Appeal No. 03-3802

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

RECORDING INDUSTRY ASSOCIATION OF AMERICA,

Appellee.

v.

CHARTER COMMUNICATIONS, INC.,

Appellant.

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

BRIEF OF APPELLEE

Of Counsel:

Donald B. Verrilli, Jr.
Thomas J. Perrelli
JENNER & BLOCK LLP
601 13th Street, NW
Washington DC 20005
(202) 639-6000

Matthew J. Oppenheim
Stanley Pierre-Louis
RECORDING INDUSTRY ASSOCIATION
OF AMERICA
1330 Connecticut Avenue, NW
Suite 300
Washington, DC 20036

Thomas C. Walsh
K. Lee Marshall
BRYAN CAVE LLP
One Metropolitan Square
211 North Broadway, Suite 3600
St. Louis, MO 63102-2750
(314) 259-2000
(Counsel of Record)

SUMMARY OF THE CASE

Congress enacted the Digital Millennium Copyright Act ("DMCA") to combat the "massive piracy" of copyrighted works on the Internet. S. Rep No. 105-190, at 8, 40 (1998). Section 512(h) of the DMCA authorizes copyright owners to obtain from the clerk of any United States District Court subpoenas directing Internet Service Providers ("ISPs") to provide the identities of copyright infringers who use an ISP's network to disseminate copyrighted materials illegally.

This case involves the kind of massive copyright piracy that Congress enacted the DMCA to combat. The Recording Industry Association of America ("RIAA") served a DMCA subpoena on Charter seeking the identities of 93 of Charter's subscribers who collectively made more than 100,000 copyrighted songs available for illegal copying and downloading.

Oral argument is necessary because this appeal raises important questions of statutory interpretation with far-reaching consequences. Section 512(h) subpoenas are critical to copyright owners' efforts to combat billions of acts of infringement on the Internet. Moreover, this appeal raises several questions of first impression in the courts of appeals. The D.C. Circuit has ruled on one issue in this case, but no federal circuit court has ruled on the others. Accordingly, RIAA believes 30 minutes per side for oral argument is necessary.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, appellee Recording Industry Association of America states that it is a non-profit, trade association acting in this case (pursuant to 17 U.S.C. § 512(h)) as the agent of its members, Universal Music Group, EMI Music North America, Sony Music Entertainment, Inc., BMG Music, and Univision Music, Inc.

Universal Music group is a subsidiary of Vivendi Universal, S.A., which is publicly traded in the United States.

EMI Music North America is a division of EMI Group, PLC, which is publicly traded in the United Kingdom.

Sony Music Entertainment Inc. is a subsidiary of Sony Corporation of America, which is publicly traded in the United States.

BMG Music is a unit of Bertelsmann, Inc. and Bertelsmann AG, neither of which is publicly traded.

Univision Music, Inc. is a subsidiary of Univision Communications, Inc., which is publicly traded in the United States.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS, STATUTES AND RULES

LEGISLATIVE MATERIALS

MISCELLANEOUS

JURISDICTIONAL STATEMENT

The district court had jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337 and 1338, and 17 U.S.C. § 512(h). The decision under review is a final disposition of a subpoena enforcement proceeding and is properly appealed pursuant to 28 U.S.C. § 1291.

STATEMENT OF ISSUES PRESENTED

1. Whether 17 U.S.C. § 512(h) requires an ISP to respond to DMCA subpoenas, regardless of the function the ISP is performing, as the statutory text, structure, purpose and legislative history dictate.

· 17 U.S.C. § 512.

2. Whether § 512, which requires ISPs to comply with DMCA subpoenas "notwithstanding any other provision of law," supersedes potentially inconsistent, previously enacted provisions of the Cable Act.

· *Cisneros v. Alpine Ridge Group*, 508 U.S. 10 (1993).

· 17 U.S.C. § 512(h)(5).

3. Whether Article III of the Constitution prevents a district court clerk from issuing a subpoena pursuant to express congressional authorization under § 512(h), where the copyright owner can use subpoenaed information only to protect its copyrights, and where the copyright holder and the ISP are adverse parties with a live controversy when the clerk issues, and when the court is asked to enforce, the subpoena.

· *ICC v. Brimson*, 154 U.S. 447 (1894).

· *Morrison v. Olson*, 487 U.S. 654 (1988).

· U.S. Constitution, Article III.

4. Whether § 512(h) violates the First Amendment, notwithstanding (1) there is no free speech interest in stealing copyrighted sounds recordings anonymously; (2) § 512(h) neither suppresses nor regulates constitutionally protected speech in any respect; and (3) the DMCA incorporates multiple procedural protections to prevent the chilling of speech.

· *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539 (1985).

· *Smith v. Maryland*, 442 U.S. 735 (1979).

· *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186 (1946).

5. Whether § 512 authorizes disclosure of a copyright infringer's e-mail address.

· 17 U.S.C. § 512(h).

STATEMENT OF THE CASE

In June and July of 2003, the Recording Industry Association of America ("RIAA") discovered 93 individuals illegally disseminating more than 100,000 copyrighted sound recordings over Charter's cable broadband network. 309A. RIAA ascertained the Internet Protocol ("IP") address and screen name of the copyright infringers, the date and time at which they engaged in unlawful conduct, and the particular sound recordings they were unlawfully disseminating. *See, e.g.*, 104-05A. RIAA could not, however, determine the infringers' identities. Only an Internet Service Provider ("ISP") – Charter, in this case – knows the identities of subscribers at specific IP addresses because the ISP assigns IP addresses to subscribers and maintains logs documenting those assignments.

