively protected First Amendment rights. *See Blount*, 400 U.S. at 418. Moreover, the very idea of an *ex parte* proceeding that would strip away an individual's anonymity without that individual having the opportunity to defend himself or herself raises serious First Amendment concerns. *See, e.g.*, *Carroll v. President and Comm'ners of Princess Anne*, 393 U.S. 175, 180 (1968) (use of *ex parte* temporary restraining orders is severely limited in First Amendment context). Accordingly, for these reasons alone, Section 512(h) violates the First Amendment.[12]

Because of this lack of adversarial process (and the accuracy that such process ensures), Section 512(h), if construed to encompass XYZ's subpoena, threatens to sweep within its ambit a substantial amount of protected speech. "The Constitution gives significant protection from overbroad laws that chill speech within the First Amendment's vast and privileged sphere." *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 244 (2002). Section 512(h) inevitably will lead to both honest mistakes and deliberate abuse – thereby stripping Internet users of anonymity even where the underlying speech and association is fully protected. The lax standard applicable to Section 512(h) *already* has led to serious mistakes.[13] While the Section 512(h) mechanism

---

[12] The fact that an ISP may subsequently challenge the subpoena under Rule 45 does not solve the First Amendment problem. First, the burden is unconstitutionally shifted to the ISP to defend the presumptively protected speech of its subscriber. *See, e.g.*, *Freedman v. Maryland*, 380 U.S. 51, 58-60 (1965) (government must bear burden of proving speech is unprotected); *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 775-78 (1986) (libel plaintiff must bear burden of proving speech is false). Second, because the service provider cannot access the material at issue, it cannot formulate copyright defenses, such as fair use or the public domain nature of the material for its subscriber. Third, because there is no notice to the subscriber (notice would be impossible in the context of a demand for numerous names returnable on less than 10-days notice), the subscribers have no opportunity to defend themselves prior to the revelation of their identity.

[13] Copyright owners and their agents have taken to using electronic robots to search the Internet for word groups that *might* suggest the presence of copyrighted works. Thus, a child's book report on one of the Harry Potter stories has been mistaken for a potentially infringing copy of the film Harry Potter and the Sorcerer's Stone. A recording industry group sent an accusatory

will undoubtedly capture the identities of some copyright infringers, judicial process cannot be used to "suppress lawful speech as the means to suppress unlawful speech." *Free Speech Coalition*, 535 U.S. at 254. "Protected speech does not become unprotected merely because it resembles the latter." *Id.* at 255.[14]

In addition to honest mistakes, the lack of any judicial supervision or oversight will encourage abuse. An individual with sinister intentions could carry cyberstalking one step further by alleging that someone he or she "met" in a chat room is a possible copyright infringer, thereby "expeditiously" obtaining that person's name, address, and telephone number. Federal Trade Commission, *Privacy Online: A Report to Congress* at 4-5 (June 1998) ("[The collection of "detailed personal information . . . online from and about children"] present[s] unique privacy and safety concerns because of the particular vulnerability of children ...."). This threat to privacy, and even personal safety, will substantially chill speech and association on the Internet. *Talley*, 362 U.S. at 64; *McIntyre*, 514 U.S. at 342.[15]

(Continued . . .)
notice to Penn State's Department of Astronomy and Astrophysics, based on its association of a humorous song about gamma rays written by a faculty member named Peter Usher with copyrighted songs by the musician known as Usher. The same recording industry association recently launched a campaign using bots to "warn" users of peer-to-peer software about copyright infringement, but later admitted that it made *several dozen* errors in one week. *See* Declan McCullagh, ***RIAA apologises for more mistaken warnings,*** ZD Net UK News, May 14, 2003, at <http://news.zdnet.co.uk/story/0,,t280-s2134658,00.html>.

[14] In *Verizon II*, the district court held that the ISP was entitled to raise the constitutional rights of its subscribers, 257 F. Supp. 2d at 257-58, and that the Internet users do have a First Amendment right to speak and associate anonymously, *id.* at 258-60. The district court erred, however, in determining that the mere "good faith" accusation of infringement provided sufficient safeguards to protect the presumptively protected First Amendment rights of Internet users. *Id.* at 260-64. Other courts have required more. *See, e.g., Columbia Ins.*, 185 F.R.D. at 579; *see also Rancho Publ'ns*, 68 Cal. App. 4th at 1549-50 (disallowing civil discovery of "presumptively protected" private identifying information on the basis of "rank conjecture" that there was a connection between the anonymous individual and possibly illegal conduct).

