No. 03-3802

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

THE RECORDING INDUSTRY ASSOCIATION OF AMERICA,

Appellee,

v.

CHARTER COMMUNICATIONS, INC.,

Appellant.

Appeal from the United States District Court
for the Eastern District of Missouri
Hon. Carol E. Jackson, Chief United States District Judge

APPELLANT'S OPENING BRIEF

Paul Glist
John D. Seiver
Geoffrey C. Cook
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
202-659-9750

Stephen B. Higgins
Mark Sableman
James W. Erwin
Thompson Coburn LLP
One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000

Attorneys for Appellant Charter Communications, Inc.

SUMMARY OF THE CASE

The resolution of this appeal will establish whether and how copyright owners may use an unsupervised judicially aided subpoena process to learn the identity of individuals suspected of copyright infringement by sharing files over the Internet. The issue is whether the Digital Millennium Copyright Act authorized the court clerk, on request of Appellee, to issue subpoenas that were served on Appellant, an Internet Service Provider (ISP), seeking personal information about individual Internet users whom Appellee believed were trading copyrighted works over the Internet using peer-to-peer file sharing computer programs. The subpoenas were enforced without any evidence of actual copyright infringement, and without an underlying suit, over Appellant's constitutional and statutory objections.

Appellant requests 30 minutes for oral argument because this case presents important issues on (1) the nature and scope of the DMCA, and (2) whether the special subpoena provision designed to aid in the hunt for suspected copyright infringers, if it is constitutional, can override pre-existing constitutional and statutory limitations on disclosure by a cable ISP of its customers' personal information.

CORPORATE DISCLOSURE STATEMENT

Charter Communications, Inc. has no parent corporation and no publicly held company owns ten percent (10%) or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Constitutional Provisions

JURISDICTIONAL STATEMENT

This is an appeal from an order of the United States District Court for the Eastern District of Missouri enforcing subpoenas directed to Charter Communications, Inc. by The Recording Industry Association of America, Inc. ("RIAA"). The jurisdiction of the district court was invoked under the Digital Millennium Copyright Act of 1998 ("DMCA"), 17 U.S.C. § 512(h).

The order entered by the district court was a final order within the meaning of 28 U.S.C. § 1291. Charter invokes the jurisdiction of this Court under that statute.

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

1. Whether the district court erred as a matter of law when it enforced subpoenas under 17 U.S.C. § 512(h) that did not and could not comply with the express terms of the DMCA.

Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir., Dec. 19, 2003)

United States Catholic Conference v. Abortion Rights Mobilization, Inc., 487 U.S. 72 (1988)

In re Marc Rich & Co., A.G., 707 F.2d 663 (2nd Cir. 1983)

17 U.S.C. §§ 512(h), 512(c)(3)(A) & 512(a)

2. Whether the district court erred as a matter of law when it enforced the RIAA's subpoenas in the absence of a case or controversy sufficient to support that exercise of judicial power.

United States Catholic Conference v. Abortion Rights Mobilization, Inc., 487 U.S. 72 (1988)

Houston Business Journal, Inc. v. Office of Comptroller of Currency, 86 F.3d 1208 (D.C. Cir. 1996)

In re Marc Rich & Co., A.G., 707 F.2d 663 (2nd Cir. 1983)

U.S. CONST., art. III, § 2

3. Whether the district court erred as a matter of law when it enforced the subpoenas in contravention of the privacy requirements applicable to cable operators in the Communications Act of 1934.

United States v. Cox Cable Communications, 1998 WL 656574 (N.D. Fla. 1998)

United States v. Menache, 348 U.S. 528 (1995)

United States Catholic Conference v. Abortion Rights Mobilization, Inc., 487 U.S. 72 (1988)

Houston Business Journal, Inc. v. Office of Comptroller of Currency, 86 F.3d 1208 (D.C. Cir. 1996)

47 U.S.C. § 551(c)

17 U.S.C. § 512(h)

4. Whether the district court erred as a matter of law when it enforced the subpoenas in violation of the First Amendment.

Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., No. CV01-08541, 2003 WL 1989129 (C.D. Cal. April 25, 2003)

Blount v. Rizzi, 400 U.S. 410 (1971)

Broadrick v. State of Oklahoma, 413 U.S. 601 (1973)

Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002)

U.S. CONST., amend. I

17 U.S.C. §§ 512(h) & 512(c)(3)(A)(v)

5. Whether the district court erred when it ordered Charter to provide the RIAA e-mail addresses of its subscribers.

17 U.S.C. §§ 512(h)(3), 512(c)(3)(A)(iv) & 512(g)(3)(D)

STATEMENT OF THE CASE

This action was initiated by the RIAA's request to the clerk of the district court under 17 U.S.C. § 512(h) for the issuance of subpoenas to Charter in its capacity as an Internet Service Provider ("ISP"). These subpoenas sought the names, physical addresses, telephone numbers and e-mail addresses for approximately 200 of Charter's subscribers who allegedly shared material over the Internet in violation of RIAA members' copyrights. *See* Separate Appendix ("SA") 7A. The clerk issued the subpoenas, which were served on Charter on September 23, 2003.

On October 3, Charter filed a motion to quash the subpoenas. SA 290A. On November 17, 2003, the district court held a hearing at which argument was presented by counsel. *See* Transcript 15. No evidence was offered other than the parties' respective supporting affidavits.

The court denied Charter's motion in all respects, except that it held that Charter should not provide the subscribers' telephone numbers. SA 316A. The court directed Charter to provide the names, addresses, and e-mail addresses of 150 subscribers by November 21, 2003, and to

provide the same information for an additional 50-70 subscribers by December 1, 2003.

Charter filed its notice of appeal on November 20, 2003. Charter also sought an emergency stay of the order in the district court and this Court. The district court declined to rule on the motion for stay and this Court denied Charter's motion on November 21. Later, the district court denied Charter's motion as moot. Charter turned over the information on its subscribers to the RIAA as directed.

STATEMENT OF FACTS

This case concerns the issue of whether the Digital Millennium Copyright Act, specifically 17 U.S.C. § 512(h), permits copyright owners and their representatives to obtain and serve subpoenas on ISPs to obtain information about the ISPs' subscribers, such as names, addresses, e-mail addresses, phone numbers, and other data, who are alleged to be trading copyrighted works through the Internet using so-called "peer-to-peer" or "P2P" file sharing computer programs. Many people in this country and around the world share digital files using P2P computer programs with names such as KaZaA, Morpheus, and Grokster. Unlike centralized file-sharing programs, such as Napster, that rely upon a single facility for storing files, P2P file sharing programs allow an individual Internet user to access through the Internet the files located on other individuals' own computers.