To ascertain the identities of the infringers, RIAA invoked § 512 of the Digital Millennium Copyright Act ("DMCA"). Section 512(h) authorizes "a copyright owner or a person authorized to act on the owner's behalf [to] request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer." 17 U.S.C. § 512(h)(1). RIAA obtained a subpoena requiring Charter to disclose the identities of the 93 infringers. Charter moved to quash. Following briefing and argument, the district court ordered Charter to provide the names, home addresses, and e-mail addresses of the subscribers. Charter complied and filed this appeal.

STATEMENT OF FACTS

A. The Internet and Digital Piracy

Copyright piracy on the Internet has reached epidemic proportions. Armed with a personal computer and a telephone line, an individual can unlawfully disseminate copyrighted works (such as music, movies or software) to millions of people.[1] As the Copyright Office explained in 1997, "a disgruntled former employee, a dissatisfied customer, [or] an Internet user opposed to the fundamental concepts of copyright law" can inflict "tremendous damage to the market for a copyrighted work." *Copyright Piracy and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 8, 9 (Sept. 11, 1997) (Marybeth Peters, Register of Copyrights).

This problem is not new. Two decades ago, even before the development of the World Wide Web, the Internet offered numerous options for copyright piracy. As early as the 1980s, Internet users were "posting" copyrighted works on electronic bulletin boards ("BBSs"); other Internet users would then copy and

[1] Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring over the Internet*, 18 Hastings Comm. & Ent. L.J. 729, 737 (Summer 1996) ("[I]n a matter of seconds and at a cost of mere pennies," a copyrighted work can be transmitted "via E-mail to thousands of people.")

download works from the BBS.[2] By the thousands, users transformed their own home computers into BBSs or file transfer protocol ("FTP") sites[3] from which others could download copyrighted material. Internet users also directly exchanged copyrighted works by e-mail[4] or Internet Relay Chat ("IRC").[5] In addition to allowing inexpensive and broad dissemination of copyrighted works, these technologies offered another advantage to copyright infringers: they could commit infringement anonymously, hidden by a screen name or Internet alias.

Beginning in the early 1990s, copyright owners began suing individuals who unlawfully disseminated copyrighted music, photographs and software. These early suits targeted BBSs operated from computers in people's homes. *E.g., Sega*

---

[2] A BBS allows users to post files for others to download. A BBS requires inexpensive software, a home computer, and a telephone line. *See* T.R. Reid, *Power Computing*, Wash. Post, Dec. 2, 1991, at F18 ("If you have a telephone, a personal computer and about $100 to cover start-up costs, you can broadcast to a national audience as early as tomorrow by going on-line with your own BBS").

[3] FTP software turns any computer into a server from which others can download files. *See* Andrew Leonard, *Mutiny on the Net*, Salon, March 1998, *available at* http://archive.salon.com/21st/feature/1998/03/cov_20feature.html (FTP software "allows anyone with a computer and a modem to make [pirated music] files on their home computer accessible to the rest of the Net").

[4] *See* Kenneth D. Suzan, *Tapping to the Beat of a Digital Drummer: Fine Tuning U.S. Copyright Law for Music Distribution on the Internet*, 59 Alb. L. Rev. 789, 807 (1995) ("It is quite feasible for someone to download a song from a commercial site such as CompuServe and then e-mail or post the 'digitized audio file' on a bulletin board for others to copy. In essence, 'there is no way to ensure a teen-ager who buys a new record will not send it to 1,000 of her closest friends.'").

[5] IRC allows direct communication among users, without posting information on a server. IRC users directly exchange copyrighted files. *See* Andy Patrizio, *Cyberchatters Trade Electronic Booty*, CMP TechWeb, Dec. 30, 1998.

Enters. Ltd. v. MAPHIA, 857 F. Supp. 679, 682-83 (N.D. Cal. 1994) (copyrighted video games distributed by BBS "run from [the infringer's] residence where the computer and memory comprising the bulletin board [were] located"); *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1555-56 (M.D. Fla. 1993) (BBS operated from home computer). In other cases, copyright owners sued both the person running the home BBS and the ISP that linked the BBS to the Internet. *E.g., Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). As early as 1993, the Department of Justice prosecuted Internet infringers, including "hobbyists" who offered pirated software from home BBSs. *E.g., United States v. Stowe*, No. 96C2702, 1996 WL 467238, at *1 (N.D. Ill. Aug. 15, 1996).[6]

Despite these efforts, digital piracy continued to grow as improvements in digital technology made piracy easier. In 1998, a new compressed digital format – mp3 – became the medium of choice for infringers. *See* Benny Evangelista, *Download That Tune*, S.F. Chron., Dec. 3, 1998, at A1 ("copying, trading by e-mail, and posting songs in the MP3 format is one of the fastest-growing phenomena on the World Wide Web"). By 1998, approximately 3 million sound

[6] *See also Third Largest BBS in US Hit in FBI Raid*, Newsbyte, Feb. 19, 1993 (describing raid of home BBS utilizing 125 computers and causing millions of dollars in copyright theft).

recordings were downloaded from the Internet every day, the vast majority of which were pirated. *See The Music Industry*, The Economist, Oct. 31, 1998, at 67.