[15] At the very least, the serious constitutional concerns raised by a broad application of Section 512(h) require this Court to construe subsection (h) narrowly. *See N.L.R.B. v. Catholic Bishop*, 440 U.S. 490, 500 (1979) ("[A]n Act of Congress ought not be construed to violate the Constitution if *any other possible construction* remains available." (emphasis added)); *Ashwander*, 297 U.S. at 348 (Brandeis, J., concurring). Reading Section 512(h) to apply only where the subscriber stores his or her allegedly infringing material on the ISP's system or network is an alternative construction that avoids the serious First Amendment questions raised by application of Section 512(h) to private email, web browsing, and chat room activity. Under this reading, those activities where the subscriber's privacy and anonymity interests are at their zenith, in connection with material stored on the subscribers' own personal computers, would not

IV. THE SUBPOENA PROVISION VIOLATES THE DUE PROCESS RIGHTS OF ABC AND ITS SUBSCRIBERS.

Even apart from the heightened protection required in the First Amendment context, elemental principles of due process require more than Section 512(h) accords here. *See, e.g., Connecticut v. Doehr*, 501 U.S. 1, 13-14 (1991) ("good faith" *ex parte* attachment statute creates "too great a risk of erroneous deprivation"); *Fuentes v. Shevin*, 407 U.S. 67, 83 (1972) (applicant's self interested statement of "belief in his [own] rights" insufficient to work a deprivation of property or liberty). "The fundamental requirement of due process is the opportunity to be heard 'at a meaningful time and in a meaningful manner.'" *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976) (quoting *Armstrong v. Manzo*, 380 U.S. 545, 552 (1965)). The absence of any required notice to the subscribers whose liberty and privacy rights are at issue, and any other safeguards to protect their anonymity as well as ABC's interest in its subscriber list information, renders the Section 512(h) subpoena process unconstitutional under the Fifth Amendment.

First, Internet users' interest in engaging in online communications and associations with anonymity is beyond dispute. *See supra* Part III. Moreover, ABC has a protectible property interest in its subscriber list. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003 (1984); *Barnes Group, Inc. v. O'Brien*, 591 F. Supp. 454, 460 (N.D. Ind. 1984). Indeed, ABC would risk suffering great competitive harm if a substantial portion of its subscriber list made its way into the hands of competitors. Thus, that both ABC and its subscribers have interests protected by the Due Process Clause of the Constitution is beyond peradventure.

Second, as described above, Section 512(h)'s *ex parte* process lacks any of the safeguards normally required to satisfy Due Process. Indeed, self-interested copyright owners are not even required to make a *prima facie* showing of infringement that could withstand a motion to dismiss or is subject to Rule 11 sanctions. *See supra* Part II.C. Most disturbingly from a due process

---

(Continued . . .)
be subject to the truncated subpoena process. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (expressive activity that may be proscribed outside the home is constitutionally protected inside the home).

standpoint, Section 512(h) does not require that the accused Internet user even be given notice of the subpoena – much less an opportunity to defend himself or herself – before a subpoena is issued purporting to require an ISP to reveal the identity of that user. *See* 17 U.S.C. § 512(h). The expedited nature of the Section 512(h) subpoena process and the bundling of multiple users on a single subpoena render it impossible for ordinary Internet users to receive any notice or opportunity to defend their anonymity prior to compliance. Nor does a judge oversee the process of subpoena issuance; instead, the clerk is required, no matter how obviously far-fetched the claim may be, to issue a subpoena "expeditiously" if everything on the checklist of materials has been submitted. *Id.* Such lack of scrutiny is important because, as observed in *Fuentes*, the applicant's self-interested statement of "belief in his [own] rights" is insufficient to permit a deprivation of property or liberty. 407 U.S. at 83.