In recent years, the RIAA has sought to identify individuals whom it claims are trading copyrighted works of music through P2P file sharing programs. As part of its effort to identify computer users it believes are infringing copyrights, the RIAA has employed tracking programs to identify the Internet Protocol (IP) addresses of computer users

suspected of trading copyrighted music files. With an IP address, the RIAA can identify the ISP providing Internet access to an alleged infringing party. Only the ISP, however, can link a particular IP address with an individual's name and physical address. The RIAA does not claim that Charter itself is storing allegedly infringing material on its servers. Rather, at issue here is whether, under § 512(h), the RIAA may simply suspect that infringing materials are being exchanged yet obtain and serve subpoenas on ISPs requiring them to provide data about those suspected subscribers when the ISP functions solely as a conduit for the transmission of information by its subscribers.

In this case, the RIAA issued subpoenas to Charter, pursuant to § 512, to produce the names, physical addresses, telephone numbers, and e-mail addresses of approximately 200 of Charter's subscribers. SA 7A. On October 3, 2003, Charter filed a Motion to Quash the subpoenas on several grounds, including that "the DMCA does not authorize issuance of subpoenas to service providers where the service providers are involved solely in the transmission of peer-to-peer communications." SA 290A.

In a hearing held on November 17, 2003, the district court denied Charter's Motion to Quash. *See Minute Order*, (Nov. 17, 2003), Addendum at 1a; SA 316A. The district court ordered Charter to give the RIAA by November 21 the names, addresses, and e-mail addresses of 150 subscribers who had received notice of the subpoenas, and to produce the same information by December 1 for another 50 to 70 subscribers who had not yet received notice. *See id*. The district court declined to order Charter to provide the telephone numbers of subscribers. *See id*.

On November 20, 2003, Charter filed a Notice of Appeal and a Motion to Stay the District Court's Order. SA 317A. The district court declined to act on the motion to stay its Order before the compliance deadline of November 21, 2003. On November 21, 2003, Charter filed with this Court its Emergency Motion to Stay Order of Enforcement of Subpoena Pending Appeal. The Court denied a stay that same day. As a result, Charter turned over the subpoenaed names and addresses of its subscribers to the RIAA.

SUMMARY OF THE ARGUMENT

Section 512(h) of the Digital Millennium Copyright Act ("DMCA") authorizes the clerks of federal district courts to issue subpoenas to copyright owners or their agents, without judicial supervision, for service on Internet Service Providers ("ISPs") in order to obtain the identity of subscribers alleged to be engaged in copyright infringement. A condition for issuing these subpoenas under the DMCA is that the copyright owners must also identify the allegedly infringing material so as to permit the ISP to "locate" and "remove" it.

In this case, the RIAA suspects approximately 200 of Charter's subscribers of trading copyrighted music files over the Internet using so-called "peer-to-peer" or "P2P" file sharing computer software. P2P file sharing is accomplished without an ISP's knowledge or the use of an ISP's computers; it is accomplished solely using a subscriber's own computer sending files over the Internet. Significantly, in the P2P context, entities such as the RIAA have no evidence of an actual infringement or where any infringement could have taken place, only an unverifiable suspicion of infringement. As such, an ISP such as Charter cannot verify the claims of infringement or even "locate" or

"remove" any allegedly infringing materials, if indeed there are any infringing materials. Yet the RIAA's subpoenas require Charter to produce personally identifying information on all these "suspicious" subscribers. Because there is no evidence of infringement, and no way for Charter to locate, verify or remove any files from a subscriber's computer, the RIAA's subpoenas necessarily fail to meet the requirements of the DMCA. Accordingly, the district court committed reversible error when it enforced the RIAA's subpoenas over Charter's objections.

In addition, the subpoenas should have been quashed because there were no underlying "cases or controversies" involving these suspected subscribers. All that has occurred is suspicious activity that RIAA interprets as copyright infringement. But, without a genuine case or controversy, and the necessary evidence of infringement to support a case, the subpoenas are invalid and void. Also, because Charter is a cable operator as well as an ISP, it has a separate statutory obligation under the Cable Act to protect its subscribers' privacy that cannot be compromised by a DMCA subpoena where there is no underlying case or controversy.

Moreover, these subpoenas implicate substantial First Amendment rights of Internet users. Because there is no evidence of infringement at all – only suspicion and speculation – identifying these individuals necessarily chills expressive activities by stripping Internet users of their anonymity and subjecting them to potentially invalid claims that will result in intimidation and harassment.

Finally, the requirement that ISPs provide e-mail addresses of these suspected infringers exceeds the terms of the DMCA and would allow third parties to not only learn the identity of individuals they may dislike, but also contactthose Internet users electronically and intrude into their lives without legitimate basis or judicial supervision.

The subpoena power under the DMCA is necessarily constrained by the constitutional and statutory rights of ISPs and Internet users. The district court's order trampled these rights and must be reversed. Moreover, in order to preserve these rights, the RIAA should be ordered to return the information supplied under the subpoenas and make no further use of it.

ARGUMENT

Standard of Review

The district court's Order, enforcing the RIAA's subpoenas over Charter's objection, necessarily concluded that the subpoenas were authorized by 17 U.S.C. § 512 and therefore constituted a ruling of law. This Court reviews *de novo* a district court's rulings on issues of law. *See, e.g., National Union Fire Insurance Co. v. Terra Industries*, 346 F.3d 1160, 1164 (8th Cir. 2003).

The Court reviews the existence of subject matter jurisdiction *de novo*. *See V S Ltd. Partnership v. Department of Housing and Urban Development*, 235 F.3d 1109, 1112 (8th Cir. 2000); *United Sates v. Peninsula Communications, Inc.*, 265 F.3d 1017, 1024 (9th Cir. 2001); *Norfolk Southern Ry. Co. v. Guthrie*, 233 F.3d 532, 534 (7th Cir. 2000).

I.