B. The Congressional Record

Congress took up the issue of digital piracy repeatedly throughout the 1990s. In so doing, Congress sought to balance the interests of two groups: 1) copyright owners suffering from piracy committed by anonymous infringers,[7] and 2) ISPs fearing liability for copyright infringement committed by their subscribers.[8]

Congress amassed an enormous legislative record related to Internet piracy. That record documented piracy by ISP subscribers, based on technologies in wide use by the mid-1990s, using their home computers to make infringing material directly available to other Internet users. The Department of Justice testified about infringement committed from FTP and BBS sites run on home computers. *See Copyright Pirac, and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 17-18 (Sept. 11, 1997) (Kevin DiGregory, Deputy

---

[7] *See The Copyright Infringement Liability of Online and Internet Service Providers*: *Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 15 (Sept. 4, 1997) (Cary Sherman, General Counsel, RIAA).

[8] *See, e.g., The Copyright Infringement Liability of Online and Internet Service Providers*: *Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 32 (Sept. 4, 1997) (Roy Neel, President, United States Telephone Association) (claiming that copyright owners should sue direct infringers transmitting copyrighted materials, not the ISPs themselves); *id.* at 102 (George Vradenburg, General Counsel, America Online, Inc.) (claiming that such liability would "wreak havoc" on ISPs).

Assistant Attorney General, Department of Justice) ("DiGregory Testimony"). ISP witnesses testified about the *Sega, Playboy* and *Netcom* cases – all of which involved infringing activity on home computers linked by ISPs to the Internet – because they feared liability for merely transmitting information from one infringing user to another.[9] Congress also heard testimony about the "growing use of 'blanket' e-mail messages" to commit copyright infringement and about infringers using e-mail (and attachments) to disseminate hundreds of copyrighted software programs – which likewise involved transmissions from one home computer to another.[10] One songwriter explained that e-mail distribution systems were difficult to police because ISPs had no obligation to reveal the identities of e-mail customers, absent a court order.[11]

---

[9] *See, e.g.*, S. Rep. No. 105-190 at 19 n.20 (1998) (noting *Netcom* and *Playboy*); *The Copyright Infringement Liability of Online and Internet Service Providers*: *Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 101-03 (Sept. 4, 1997) (Vradenburg) (discussing *Netcom* and *Sega*).

[10] *Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 172, 175 (Sept. 16-17, 1997) (Ronald Dunn, President, the Information Industry Association); *NII Copyright Protection Act of 1995 (Part 2): Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 84, 88 (Feb. 7-8, 1996) (Garry L. McDaniels on behalf of the Software Publishers Association); *see* DiGregory Testimony, at 17-18 (describing use of e-mail to commit infringement of software programs).

[11] *See Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 160 (Sept. 16-17, 1997) (Allee Willis, songwriter).

By 1998, Congress was thus aware that ISP subscribers were storing infringing material on their home computers and using an ISP as a conduit to transmit that material to others. Indeed, in 1996 one ISP proposed to Congress that ISPs should be required, "[i]n those cases where the allegedly infringing content is not on facilities controlled by the [ISP], . . . [to] take[] reasonable steps to assist the copyright owner in identifying the party that does control the hosting facility (upon receipt of a subpoena if necessary)." *NII Copyright Protection Act of 1995: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 261 (Feb. 7-8, 1996) (Stephen Heaton, General Counsel, Compuserve).

C. The DMCA

In 1998, based on this extensive legislative record, Congress enacted the DMCA. In Title II of the DMCA, 17 U.S.C. § 512, Congress responded to the principal concerns that copyright owners and ISPs had documented. Section 512 has two principal goals: to encourage the development of the Internet by addressing ISPs' fear of liability for infringement committed by users of their networks, and to assist copyright owners in stopping the "massive piracy" of copyrighted works occurring over the Internet. S. Rep. No. 105-190, at 8 (1998) ("S. Rep."). To those ends, Congress created a balanced system of "strong incentives for service providers and copyright owners to cooperate to detect and

deal with copyright infringements that take place in the digital networked environment." *Id*. at 40. In § 512, Congress gave ISPs new protections that limit their liability for their subscribers' infringement. In exchange, Congress imposed obligations on ISPs to assist copyright owners in combating such infringement.

The protections given to ISPs are set forth in subsections (a)-(d) of § 512, which establish four distinct limitations on liability for copyright infringement. Each limitation applies to a particular ISP function. Subsection (a) limits the liability of ISPs that transmit infringing material – that is, when the ISP is a mere conduit. Subsections (b), (c), and (d) limit the liability of ISPs when they are caching, storing, or linking to infringing material. §§ 512(b) (caching), 512(c) (storing), 512(d) (linking).

These protections are conditional. To qualify for *any* of them, an ISP must maintain and enforce a policy of terminating the accounts of subscribers who are "repeat infringers." § 512(i)(1)(A). To retain the limitations in subsections (b)-(d) (which cover storage functions), an ISP must also promptly remove or disable access to infringing material upon receiving a notification of infringement. The DMCA does not, however, require an ISP to take any of these steps; rather, failure to do so results in the loss of the limitations on liability.

In addition, in § 512(h) Congress imposed on ISPs a separate obligation to disclose to copyright owners the identity of subscribers using their networks to

infringe. A copyright owner or its agent may request that "the clerk of any United States district court" issue a subpoena requiring an ISP to disclose the identity of such infringers when the copyright owner comes forward with good faith claims of infringement. § 512(h)(1). To obtain a subpoena, a copyright owner must provide three things: a form subpoena, a sworn declaration that "the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title," § 512(h)(2)(C), and a copy of a notification to the ISP described in § 512(c)(3)(A). The notification establishes the bona fides of the copyright owner's request and provides information sufficient for the ISP to identify the infringer.