V. THE SUBPOENA SUFFERS FROM ADDITIONAL DEFECTS.

This subpoena suffers from at least five specific defects that require that this Court quash the subpoena or modify the terms of compliance, regardless of its ruling on the other issues in this proceeding.[16] First, Section 512(h) does not authorize a single subpoena that seeks the identities of multiple subscribers asserted to have engaged in completely unrelated acts of infringement. *See, e.g.*, 17 U.S.C. § 512(h)(1) (providing for issuance of a subpoena "for identification of *an* alleged infringer); *id.* § 512(h)(2)(C) ("the purpose for which the subpoena is sought is to obtain the identity of *an* alleged infringer"); *id.* § 512(h)(3) ("identify *the* alleged infringer") (emphases added). Although the notice requirement of Section 512(c)(3)(A), incorporated by Section 512(h)(4), does permit a purported copyright owner to issue a "single notification" for "multiple copyrighted works," it limits the "single notification" to "*a single online site.*" *Id.* § 512(c)(3)(A) (emphasis added).

Second, ABC objects to the subpoena because there is no tender or agreement to compensation. Under Fed. R. Civ. P. 45(c)(3)(B), as a third-party asked to provide confidential

[16] There may be other defects associated with the service of this subpoena, including lack of personal service and service beyond the 100-mile limit of Fed. R. Civ. P. 42(b).

business information, ABC is entitled to compensation for its effort in identifying, verifying, and conveying the information pursuant to the subpoena. *See Broussard v. Lemons*, 186 F.R.D. 396, 398 (W.D. La. 1999) (third parties subjected to repeated multiple subpoenas would be subject to "significant" expenses for compliance in the aggregate, and therefore should be reimbursed for cost of compliance even where costs for compliance with single subpoena is merely $43). ABC must undertake significant time and effort to obtain and verify IP addresses and associate them with the identity of a particular subscriber. As a third-party witness, ABC is entitled to compensation for the costs of compliance.

Third, ABC objects to producing confidential business information outside the context of a properly crafted protective order or non-disclosure agreement that adequately protects against disclosure that will harm ABC's competitive and property interests in its subscriber data. *Covey Oil Co. v. Continental Oil Co.*, 340 F.2d 993 (10th Cir. 1965) (when third parties are forced to reveal confidential information, courts should supply reasonable protective measures, such as limiting distribution and scope of use of information and ordering that information be sealed). ABC cannot be forced to produce commercially sensitive material without proper protections, including, *inter alia*, limitations on use to avoid disclosure to personnel who are involved in business decisions for competitors, restrictions on proper handling and copying, and return or destruction of the material upon completion of its authorized use. *See, e.g.*, *Compaq Computer Corp. v. Packard Bell Electronics, Inc.*, 163 F.R.D. 329, 339-40 (N.D. Cal. 1995).

Fourth, the subpoena fails to comply with the "sworn declaration" requirement of Section 512(h)(2)(C), that the information sought "will *only* be used for the purpose of protecting rights under this title." (emphasis added).

Finally, the subpoena is overbroad even assuming that it is otherwise valid. Section 512(h)(3) states that the subpoena may require production of "information sufficient to identify the alleged infringer of the material described in the notification." Obviously, the individual's name, address, and telephone number constitute "information sufficient to identify" the person at issue. An Internet user's email address, by contrast, is not "information sufficient to identify"

the subscriber, as the email address itself may not relate in any way to the user's identity, and ABC's subscribers may choose to use any email service, including services offered by other ISPs. As email addresses are mentioned elsewhere in the statute, *see* 17 U.S.C. § 512(c)(3)(A)(iv), but not in Section 512(h), it seems clear that the statute does not authorize a subpoena demanding a subscriber's email address. Moreover, revelation of the email address, to the extent it is accurate, would constitute an additional invasion on the subscriber's privacy, allowing XYZ to monitor or track the subscriber's activity beyond the specific use of peer-to-peer software specified in the notice and the subpoena. Depending upon XYZ's intended use of the email address, it might also raise issues of spamming, harassment, or other tort liability under various state laws.

CONCLUSION

For the foregoing reasons, ABC respectfully requests that the Court quash XYZ's subpoena.