The District Court Lacked Jurisdiction Of The Subject Matter Because § 512(h) Applies Only To ISPs Engaged In Storing Copyrighted Material And Not To ISPs, Such As Charter, Who Are Engaged Solely As A Conduit For The Transmission Of Information By Others

When a district court lacks the statutory authority to issue a subpoena, it lacks jurisdiction of the subject matter in any enforcement proceeding. *See, e.g., In re Marc Rich & Co., A.G.*, 707 F.2d 663, 669 (2nd Cir. 1983)("A federal court's jurisdiction is not determined by its power to issue a subpoena; its power to issue a subpoena is determined by its jurisdiction.") Even though there is no actual case or controversy between the RIAA and Charter's subscribers in the Article III sense, *see infra* Part II, Charter may nevertheless raise the lack of subject matter jurisdiction in a subpoena enforcement proceeding directed to it, even on appeal. *See United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72 (1988); *Bueford v. Resolution Trust Corp.*, 991 F.2d 481, 485 (8th Cir. 1993).

The question of whether § 512(h) authorizes the issuance of a subpoena to an ISP such as Charter to obtain information about its subscribers who are allegedly infringing RIAA members' copyrights was

recently decided by the District of Columbia Circuit Court of Appeals in *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir., Dec. 19, 2003). There, the Court held that § 512(h) only permits a copyright owner to obtain and serve a subpoena on an ISP for identifying information about an alleged infringer if the ISP is provided statutory notification under 17 U.S.C. § 512(c)(3)(A), which, in turn, requires that the ISP be able to both locate and remove the allegedly infringing material. *See id*. at 1233-34. These requirements are by no means technical, but fundamental: the requirements of subsection (c)(3)(A) were based on the "notice and takedown" provisions in subsection (c) because the premise is that an ISP can respond to the subpoenas by accessing and verifying whether material residing on its servers support or refute the allegations of infringement.

However, when an ISP such as Charter is engaged solely as a conduit for the transmission of material by others, as occurs with subscribers using P2P file sharing software to exchange files stored on their personal computers, the provisions governing the legal consequences are contained in § 512(a), not (c). Recognizing that the

ISP cannot verify the allegations of infringement under subsection (a), the DMCA does not allow clerk-issued subpoenas to be handed out when subsection (a) is implicated because the ISP cannot locate any allegedly infringing material on, or remove it from, others' computers. Thus, the required notification under § 512(c)(3)(A) cannot take place, and, because that notification is not a technical requirement but rather is an essential element for valid clerk-issued subpoenas under subsection (h), a subpoena may not be issued under § 512(h) to ISPs when the underlying claim relates to P2P file exchanges. *See id*. at 1234-37.

The D.C. Circuit's conclusion flows inexorably from the language and structure of the DCMA provisions at issue. Section 512(h)(1) provides:

> A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

17 U.S.C. §512(h)(1).

However, a copyright owner may obtain a subpoena from the clerk only if certain statutory requirements are met. One of those requirements is that notification be provided to the ISP under

§ 512(c)(3)(A). In particular, three distinct parts of subsection (h) reference the § 512(c)(3)(A) notification requirement.

First, subsection (h)(2), entitled "Contents of request," states, in pertinent part, that "[t]he request may be made by filing with the clerk – (A) a copy of a notification described in subsection (c)(3)(A)".

Second, subsection (h)(4), entitled "Basis for granting subpoena," authorizes the clerk to issue a subpoena if, *inter alia*, "the notification filed satisfies the provisions of subsection (c)(3)(A)."

Third, subsection (h)(5), entitled "Actions of service provider receiving subpoena," provides that an ISP is required to respond to a clerk-issued subpoena that is "either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A)." Clearly, a subpoena under § 512(h) may not be issued without meeting the notification requirements of § 512(c)(3)(A).

Section 512(c)(3)(A) in turn requires notification to an ISP to include identification of allegedly infringing material sufficient to permit the ISP to "locate" and "remove" it. Specifically, (c)(3)(A) provides:

> To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: . . . (iii) Identification of the material that is

> claimed to be infringing or to be the subject of infringing activity and *that is to be removed or access to which is to be disabled*, and information reasonably sufficient *to permit the service provider to locate the material*.

17 U.S.C. § 512(c)(3)(A)(emphasis added).

Here, as in *Verizon*, the RIAA's subpoenas fail to meet the requirements of § 512(c)(3)(A)(iii) because the P2P file sharing does not involve the storage of infringing materials on an ISP's own computers, and therefore an ISP such as Charter or Verizon cannot "locate" or "remove" such materials. The *Verizon* Court explained:

> Infringing material obtained or distributed via P2P file sharing is located in the computer (or in an off-line storage device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the ISP can neither "remove" nor "disable access to" the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers.

Id. at 1235.

Indeed, there is absolutely no evidence at all that any infringement has occurred. Indeed, all anybody knows is that the RIAA *suspects* an infringement occurred and that the allegedly infringing files *may* be "located" on an individual subscriber's computer. The RIAA also knows that Charter, like any ISP, has no control over what is on a subscriber's

computer or sent by him or her over the Internet. For example, ISPs such as Charter cannot view the index of subscribers' files stored on their hard drives, cannot see what files may contain music, nor otherwise examine the contents of subscribers' computers.

Significantly, the D.C. Circuit rejected the RIAA's argument that its subpoenas for the identities of alleged P2P infringers should nevertheless be issued and enforced under § 512(h). The RIAA argued that the ISP could "disable access" to infringing material by terminating an offending subscriber's Internet account. *See id*. at 1235. In response, the D.C. Circuit pointed out that, where Congress wanted to authorize the termination of subscriber accounts, it had done so explicitly, for example, in § 512(j)(1)(A)(ii), and that such an extreme remedy was not contemplated by § 512(c)(3)(A)'s reference to removing or disabling access to particular infringing material. *Id*. at 1235-36.[1]

[1] Indeed, terminating a subscriber's entire account is a much broader sanction than merely removing specific material alleged to infringe a copyright. Moreover, ISPs follow different standards under § 512(i) for implementing a policy that provides for termination of subscriber accounts of subscribers who are "repeat infringers." *See Ellison v. Robertson*, 189 F.Supp. 3d 1051, 1056-57 (C.D. Cal. 2002). The DMCA does not provide for termination based on unverifiable allegations or speculation of infringement. This is pointed out by the RIAA's own

The RIAA also argued that a notification could be "effective" under § 512(c)(3)(A) if it substantially met the requirements of (A)(i)-(ii) and (A)(iv)-(vi), even if it did not meet the requirements of subsection (A)(iii). *Id*. The Court also rejected this contention, finding that

> [t]he defect in the RIAA's notification is not a mere technical error; nor could it be thought 'insubstantial' even under a more forgiving standard. The RIAA's notification identifies absolutely no material Verizon could remove or access to which it could disable, which indicates to us that § 512(c)(3)(A) concerns means of infringement other than P2P file sharing.