The obligation Congress imposed in § 512(h) is distinct from, and in no way dependent upon, an ISP's conditional obligations under §§ 512(a)-(d). Unlike §§ 512(a)-(d), nothing in § 512(h) requires an ISP to remove or disable access to infringing material upon receiving a subpoena and accompanying notification. Nor does § 512(h) require an ISP to terminate the account of a subscriber specified in such a subpoena and notification. An ISP's sole obligation under § 512(h) is to disclose the identity of infringing subscribers. That obligation, however, is mandatory and unqualified. Upon receiving a subpoena and notification, the ISP "shall expeditiously disclose" the identities of infringing subscribers. § 512(h)(5). The statute makes it explicit that ISPs must disclose subscribers' identities

"regardless of whether" the ISP believes that a notification also triggers any duty to remove or disable access to infringing material. § 512(h)(5). Moreover, Congress specified that § 512(h) trumps all other laws by requiring ISPs to comply "notwithstanding any other provision of law." *Id*.

Section 512(h) is essential to the balance created by the DMCA. A core premise of § 512 is that copyright owners should seek legal redress in the first instance against direct infringers – and not against the ISPs whose networks the direct infringers use to commit unlawful conduct. Copyright owners cannot do so unless they know the identities of the direct infringers. Section 512(h) provides them with a means to identify infringers, and thus to protect their copyrighted works in the digital era. Without this provision, the DMCA would shield copyright infringement, not prevent it.

D. Peer-to-Peer Piracy

In 1999, the massive piracy that Congress enacted § 512 to combat reached new levels with the emergence of peer-to-peer ("P2P") systems. Napster was the first and most notorious P2P system, until the courts shut it down.[12] *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Others have arisen

[12] Napster merged two types of software that had long been used for copyright piracy. *See* Chris Sherman, *Napster: Copyright Killer or Distribution Hero?*, Online, Nov. 1, 2000 (describing how Napster combined FTP software to allow downloading of material with Internet Relay Chat software to allow direct searches between users' computers).

in Napster's wake including KaZaA, Grokster and iMesh. Like BBS or FTP sites, P2P systems allow users to disseminate files stored on their home computers to other Internet users. Unlike BBS and FTP sites, a P2P system allows users to search directly for desired material on other users' computers without previously knowing where on the Internet the material resides.

P2P piracy is staggering in its scope. Approximately 90% of the content on P2P systems is copyrighted movies, software, images, and music disseminated without authorization. *See, e.g., Napster*, 239 F.3d at 1013. More than *2.6 billion* infringing music files are downloaded each month. Lev Grossman, *It's All Free,* Time, May 5, 2003. This propagation of illegal digital copies over the Internet has devastated the music industry, which is losing billions of dollars in revenue. Music industry retail sales declined 7% in 2000, 10% in 2001 and 11% in 2002. *See* http://www.riaa.com/news/marketingdata/pdf/year_end_2002.pdf.

In contrast, cable ISPs such as Charter can profit handsomely from this illegal conduct. Users of P2P systems drive the demand for broadband services, such as cable modem services, which offer faster speeds for Internet access and downloading. By some estimates, infringers copying files on P2P systems account for more than 50% of the usage of cable broadband networks. 306A.

E. The Subpoenas in this Case

RIAA is a trade association representing record companies that create, manufacture and/or distribute almost all legitimate sound recordings produced and sold in the United States. In June 2003, RIAA announced a nationwide effort to identify and sue individuals committing copyright infringement using P2P systems. At about the same time, RIAA discovered 93 infringers using Charter's network to disseminate copyrighted music without authorization. 309A. RIAA found these individuals by logging onto P2P networks and observing them offering *more than 100,000 copyrighted sound recordings* for downloading. 306-07A; 309-10A. To ensure that these individuals were indeed committing infringement, RIAA downloaded files offered by each individual and verified that they were illegal copies of copyrighted sound recordings. *Id*.

By observing the infringing P2P activity, RIAA ascertained the IP address and user name (*e.g.*, eddy400@KaZaA) of each infringer, the date and time of their unlawful conduct, and the specific sound recordings they were disseminating. *E.g.*, 104-05A. RIAA could not, however, determine the infringers' identities. That information was available only to Charter, which maintains logs documenting which subscribers use which IP addresses.

Pursuant to § 512(h), RIAA obtained a subpoena from the clerk of the District Court for the Eastern District of Missouri requiring Charter to identify the

93 infringers (and later obtained additional subpoenas relating to additional infringers). 310A. On October 3, 2003, Charter filed a motion to quash. 290A. Charter notified the 93 subscribers of the subpoenas. None intervened or moved to quash the subpoenas.

On November 17, 2003, the district court denied Charter's motion, and ordered Charter to provide RIAA with the names, home addresses, and e-mail addresses of the subscribers. 316A. This Court denied Charter's request for a stay. Charter complied with the district court's order, and filed this appeal.

SUMMARY OF ARGUMENT

I. Section 512(h) of the DMCA requires ISPs to identify subscribers who commit infringement by transmitting material on an ISP's network, and not merely subscribers who store infringing material on the network.