Respectfully submitted,

By:_____

Counsel for Movant
ABC Corporation

UNITED STATES DISTRICT COURT

IN RE: **SUBPOENA ENFORCEMENT MATTER**	)	CV 00000000000000

ORDER QUASHING XYZ'S SUBPOENA SERVED ON ABC CORPORATION

XYZ Corporation ("XYZ") served a subpoena on ABC Corporation ("ABC") seeking the name, address, telephone number, and email address of numerous ABC subscribers. XYZ claims that these Internet users employed peer-to-peer software to offer its copyrighted material over the Internet from their personal computers. No copyright infringement action has been filed and the elements of a copyright infringement case have not been placed before the Court as to any of these individuals. ABC does not monitor or control the content of the communications at issue in this proceeding. ABC has filed a Motion To Quash XYZ's Subpoena based on both statutory and constitutional grounds.

The Court, having reviewed the papers submitted by the parties, and for good cause shown, hereby ORDERS that Movant ABC's Motion is GRANTED for the following reasons.

First, the subpoena is not authorized by the Copyright Act because the subpoena power contained in 17 U.S.C. § 512(h) is limited to situations where the Internet service provider ("ISP") hosts potentially infringing material on its own network (such as a website). Extension of the subpoena power to material residing on the personal computers of the over 100 million Internet users is contrary to the text, structure, and purpose of this statute. *See Robinson v. Shell Oil Co.*, 519 U.S. 337, 343-44 (1997); *Estate of Joseph Leder v. Comm'r of Internal Revenue*, 893 F.2d 237, 241 (10th Cir. 1989); *Overseas Educ. Ass'n v. FLRA*, 824 F.2d 61, 65 (D.C. Cir. 1987). Even if the subpoena power could be read to extend to any situation where a take-down notice is authorized by the statute, no take-down notices are authorized by 17 U.S.C. § 512(a), the

provision that applies to ABC in this proceeding, and Congress's decision to omit take-down notices from subsection (a) of the statute must be given effect. *See United States v. Male Juvenile,* 280 F.3d 1008, 1015 (9th Cir. 2002) (citing *Russello v. United States,* 464 U.S. 16, 23 (1983)).

Second, Section 512(h) violates Article III of the Constitution because it authorizes the issuance and enforcement of third-party subpoenas outside of any pending case or controversy. *See Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *United States v. Morton Salt Co.*, 338 U.S. 632 (1950); *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72 (1988); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999). The Court must construe the statute consistent with the dictates of Article III, *see Jones v. Bates*, 127 F.3d 839, 855-56 (9th Cir. 1997), and therefore holds that subpoenas under 17 U.S.C. § 512(h) may only be issued and enforced in the context of a pending litigation under the Copyright laws.

Third, Section 512(h) violates the First Amendment's guarantee of anonymous expression and association because it requires that a copyright owner or its agent submit only a minimal, unsubstantiated, *ex parte* assertion of copyright infringement to obtain a subpoena requiring an ISP to reveal the identity of its accused subscribers, contains no notice provisions whatsoever to the subscribers involved in the types of Internet activities at issue in this proceeding, and impermissibly shifts the burden to the ISP to defend presumptively protected speech. *See Blount v. Rizzi*, 400 U.S. 410 (1971); *Reno v. ACLU*, 521 U.S. 844, 874 (1997); *Freedman v. Maryland*, 380 U.S. 51, 58-60 (1965); *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 775-78 (1986); *Columbia Ins.*, 185 F.R.D. 573; *Rancho Publ'ns v. Superior Court of Orange Count*, 68 Cal. App. 4th 1538, 1547-48, 1551 (Ct. App. 1999).

Fourth, Section 512(h) as applied fails to satisfy the minimum procedural requirements of the Fifth Amendment before depriving Internet users of their liberty interest and ISPs of their property interest in their subscriber lists. *See Connecticut v. Doehr*, 501 U.S. 1 (1991).

Fifth, the subpoena improperly bundles multiple subscribers into one subpoena, makes no provision for compensation of ABC, offers no protection for the proprietary data that it purports to require ABC to produce, and fails to comply with the "sworn declaration" requirement of

Section 512(h)(2)(C). *See Covey Oil Co. v. Continental Oil Co.*, 340 F.2d 993 (10th Cir. 1965); *Broussard v. Lemons*, 186 F.R.D. 396, 398 (W.D. La. 1999).

SO ORDERED on this ___ day of _____, 2003.