Id. at 1236.

The Court found unpersuasive RIAA's suggestion that the subpoena authority of § 512(h) was not limited to ISP's engaged in storing copyrighted material. The D.C. Circuit instead agreed with Verizon that

> The presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) [involving "transitory" communications] suggests the subpoena power of § 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.

---

actions: they have served more than 2000 subpoenas directed at identifying suspected infringers, but have brought less than 400 lawsuits. *See* http://rss.com.com/2100-1027_3-5129687.html?part=rss (Court: RIAA lawsuit strategy illegal) and http://abcnews.go.com/sections/scitech/TechTV/RIAA_ruling_fallout_techtv_031224.html (The Lawsuit Beat Goes On).

Id. at 1236-37.

Finally, the D.C. Circuit found that the RIAA's general references to legislative intent underlying the DMCA could not serve as a basis to contradict the text of the statute itself. Noting that "P2P software was 'not even a glimmer in anyone's eye when the DMCA was enacted,' " the court emphasized that it was the province of Congress, not of the courts, to decide whether to rewrite the DMCA "in order to make it fit a new and unforeseen [I]nternet architecture" and "accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." *Id*. (citing *Sony Corp. v. Universal Studios, Inc.*, 464 U.S. 417, 431 (1984)).

The D.C. Circuit's conclusions that "any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of § 512(c)(3)(A) and is therefore ineffective" and that "§ 512(h) does not by its terms authorize the subpoenas issued [by the RIAA]," *id*. at 1236, apply with equal force to the RIAA's subpoenas obtained from the clerk and served on Charter in this case. Just like Verizon, Charter is an ISP that provides Internet access to its customers but does not have access to any of its subscribers' own computer files and does not have the

capability of searching its subscribers' computers. Just like Verizon, Charter cannot "locate" or "remove" allegedly infringing material on its subscribers' own computers. *See id.* at 1235. Here, none of the RIAA's subpoenas satisfy the statutory notification requirement of § 512(c)(3)(A). Unless and until Congress amends the DMCA, the RIAA may not obtain subpoenas from the clerk and the court may not enforce them when the allegations implicate P2P file sharing. Accordingly, the clerk of the district court lacked the authority to issue the subpoenas. Without supporting statutory authority to issue the subpoenas, the court lacked subject matter jurisdiction to enforce them.

II.

A Judicial Subpoena Is a Court Order That Must Be Supported by a Case or Controversy at the Time of its Issuance

If the Court finds that § 512(h) does not authorize the issuance of a subpoena for subscriber information to Charter because it does not store allegedly infringing materials on its servers, then that is the end of the matter. If, however, the Court disagrees, then it must face the second, constitutional jurisdictional question – is there an Article III case or controversy here that allows the federal courts to exercise their judicial power?

The *Verizon* court did not address the issue in detail, except to suggest in a footnote that the application for a subpoena opposed by the party to whom it is issued is a sufficient case or controversy to give the court subject matter jurisdiction in the constitutional sense. *See Verizon*, 351 F.3d at 1231, first footnote *.

However, for the reasons discussed below, there is no case or controversy sufficient to satisfy Article III. There is no existing case or controversy at all between the RIAA – only the possibility of one.[2] The present dispute between the RIAA and Charter cannot be used to bootstrap that lacunae into a reason why the federal courts have power to decide whether to enforce what is, after all, a method of harnessing the judicial power to serve the ends of a private party looking for a reason to sue but lacking a defendant.

There is little doubt that the federal courts are not "free floating investigative bodies" to discover facts unconnected to the adjudication of actual cases or controversies. *Hayburn's Case*, 2 U.S. (2 Dall.) 408

---

[2] For example, the RIAA has filed less than 400 cases although it has served at least 2000 subpoenas (*see* note 1, *supra*), demonstrating that there would not be a valid case underlying more than 75% of the clerk-issued subpoenas the RIAA has served on Charter and other ISPs.

(1792); *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 171-72 (1803); *United States v. Ferreira*, 54 U.S. (13 How.) 40 (1851); *Yale Todd's Case*, *printed at* 54 U.S. (13 How.) 52 (1851); *Gordon v. United States*, 117 U.S. Appx. 697, 699-706 (1864); *Muskrat v. United States*, 219 U.S. 346, 353-63 (1911); *United States v. Morton Salt Co.*, 338 U.S. 632, 641-42 (1950); *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988); *Hoffmann-La Roche Inc. v. Sperling*, 493 U.S. 165, 174 (1989).

In *Morton Salt*, the Supreme Court made clear that "[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." 338 U.S. at 642 (emphasis added). The Supreme Court reaffirmed this principle in *Catholic Conference*, holding 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. at 76 (quoting *Morton Salt*, 338 U.S. at 642) (emphasis added).

The D.C. Circuit, relying upon both *Catholic Conference* and *Morton Salt*, held in *Houston Business Journal, Inc. v. Office of Comptroller of Currency*, 86 F.3d 1208 (D.C. Cir. 1996), that a district court is "*without power to issue a subpoena* when the underlying action is not even asserted to be within federal court jurisdiction." *Id.* at 1213 (emphasis added); *accord Barwood, Inc. v. District of Columbia*, 202 F.3d 290, 294-95 (D.C. Cir. 2000).

The question here is: What is the "underlying action . . . within federal court jurisdiction"? There is none, and thus there is no Article III jurisdiction to support issuance or enforcement of the subpoenas. A subpoena issued by a federal district court is not just a piece of paper that Charter could acknowledge or ignore at its leisure. It is an order of the court that must be obeyed, or the recipient is at peril of being held in contempt of court. *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."); Rule 45(e).

But in order to issue or enforce a subpoena, there must be a case or controversy within the federal court's jurisdiction pending somewhere. It may be a case in another district, *see* Rule 45(a)(2), or may be in aid

of another entity such as an arbitral panel, *see* 9 U.S.C. § 7. Nonetheless, there must be a case or controversy in the Article III sense that supports the issuance of a subpoena.