The plain text of § 512(h) compels that result. By its terms, § 512(h) requires all service providers to respond to subpoenas seeking the identity of infringing subscribers. As used in § 512(h), "service provider" is a defined term that expressly covers ISPs providing all functions, including mere transmission. § 512(k)(1)(B). No language in § 512(h) limits its application to ISPs that store infringing material. Congress easily could have included such a limitation had it intended one. Congress, however, did the opposite. In § 512(h)(5), Congress made § 512(h) independent of the limitations on liability set forth in §§ 512(a)-(d), and expressly required ISPs to respond to § 512(h) subpoenas irrespective of whether they have other obligations under the statute.

The structure and purposes of § 512 dictate the same result. Congress included § 512(h) in the DMCA to ensure that copyright owners can take action directly against infringing Internet users. Because copyright owners can ascertain the identity of direct infringers only from ISPs, § 512(h) provides copyright owners with the information they need to enforce their rights. Section 512(h) thus

advances both goals of the DMCA – it allows copyright owners to sue infringers directly, rather than pursuing ISPs on a theory of derivative liability.

Indeed, it would make no sense to limit the scope of § 512(h) to ISPs storing infringing material. A subscriber's piracy is equally unlawful whether the subscriber stores infringing material on a home computer or the ISP's network. A copyright owner's injury is the same irrespective of where the material is stored. And the ISP's burden in responding to a § 512(h) is identical in both situations. Limiting the scope of § 512(h) would thus eviscerate the copyright protection scheme Congress created in the DMCA, without any justification.

Charter's contrary interpretation of § 512(h) lacks any foundation in the text or structure of § 512, and is antithetical to Congress's purposes. Drawing on the D.C. Circuit's decision in *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), Charter contends that cross references in § 512(h) to § 512(c)(3)(A) of the DMCA limit the subpoena provision to ISPs storing infringing material. That is a misreading of the statute. Section 512(c)(3)(A) merely sets forth a notification device that serves multiple purposes in § 512. Nothing in that provision limits the scope of § 512(h) to situations where ISPs store infringing material on their networks.

Finally, there is no merit to Charter's suggestion that the 1998 Congress failed to foresee that Internet users might directly exchange files containing

copyrighted works, and therefore failed to draft § 512(h) broadly to cover that practice. It is clear from the face of § 512 that Congress legislated with this problem in mind. Section 512(a) limits ISP liability in this very circumstance. Moreover, the legislative history is replete with testimony of Internet users directly exchanging files containing copyrighted works through technologies widely in use by 1998. *Supra* at 5-10. Given Congress's awareness of this problem in 1998, it is inconceivable that Congress would have inadvertently shielded these forms of Internet piracy. Yet that is exactly what Charter contends Congress did.

II. There is no "conflict" between § 512(h) and the Cable Act. Congress directed ISPs to comply with DMCA subpoenas "notwithstanding any other provision of law." § 512(h)(5). That command supercedes any hypothetical Cable Act obligation Charter may have.

III. Section 512(h) does not violate Article III of the Constitution. Charter's contrary argument erroneously assumes that an Article III "case or controversy" cannot exist unless a complaint has been filed. It has, however, been clear since the time of the Framers that Congress can authorize pre-litigation discovery so long as there exists a controversy cognizable in the federal courts. That is plainly true here. Indeed, § 512(h) establishes a narrow, pre-complaint discovery mechanism, indistinguishable from Fed. R. Civ. P. 27.

Moreover, the issuance of a subpoena – even by a clerk of court – is a ministerial function, not the exercise of Judicial Power. As the Supreme Court established more than a century ago, Congress may authorize issuance of a subpoena, backed by enforcement in federal court, absent a pending case or controversy. *ICC v. Brimson*, 154 U.S. 447 (1894). Consistent with this understanding, Congress has authorized clerks, administrative agencies, and even private parties to issue such subpoenas under a host of federal statutes.

IV. Section 512(h) does not violate the First Amendment. The conduct at issue in this case – copyright infringement – is not speech and thus neither Charter nor its subscribers has any First Amendment interest to assert. Moreover, § 512(h) neither suppresses nor deters protected speech. It merely authorizes disclosure of the business records of an ISP to whom subscribers voluntarily disclose their identities. As the Supreme Court has repeatedly held, there is no expectation of privacy in such information, even where First Amendment interests are at stake.

V. Copyright owners are entitled to obtain a subscriber's e-mail address in response to a DMCA subpoena. The statute's requirement of disclosure of "information sufficient to identify the alleged infringer" encompasses an e-mail address.

ARGUMENT

This Court reviews *de novo* the district court's rulings on questions of statutory interpretation. *Haug v. Bank of Am., N.A.*, 317 F.3d 832, 835 (8th Cir. 2003).

I. SECTION 512(h) APPLIES TO ISPs PERFORMING ALL FUNCTIONS.

The principal issue before this Court is whether § 512(h) obligates ISPs to identify infringing users of their networks in all circumstances or whether § 512(h) applies only when ISPs store infringing material (as Charter contends). In resolving that issue, "the starting point . . . is the language of the statute itself." *Consumer Prod. Safety Comm'n. v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980). It is, however, a "fundamental principle of statutory construction" that statutory terms should be read in context, not in isolation. *United States v. Deal*, 508 U.S. 129, 132 (1993). Most importantly, a court must interpret statutory text "in light of the purposes Congress sought to serve." *In re Windsor on the River Assocs., Ltd.*, 7 F.3d 127, 130 (8th Cir. 1993) (internal quotation omitted).