The case or controversy requirement cannot be relaxed or modified by the Congress. In *Hayburn's Case*, for example, the Court concluded that a law assigning federal judges the role of making recommendations to the Secretary of War on pension applications imposed duties "not of a judicial nature." 22 U.S. at 410-14. Similarly, in *Ferreira*, the Supreme Court struck down a law that assigned to district court judges in Florida the adjustment of claims by Spanish inhabitants under a treaty. 54 U.S. 40. The Court found that the role assigned by statute was not judicial in nature:

> For there is to be no suit; no parties in the legal acceptance of the term, are to be made–no process to issue; and no one is authorized to appear on behalf of the United States, or to summon witnesses in the case. The proceeding is altogether *ex parte*; and all that the judge is required to do, is to receive the claim when the party presents it, and to adjust it upon such evidence as he may have before him, or be able himself to obtain. But neither the evidence, nor his award, are to be filed in the court in which he presides, nor recorded there.

Id. at 46-47.

The D.C. Circuit's suggestion that subsequent litigation can supply the necessary "case" or "controversy" for purposes of Article III, *see Verizon*, 351 F.3d at 1231, is not correct. As the Second Circuit has held, "A federal court's jurisdiction is not determined by its power to issue a subpoena; its power to issue a subpoena is determined by its jurisdiction." *In re Marc Rich,* 707 F.2d at 669. Both *Catholic Conference* and *Houston Business Journal* make clear that the subsequent dispute over the legality of the subpoenas does not create the requisite federal case or controversy to support their issuance in the first place. Instead an existing live controversy is required – not just the expectation of one in the future – for the court to issue or enforce a subpoena. That is all the more so here because there is *no* evidence of infringement by any of Charter's subscribers, only speculation and suspicion, neither of which have supported the commencement of litigation and thus provide no foundation for finding even a future Article III controversy. *See, e.g., Doe v. School Bd. Of Ouachita Parish*, 274 F.3d 289, 292 (5th Cir. 2001).

III.

Enforcement of Subpoenas under § 512(h) Violates the Privacy Protections For Cable Subscribers In The Communications Act

A. The DMCA and the Communications Act Impose Directly Conflicting Obligations on Cable Operators.

Section 551(c)(1) of Title VI of the Communications Act of 1934 ("Cable Act") states that a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber, and that the cable operator shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. 47 U.S.C. § 551(c)(1).[3] Cable operators that violate § 551 are subject to civil liability under 47 U.S.C. § 551(f).

At the same time, § 512(h)(5) of the DMCA requires an online service provider, upon receipt of a subpoena issued pursuant to § 512(h)(1), to

---

[3] Although there are certain exceptions to this broad prohibition against disclosure, *see* § 551(c)(2), none are relevant to the issues raised in this proceeding. One of those exceptions allows for disclosure by court order if the subscriber is notified of such order by the person to whom the order is directed. 47 U.S.C. § 551(c)(2)(B). Because there is no underlying case or controversy, however, this exception does not apply. *See infra*, Part III.C.

"expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena . . ." 17 U.S.C. § 512(h)(5). The information required by the subpoena is "information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider." *Id*. § 512(h)(3).

Consequently, where a copyright owner uses § 512(h) to subpoena from a cable operator (that offers both cable video and Internet services) information sufficient to identify an alleged infringer of copyrighted material, the cable operator faces an untenable situation. A cable operator's compliance with the subpoena request would violate the direct prohibition under § 551(c) of the Cable Act – which explicitly *prohibits* the release of personal information absent the consent of the subscriber or proper notice.[4] However, if the cable operator chooses to comply with the prohibition on disclosure under the Cable Act it would lose its safe harbor rights under the DMCA, and possibly face a court

[4] Moreover, this section of the Cable Act imposes an affirmative duty on the cable operator to "take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator." 47 U.S.C. § 551(c).

order or sanctions for failure to comply with the terms of a subpoena issued under the DMCA.

Thus, two federal statutes, the Cable Act and the DMCA, impose two directly conflicting burdens on cable operators. On the one hand, the Cable Act clearly states that a cable operator shall not disclose personally identifiable information about any subscriber absent that subscriber's consent. On the other hand, in order for a cable operator to enjoy the benefits of the safe harbor provisions under the DMCA, the cable operator must affirmatively disclose such personal information to a third party, the copyright owner, without the subscriber's consent.

B. Because Directly Conflicting Statutes Can Not Be Reconciled the More Restrictive Statute Should Be Applied.

Courts have faced the question of how the strict prohibitions under the Cable Act should operate when such provisions directly conflict with another federal statute. Another statute governing access to information used in the provision of online communications, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701, *et seq*., imposes certain duties on cable operators that provide Internet services. While the Cable Act governs the production of records

pertaining to cable services, the ECPA generally governs the interception and production of records and communications generated by subscribers of Internet services.

Until 2001, however, these statutes provided inconsistent and conflicting procedures regarding the manner in which the government could obtain records of cable subscribers receiving both cable and Internet service. By way of example, governmental entities (such as the FBI or local law enforcement agencies) often serve cable providers with subpoenas seeking information about Internet access subscribers. Although the ECPA allows for disclosures to the government in such circumstances, the Cable Act previously did not; it allowed disclosure only pursuant to a court order and continues to do so for civil cases. In addition, the Cable Act would have required advance notice to the cable Internet subscriber, while the ECPA does not. Thus, cable providers were unsure of how to respond to governmental requests for information when the government had not secured a court order. A number of federal courts have recognized that these two statutes imposed conflicting obligations on cable operators. *See United States v. Kennedy,* 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000) (noting that

statutory conflict was an issue of first impression); and *In re United States for an Order Pursuant to 18 U.S.C. 2703(d)*, 36 F. Supp. 2d 430 (D. Mass. 1999)(recognizing statutory conflict but dismissing case due to lack of ripeness).

This conflict was resolved only after Congress recognized the problems raised by imposing diametrically conflicting obligations on cable operators. Thus, in 2001 Congress amended the Cable Act, via the USA PATRIOT Act,[5] to resolve this conflict between the Cable Act and the ECPA. Congress resolved this conflict by allowing cable Internet providers to share their subscribers' personally identifiable information and other records not only upon receipt of a court order, but also in response to subpoenas and search warrants on behalf of law enforcement and governmental agencies.[6] Civil cases, however, are still governed by the Cable Act's restrictions on disclosure.

---

[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56 (October 26, 2001).

[6] *See* 47 U.S.C. § 551(c)(2)(D); 18 U.S.C. § 2703(c).

In other circumstances, where Congress has not reconciled conflicting obligations on cable operators, courts have found that the obligations imposed by the Cable Act should control. For example, in *United States v. Cox Cable Communications*, 1998 WL 656574 (N.D. Fla. 1998), a federal district court faced the question of whether a cable operator served with a summons issued pursuant to the summons authority of the Internal Revenue Service ("IRS") could be forced to reveal subscriber information in contravention of the prohibition under § 551(c). In analyzing the conflicting duties imposed on the cable operator the court noted that the general rule in a summons enforcement proceeding is that "the [IRS's] summons authority should be upheld absent express statutory prohibition [or] unambiguous directions from Congress." *Id*. at 3. However, noting that the plain language of § 551 contains no exclusionary provision the court found that the Cable Act was the controlling authority.[7] *Id*. *See also, United States v. Comcast Cable Communications, Inc*., No. 3:03-0553 (M.D.

[7] The court later considered the information sought under the test established under § 551 and concluded that the IRS was entitled to the information because it had satisfied that test. *Id*.

Tenn. Aug. 4, 2003) (denying motion to enforce IRS summons after finding that information sought in summons was personally identifiable information subject to § 551).

This approach is consistent with the approach preferred by Congress. The legislative history of ECPA clearly indicates that Congress intended that if ECPA's disclosure provisions conflict with more restrictive provisions in another statute, the more restrictive statute should control:

> The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances, however, in which a person or entity both acts a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

H.R. REP. NO. 99-647 at 65 (1986). This approach should guide the resolution of the conflict between the DMCA and the (more restrictive) Cable Act as well.

Charter provides both electronic communications service (Internet service) and cable television programming service. In its role as a provider of cable television programming, Charter is prohibited under the Cable Act from disclosing personally identifiable information about its cable television subscribers to a governmental entity without a court order or consent of the subscriber. In its role as an Internet service provider Charter is subject to the subpoena process under the DMCA. Given that Charter operates as a "combined entity" and is not allowed to disclose personal information as a cable operator entity, the appropriate outcome, as described by Congress, is to find that Charter is not required to disclose such information.

Any other interpretation of these two statutes would render the Cable Act's privacy protections superfluous. Courts repeatedly have held that statutes must be construed so as to give meaning to the entire statute and to avoid rendering particular language superfluous. *See United States v. Menache*, 348 U.S. 528, 538 (1995)(holding that "it is our duty to give effect, if possible, to every clause and word of a statute"); *National Insulation Transp. Comm. v. I.C.C.*, 683 F.2d 533, 537 (D.C. Cir. 1982)("[s]tatutes will not be interpreted as though

Congress enacted superfluous provisions."); *Burrey v. Pacific Gas & Elec. Co*., 159 F.3d 388, 394 (9th Cir. 1998) ("[i]n interpreting a statutory provision, we must avoid any construction that renders some of its language superfluous.")

Had Congress intended to require cable operators to disclose subscriber information to copyright owners in *all* circumstances, even to private parties like the RIAA when the subscriber at issue is a cable television subscriber, it would have so stated when it enacted the DMCA. Instead, Congress amended § 551 via the USA PATRIOT Act, to work ***in conjunction*** with ECPA so that cable operators providing cable modem and cable telephony services would be on an equal footing with other Internet and telephone providers when responding to subpoenas from law enforcement or governmental agencies. Short of a similar amendment governing civil subpoenas to ensure that § 551 works in conjunction with the DMCA as well, this court should not force Charter to engage in unlawful activity under the Cable Act by forcing it to reveal the subscriber information sought by the RIAA.

C. Because There Is No Valid Case or Controversy, The "Court Order Exception" Under 47 U.S.C. § 551(c)(2)(B) Does Not Operate To Allow The Disclosure Of Personal Information

Sections 551(b) and (c) of the Cable Act broadly prohibit the use or disclosure of a subscriber's personally identifiable information without the prior written or electronic consent of the subscriber. 47 U.S.C. § 551(b)(1), (c)(1). Section 551 does, however, include several exceptions to the broad prohibition against disclosure of personally identifiable information. One exception allows a cable operator to disclose personally identifiable information if the disclosure is "made pursuant to a court order authorizing such disclosure . . ." 47 U.S.C. § 551(c)(2)(B). On its face, this exception would seem to satisfy the circumstances surrounding the RIAA's attempts to enforce the subpoenas at issues in this proceeding. However, at the time this "court order" exception was enacted in the cable privacy provisions, there were no clerk-issued subpoenas and no proceedings based on speculation, only legitimate, court-filed civil and criminal suits. Congress was careful when amending the cable privacy provisions by way of the Patriot Act to keep the treatment for civil suits the same and not relax disclosure conditions as it did for ECPA and other governmental

disclosures. There has been no indication, in the legislative history or otherwise, that Congress intended to open a civil loophole for disclosing subscriber information pursuant to clerk-issued subpoenas based entirely on speculation and unverifiable factual allegations.

Accordingly, the Cable Act's "court order" exception should not be construed as operative where, as here, there is no underlying case or controversy within the meaning of Article III. The existence of a valid Article III case or controversy serves to establish the requisite jurisdictional basis for federal courts to exercise their authority, including the power to issue subpoenas. *See Catholic Conference*, 487 U.S. at 76; *Houston Business Journal*, 86 F.3d at 1213.

Absent a valid case or controversy the court lacks the necessary jurisdictional basis to enforce a subpoena requesting such information. Thus, Congress clearly expected that the court order exception under § 551(c)(2)(B) would apply *only* where there existed a valid case or controversy, such that the court had full jurisdiction over the matter.

However, as set forth in Part II, there is no valid case or controversy within the meaning of Article III. The RIAA has not filed suit against any subscriber, nor has the RIAA attempted to invoke this court's

subject matter jurisdiction. *Accord*, *In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d at 257, n. 12, *rev'd on other grounds,* 351 F.3d 1229 (D.C. Cir., Dec. 19, 2003)("at the time of issuance, a § 512(h) subpoena will not necessarily be tethered to a present or even anticipated 'adversary proceeding, involving a real, not a hypothetical, controversy'").