The text of § 512(h), read in the context of the structure and purposes of § 512 as a whole, establishes beyond doubt that ISPs must respond to § 512(h) subpoenas seeking the identities of infringing subscribers in all circumstances. Nevertheless, Charter – following the D.C. Circuit's recent opinion in *Verizon*, 351 F.3d 1229 – contends that Congress prohibited issuance of § 512(h) subpoenas to

ISPs that do not store infringing material. Charter's interpretation fails at every level. Rather than giving that text its ordinary meaning, Charter mangles the statutory language to reach a result at odds with the text and structure of the DMCA, as well as the intent of Congress. Finally, even if this Court finds the text of § 512(h) ambiguous, the statute's purpose and legislative history compel an interpretation that § 512(h) applies to all ISPs performing all functions. *See Owner-Operator Indep. Drivers Ass'n v. New Prime, Inc.*, 192 F.3d 778, 785 (8th Cir. 1999).

A. Section 512(h) Applies to All ISPs.

Congress crafted § 512(h) broadly to serve the primary aims of the DMCA: enabling copyright owners to sue infringers directly, rather than leaving them with no choice but to bring derivative claims against ISPs. The breadth of § 512(h) is clear on its face. Giving effect to that broad plain meaning is essential to achieve Congress's purposes.

1. On its face, § 512(h) applies to ISPs whether or not they store infringing material.

Entitled "Subpoena to Identify Infringer," § 512(h) authorizes copyright owners to obtain "a subpoena to a service provider for identification of an alleged infringer." § 512(h)(1). By its plain terms, § 512(h) applies to all "service providers." It contains no language limiting its application to ISPs storing infringing material. Nor does it make any reference to particular ISP functions or

to particular kinds of ISPs. As the district court in *Verizon* observed, had Congress wanted to limit § 512(h), it could have directly stated "such a limitation in subsection (h), or stated that subsection (h) does not apply to subsections (a), (b), or (d), or even have placed the subpoena authority itself within subsection (c). But Congress did not do so." *See In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24, 33 (D.D.C. 2003) ("*Verizon I*"), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003).[13]

To the contrary, Congress expressly defined the term "service provider," as used in § 512(h), to encompass all ISPs performing all functions. Section 512 contains two different definitions of "service provider." Subsection (k)(1)(A) defines the term "service provider," *as it is used in § 512(a)*, narrowly to include only ISPs performing the "conduit" function of transmitting information. Subsection (k)(1)(B) defines the term "service provider" broadly for the remainder of § 512, *including subsection (h)*. That definition encompasses any "provider of online service or network access, or operator of facilities therefor," including entities that serve merely as "conduits." *See* H.R. Rep. 105-551(II), at 64 (1998) ("H. Rep.") (§ 512(k)(1)(B) definition "includes, for example, services such as providing Internet access, e-mail, chat room and web page hosting services).[14]

---

[13] The district court in *Verizon I* engaged in a thorough and detailed statutory analysis, reaching the opposite conclusion from the D.C. Circuit.

[14] The district court in *Verizon I* found the fact that Congress defined the term broadly when it is used in subsection (h) as deserving of substantial weight. 240 F. Supp. 2d at 33-34. The D.C. Circuit panel disparaged this argument, apparently

The breadth of § 512(h) contrasts sharply with the narrowly crafted limitations on liability in §§ 512(a)-(d). In those subsections, Congress specified the functions ISPs must perform to qualify for particular limitations on liability. Each subsection contains prefatory language expressly defining a specific ISP function. *E.g.*, § 512(a)(1)-(5); § 512(b)(1)(A)-(C). Moreover, Congress legislated a rule of construction making clear that the function an ISP performs is critical to determining the application of §§ 512(a)-(d). *See* § 512(n); S. Rep. at 55 ("Section 512's limitations on liability are based on functions"). That rule of construction, however, does not apply to § 512(h). S. Rep. at 55 ("Subsection [(n)] establishes a rule of construction applicable to subsections (a) through (d)"). Unlike subsections (a)-(d), therefore, § 512(h) encompasses all ISPs irrespective of the function they perform.

The text of § 512(h) thus compels the interpretation that an ISP must respond to a subpoena whether or not the ISP stores the infringing material.

---

misunderstanding it as an argument that the definition trumped the cross-reference. 351 F.3d at 1236. The point, however, is not that the definition trumps the cross-reference. As will be shown *infra*, the cross-reference does not limit the scope of § 512(h). The point is that Congress took great care in § 512 generally, and in § 512(h) in particular, to define the scope of an ISP's duties. Given that Congress took such care to specify the scope of an ISP's duties in clear and specific terms in each subsection, it is unlikely that Congress would have intended to limit the scope of § 512(h) by a manner so indirect as an oblique cross-reference to a notification provision in § 512(c)(3)(A).

2. Interpreting § 512(h) to apply to ISPs performing all functions is essential to achieving Congress's purposes.

Applying § 512(h) to all ISP functions makes perfect sense and vindicates the purposes of § 512. Section 512(h) enables copyright owners to bring direct actions against infringers. There is no reason to deny copyright owners the right to do so when infringing material is stored on home computers rather than on an ISP's network.[15] Indeed, the nature of the ISP's role – that is, whether the ISP merely transmits or also stores infringing material – is irrelevant when a copyright owner seeks to sue a subscriber directly. The copyright owner suffers the same irreparable harm regardless of whether the subscriber's ISP stores the infringing material. The ISP's burden is no greater in one situation than the other; in either case, the ISP matches the name of the subscriber to the IP address in question. As the district court in *Verizon I* recognized, there is "no sound reason why Congress would enable a copyright owner to obtain identifying information from a service provider storing infringing material on its system, but would not enable a copyright owner to obtain identifying information from a service provider transmitting the material over its system." 240 F. Supp. 2d at 35.