The court order exception under the Cable Act, § 551(c)(2)(B), can not be satisfied in this instance, and any order forcing Charter to disclose subscribers' personal information would result in a direct violation of § 551(c).

IV.

Section 512(h) Violates The First Amendment Rights Of Internet Users

Yet another problem the court must confront if it disagrees with the D.C. Circuit's decision in *Verizon* is whether the statutory procedure violates the First Amendment rights of Charter subscribers. The RIAA argues that the court must assume – based solely upon the assurances of an interested party, the RIAA itself – that Charter subscribers whose IP addresses have been identified have in fact infringed upon RIAA members' copyrights.

There are, however, many legal uses of the material that might have been made by the subscribers. For example, a federal district court recently held that distribution of the KaZaA software did not constitute contributory or vicarious copyright infringement precisely because there are many proper uses for this file-sharing technology. *Metro-Goldwyn-Mayer Studios v. Grokster, Ltd.*, No. CV01-08541, 2003 WL 1989129, *5 (C.D. Cal. April 25, 2003).

There is no First Amendment right to engage in copyright infringement and Charter does not claim that there is. On the other hand, at the time the subpoenas are issued, there has been no determination – judicial or otherwise – that anyone has infringed any copyright. Indeed, there could be no such determination because there is only a suspicion based on filename similarity and no evidence that there was any infringement, or even that the files shared were copyrighted. Because a subpoena may be issued without any foundation beyond speculation, § 512(h) provides no protection for expression that may very well be, following more careful examination in court or otherwise, found to be fully protected.

Because § 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). The Supreme Court has repeatedly "recognized that 'the line between speech unconditionally guaranteed and speech which may legitimately be regulated . . . is finely drawn,' " and thus " '[t]he separation of legitimate from illegitimate speech calls for sensitive tools.' " *Blount*, 400 U.S. at 417 (quoting *Speiser v. Randall*, 357 U.S. 513, 525 (1958)).

Section 512(h) lacks these procedural safeguards. It strips Internet users of their anonymity based upon no more than an *ex parte*, self-proclaimed "good faith" assertion by anyone willing to assert he or she is a copyright owner, or authorized to act on behalf of a copyright owner, that copyright infringement *might* be occurring. *See*

512(c)(3)(A)(v). It does not contemplate any adversarial proceedings before destroying presumptively protected First Amendment rights.

The Supreme Court has repeatedly recognized that "[t]he possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted." *Broadrick v. State of Oklahoma*, 413 U.S. 601, 612 (1973); *see Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 254-55 (2002).[8]

---

[8] With respect to subpoenas for the identity of anonymous Internet users who have been alleged to have defamed others or committed other content-based misconduct, courts have carefully scrutinized the subpoenas to insure that they are proper and not abusive. *Doe v. 2TheMart.Com,* 140 F.Supp.2d 1088, 1092, 1097 (D.Wash. 2001) ("discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts"; recognizing chilling effect if Internet anonymity can be easily stripped away; "the constitutional rights of Internet users, including the 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 "legitimate and valuable right to participate in online forums anonymously or pseudonymously"); *Dendrite International Inc. v. Doe*, 29 Media L. Rptr. 2265 (N.J. Super Ct. July 11, 2001) (denying limited discovery to determine identities of four individuals who posted online messages about a software company using anonymous handles); *Melvin v. Doe*, 29 Media L. Rptr. 1065 (Pa. Ct. Common Pleas, Allegheny Cty., Nov. 15, 2000) (to uncover identity of Internet posters, plaintiffs must make a preliminary showing of the merit of the case; even after plaintiffs meet this burden, confidentiality order may be required). It

There is another alternative that would ensure identification and punishment of most, if not all, of the unprotected speech RIAA wishes to reach: The RIAA's member whose copyright is at issue can file a John Doe lawsuit against the alleged infringer. Or, if what RIAA wants to do is simply "send a warning," it can continue to do so through the very warning campaign it instituted in April, *see* Amy Harmon, *Music Swappers Get a Message on PC Screens: Stop It Now*, N.Y. Times, Apr. 30, 2003, at C1 (describing RIAA's messaging campaign "which seek[s] to turn a chat feature in popular file-trading software to the industry's benefit"). In this situation, as in all situations where First Amendment rights are implicated, courts should require that litigants use less restrictive and invasive means of pursuing their objectives. Accordingly,

---

makes little sense for courts to carefully safeguard the anonymity of Internet users by close scrutiny of subpoenas in one context – alleged content-based misuse – while permitting automatic breach of Internet anonymity without *any* judicial supervision in another context, of alleged copyright infringement. If the interests in protecting anonymity deserve strong judicial protection in the case of content-based misconduct, they certainly are entitled to *some* judicial protection – something more than a requirement to obtain a clerk's rubber stamp – in the context here.

issuance and enforcement of subpoenas for the identity of an ISP's P2P file sharing customers under § 512(h) cannot satisfy the narrow tailoring requirement of the First Amendment. *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 373 (2002).

V.

E-Mail Addresses Are Contact Information Outside The Scope Of "Information Sufficient To Identify" Subscribers

The subpoena provision of the DMCA does not require disclosure of all "contact" information; rather, it states that only "information *sufficient to identify*" the subscriber may be obtained. 17 U.S.C. § 512(h)(3) (emphasis added). The district court agreed with Charter that the RIAA did not need telephone numbers to identify the subscribers, but held that Charter must provide its subscribers' e-mail address. *See* SA 316A. However, giving up the subscribers' names and mailing or street addresses "identifies" them for purposes of § 512(h)(3), and that is all the district court should have ordered.

Section 512(b)(3) contrasts sharply with § 512(c)(3)(A)(iv), which deals with information that a copyright owner must provide to a service provider. The latter requires "[i]nformation sufficient to permit the service provider to contact the complaining party, such as an address,

telephone number, and, if available, *an electronic mail address*." (emphasis added). Similarly, still other portions of the DMCA – those setting forth the "counter notification" procedure – explicitly require that a counter-notification from a subscriber provide: "The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located. . . ." 17 U.S.C. § 512(g)(3)(D).