[15] Indeed, copyright owners seeking a DMCA subpoena generally do not know where infringing material is stored – they can determine only the IP address of the infringer and, through that, the ISP to which that address is assigned. *See Verizon I*, 240 F. Supp. 2d at 35.

Section 512(h) differs from §§ 512(a)-(d) in this crucial respect. Subsections (a)-(d) define the scope of ISPs' limitations on liability for their subscribers' infringement. It makes sense to create different limitations of liability depending on the function the ISP provides. On the one hand, ISPs that merely transmit infringing material are not required under § 512(a) to remove such material from their network. On the other hand, ISPs that store infringing material have an obligation under §§ 512(b)-(d) to take action when notified of infringing material on their networks. However sensible they might be in defining the limitations of ISP liability, those distinctions make no sense in the § 512(h) context because § 512(h) is intended to enable copyright owners to sue subscribers directly. The provision has no bearing on the scope of an ISP's potential liability.

Indeed, Charter's interpretation would defeat Congress's purposes by shielding infringers from liability and allowing rampant infringement to continue. Ironically, under Charter's approach, copyright owners could identify infringing ISP subscribers only in situations where the copyright owner already has another remedy under § 512 – removal of the infringing material stored on the ISP's network, *see* §§ 512(b)-(d). Copyright owners would, however, be unable to identify infringers precisely when they most need to, *i.e.*, when the only way to stop infringement is a direct suit against the infringer. Section 512(h) should not

be given a meaning that so gravely undermines the DMCA's expressed goals. *See NLRB v. Lion Oil Co.*, 352 U.S. 282, 288-89 (1957).[16]

Although Charter tries to justify this perverse result, it cannot do so. Charter suggests that Congress limited § 512(h) to situations where ISPs store infringing material to give ISPs a chance to review such material (and evaluate the allegation of infringement) before deciding whether to respond. Charter Br. at 15-17. The statute refutes that suggestion. Section 512(h)(5) imposes a mandatory duty on ISPs to respond to subpoenas seeking the identity of an infringer. ISPs thus have no discretion to decide whether to respond, based on their own evaluation of the alleged infringement or anything else.

Moreover, the DMCA's legislative history reinforces the text. In testimony before Congress, ISPs explained that they cannot evaluate a copyright owner's claim of infringement because they do not know what is copyrighted, do not know whether a work is licensed, and cannot determine the bounds of fair use.[17] ISPs

---

[16] The subpoena power Charter would preserve is of little value. Typically, an ISP storing infringing material on a website or bulletin board does not know the identity of those who send infringing material to be posted on those sites. Only ISPs that provide the initial Internet access know who the infringer (the sender) is. Under Charter's interpretation, copyright owners may subpoena ISPs that cannot identify the infringers, not the ISPs that can.

[17] *E.g.*, *The Copyright Infringement Liability of Online and Internet Service Providers*: *Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 103 (Sept. 4, 1997) ("it is impossible for them to even attempt to determine whether any particular message might contain copyrighted material and, if so, whether it is being used improperly.") (Vradenburg); *NII Copyright Protection Act of 1995:*

did not want the responsibility to review claims of infringement, and Congress enacted a statute that ensured that they did not have to.

Thus, the text and purpose of § 512(h) point to the same conclusion: it applies to ISPs performing all functions, not merely those storing infringing material.

B. The Cross Reference to § 512(c)(3)(A) Contained in § 512(h) Does Not Restrict § 512(h) to ISPs Storing Infringing Material.

Despite the breadth and clarity of § 512(h), Charter nevertheless contends that Congress authorized subpoenas only when an ISP is storing infringing material on its network. Drawing on the D.C. Circuit's analysis in *Verizon*, Charter contends that this limitation on the scope of § 512(h) is dictated by a cross-reference to another provision of the DMCA, § 512(c)(3)(A). That argument is flatly wrong.

At the outset, it is important to understand the circuitous path Charter takes to arrive at its interpretation. Section 512(h) requires a copyright owner seeking a DMCA subpoena to provide "a notification described in subsection (c)(3)(A)." § 512(h)(2). Subsection (c)(3)(A) specifies six items of information copyright owners must provide to notify an ISP that copyright infringement is occurring and

---

Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. 256 (Feb. 7-8, 1996) (Heaton) (first "key principle" – "no copyright analysis").

to allow the ISP to identify the infringer.[18] Charter concedes that a copyright owner seeking the identity of a subscriber using a P2P system can provide all but one of these items. Charter asserts, however, that one such prerequisite can *never* be satisfied – namely, "[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, and information reasonably sufficient to permit the service provider to locate the material." § 512(c)(3)(A)(iii). According to Charter, an "ISP can neither 'remove' nor 'disable access to' the infringing material" when it resides on a subscriber's computer rather than the ISP's network. Charter Br. at 18. For this reason, Charter contends, a copyright owner can never provide an effective § 512(c)(3)(A) notice when infringing material resides on a home computer. Thus, Charter concludes, a copyright owner can never obtain a § 512(h) subpoena in that circumstance.

Charter's reading of the interplay between § 512(h) and § 512(c)(3)(A) is misconceived. Ignoring the structure and purposes of § 512, Charter misinterprets the purpose and effect of the cross-reference to § 512(c)(3)(A) in § 512(h).