Congress' choice not to include or "electronic mail addresses" in the subpoena provision clearly indicates that Congress did not intend to require ISPs to disclose e-mail addresses in response to subpoenas. The only reason that copyright holders are permitted to obtain any information from an ISP is that the identity of a subscriber cannot be ascertained from the IP address alone. Conversely, once a copyright holder has obtained a name and mailing or street address through a proper DMCA subpoena, then the copyright holder may avail itself of ordinary methods to obtain a telephone number or e-mail address if it so desires. Even if all the RIAA wants to do is "contact" the alleged infringer, letters will still reliably be delivered to mailing or street

addresses. The DMCA was never designed to transform ISPs into a copyright holder's personal information hotline.

The extent of information disclosed under § 512(h) – that is, how deeply the § 512(h) subpoena intrudes into Internet users' homes – is not inconsequential. Whether it is applied solely to material subject to the § 512(c) notice-and-takedown provisions, or extended as well to P2P activities such as are involved here, the § 512(h) subpoena clearly intrudes into Internet users' lives and activities, without any judicial supervision. The subpoena process is available not only to trade associates like RIAA but also to aggressive and extremist entities that own copyrights and object to others' use (or suspected use) of their copyrighted materials. For example, a political or other group may, on its own bare claim of suspected infringement, learn the identities of its anonymous critics who use that group's materials in their criticism (possibly in ways wholly permissible as fair use). Extremist publishers may use the subpoena power to harass those who critically quote or use their materials. Pornographers, who are copyright owners, may obtain potentially embarrassing information about persons who view or download their photographs. Owners of children-oriented materials like

games may – at least if e-mail addresses are revealed – get direct access to their under-age target customers through these automatic unsupervised subpoenas.

For such an unusual, unsupervised and intrusive tool as a § 512(h) subpoena, courts should strictly adhere to the limited statutory requirement of providing basic identifying information (names and addresses) only. As the district court properly recognized, telephone numbers carry with them a greater expectation of privacy. They also carry a greater potential for abuse, misunderstanding and taking advantage of less sophisticated persons – for example, if a legally sophisticated copyright owner calls an unaware and unsophisticated Internet user, making legal threats and demands. These same considerations apply to e-mail addresses. E-mail addresses, like telephone numbers, are often private and unpublished. Like telephone calls, e-mail messages may catch an Internet user by surprise. A threatening or legalistic e-mail message from a sophisticated copyright owner may prompt an immediate and less than fully considered reply from a teenage P2P user, or even an unsophisticated adult Internet user. Limiting copyright owners to the basic statutory requirement of

sufficient identifying information – names and addresses – will protect Internet users from such misuses of the more intrusive telephone and e-mail means of communications.

That the alleged "illegal conduct" occurs "in cyberspace" is of no moment. All conduct addressed by DMCA subpoenas necessarily must occur in cyberspace; yet Congress chose not to include "electronic mail addresses" as part of the identifying information required to be disclosed, even though Congress explicitly required it elsewhere in the Act.

In short, the district court's enforcement of the subpoenas to require the production of e-mail addresses is an unwarranted invasion of a subscriber's privacy. The Court should limit the information required to be provided to a subscriber's name and mailing or street address.

CONCLUSION

Charter has already produced confidential personal information about its subscribers (including home and e-mail addresses) in compliance with the district court's order. Charter therefore requests that the Court not only reverse the district court's order with directions to grant Charter's Motion to Quash, but also to order the clerk not to

issue any further subpoenas to Charter for the RIAA under § 512(h). Charter further requests the Court to direct the RIAA to return all subpoenaed subscriber data to Charter immediately and to make no further use of such subscriber data.

Charter has a distinct interest in not only protecting its subscribers' privacy at the outset of the subpoena process, but also retrieving personal data that was obtained by an unlawful subpoena or court order. *See, e.g., Church of Scientology of California v. United States*, 506 U.S. 9, 13 (1992) ("Even though it is now too late to prevent, or to provide a fully satisfactory remedy for, the invasion of privacy that occurred . . . a court does have the power to effectuate a partial remedy by ordering the [party that obtained personal records] to destroy or return any and all copies it may have in its possession.")

These instructions are also especially vital because personally identifiable subscriber information is protected under the Communications Act, and Charter is required to notify its subscribers about the nature, frequency, and purpose of any disclosure of such information. *See* 47 U.S.C. § 551. Even if the RIAA has begun to make use of subscriber data provided by Charter, it should not be allowed to

continue doing so, since it is clear, as illustrated by the D.C. Circuit's *Verizon* ruling, that the RIAA had no valid basis under the DMCA to obtain or enforce the subpoenas it served on Charter.

For the foregoing reasons, Charter Communications, Inc. requests the Court to enter its judgment reversing the order of the district court, giving the directions specified above, and granting such other relief as the Court deems proper in the circumstances.

Respectfully submitted,

THOMPSON COBURN LLP

By /s/ Mark Sableman

Stephen B. Higgins
Mark Sableman
James W. Erwin
One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000
FAX 314-552-7000

COLE, RAYWID & BRAVERMAN, LLP
Paul Glist
John D. Seiver
Geoffrey C. Cook
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
Tel: 202-659-9750
Fax: 202-452-0067

Counsel For Appellant Charter Communications, Inc.

Dated: January 15, 2004

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that this brief complies with Fed. R. App. P. 28(d)(2); 28(d)(3); 32(a)(7)(B); 32(a)(5); 32(a)(6); 32(a)(7)(B)(iii). It contains 9,294 words, excluding the parts of the brief exempted; has been prepared in proportionally spaced typeface using Microsoft Word 2000 in 14 pt. Century Schoolbook font; and includes a virus free 3.5" floppy disk in PDF format.

/s/ Mark Sableman

CERTIFICATE OF SERVICE

The undersigned hereby certifies that two copies of Appellant's Brief and one copy of the Separate Appendix were served on this 15th day of January, 2004, in the manner and upon each of the persons indicated below.

(Via Hand Delivery)
K. Lee Marshall, Esq.
Bryan Cave, LLP
One Metropolitan Square
211 North Broadway, Suite 3600
St. Louis, MO 63102

(By Federal Express)
Yvette Molinaro, Esq.
Patricia H. Benson, Esq.
Mitchell Silberberg & Knupp LLP
Trident Center
11977 West Olympic Blvd.
Los Angeles, CA 90064

(By Federal Express)
Thomas J. Perrelli, Esq.
Steven B. Fabrizio, Esq.
Jenner & Block, LLC
601 Thirteenth Street, N.W.
Suite 1200 South
Washington, DC 20005

/s/ Mark Sableman

A D D E N D U M