[18] Under subsection (c)(3)(A), a copyright owner must provide (i) a signature of a person authorized to act on behalf of a copyright owner; (ii) identification of the copyrighted work(s) claimed to be infringed, or a representative list of works thereof; (iii) identification of the material that is claimed to be infringing and information reasonably sufficient to permit the service provider to locate the material; (iv) information reasonably sufficient to permit the ISP to contact the complaining party; (v) a statement that the complaining party has a good faith belief that the use of the material is infringing; and (vi) a statement that the information in the notice is accurate and, under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.

Moreover, even reading the statutory language in isolation, Charter's argument fails because an ISP plainly can "disable access" to infringing material on a subscriber's home computer.

1. Subsection (c)(3)(A) is not a limitation on § 512(h).

Congress did not intend for the cross-reference to § 512(c)(3)(A) to impose a substantive limit on the scope of § 512(h). As described *supra*, Charter's contention is that a § 512(c)(3)(A) notification cannot be "effective" for purposes of § 512(h) unless the ISP is able to remove or disable access to the material identified in the notification. That is not, however, what the text of § 512(c)(3)(A) actually says. The provision does not require an ISP to remove or disable access to infringing material and does not mention where the infringing material is stored. It merely requires a copyright owner to identify "the material that is claimed to be infringing . . . 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."

The requirement that an ISP remove or disable access to infringing material stored on its network is set forth in an entirely different provision (§ 512(c)(1)(C)), which Congress pointedly did not cross-reference in § 512(h). Thus, the cross-reference to § 512(c)(3)(A) does not establish, directly or indirectly, that an ISP must respond to a subpoena only when it can remove or disable access to

infringing material on its network. To the contrary, § 512(h) requires ISPs to comply with DMCA subpoenas "regardless of whether the service provider responds to the notification" by removing or disabling access to infringing material. § 512(h)(5). In other words, an ISP must respond to a § 512(h) subpoena even if it does not – or cannot – remove or disable access to infringing material. The legislative history likewise makes clear that §512(c)(3)(A) sets forth only "procedures," not substantive limitations. *See* H. Rep. at 55.

Equally to the point, it would make no sense to infer a restriction on the scope of § 512(h) from the cross-reference. The subsection (c)(3)(A) notification device serves a different function under § 512(h) than it does under §§ 512(b)-(d). In subsections (b)-(d), the notification alerts an ISP that infringing material resides on its network, and triggers the ISP's conditional duty to remove the infringing material. Section § 512(h) does not require such steps; it requires only disclosure of information – which an ISP can do whether or not it stores infringing material. For purposes of subsection (h), the notification serves the different function of providing ISPs with sufficient information to comply with the subpoena (*i.e.* by identifying the subscriber) and establishing the bona fides of the copyright owner's infringement claim.

Nor can Charter salvage its argument with the assertion that, for purposes of § 512(c)(3)(A), it can "locate" only material stored on its network. *See* Charter Br.

at 18-19. The IP addresses provided in RIAA's subpoena and accompanying notification were obviously "reasonably sufficient" for Charter to "locate" the home computers of the infringing subscribers. Charter in fact "located" those subscribers, informed them that they were the subject of RIAA subpoenas, and disclosed their identities after this Court denied a stay. Charter's real contention is that it may not, in advance of responding to a subpoena, be able to *review* allegedly infringing material residing on a subscriber's home computer. As demonstrated (*supra* at 12-13, 27-28), however, Charter has no obligation to review allegedly infringing material before responding. To the contrary, Charter must respond irrespective of whether it believes the material is infringing, and irrespective of whether it takes other action against the infringing material or the infringer. § 512(h)(5).

Thus, when the cross-reference to § 512(c)(3)(A) is read as the Supreme Court requires – in context – there is no basis for Charter's contention that it implicitly limits the scope of § 512(h).

2. The plain meaning of the statutory text defeats Charter.

Wholly apart from its inconsistency with the structure and purposes of § 512, Charter's argument fails because Charter has misread the words of § 512(c)(3)(A). Charter claims that subsection (c)(3)(A) may be satisfied only if an ISP *can* "remove" or "disable access" to the infringing material. Congress did

not, however, define "disable access."[19] Where – as here – Congress does not expressly define a statutory term, the text "must be given [its] ordinary meaning." *United States v. Granderson*, 511 U.S. 39, 71 (1994) (internal quotation and citation omitted). Doing so defeats Charter's argument.

As a matter of plain English and common sense, an ISP can "disable access" to material residing on a subscriber's home computer. To "disable" means to "make incapable or ineffective." *Webster's Third New International Dictionary* 642 (1993). As the district court in *Verizon I* concluded, terminating a subscriber's account disables access to infringing material stored on a home computer. 240 F. Supp. 2d at 33 n.5. Thus, although an ISP receiving a § 512(h) is not required to disable access to any material, it undoubtedly *can* do so. By terminating the account, the ISP cuts the connection between the Internet and the subscriber's computer. As a result, other Internet users can no longer gain access to infringing material on that computer. Access to the infringing material is thus rendered ineffective, *i.e*, disabled.

Charter does not appear to dispute that it can disable access in just this manner. Rather, ignoring the requirement that undefined statutory terms be given their ordinary meaning, Charter contends that the term "disable access" must be

[19] Nor does the phrase have a specialized meaning in the legal or computer fields that differs from the phrase's ordinary meaning. *See Community for Creative Non-Violence v. Reid*, 490 U.S. 730, 739-40 (1989); *McDermott Int'l, Inc. v. Wilander*, 498 U.S. 337, 342 (1991).

given a specialized meaning that excludes "terminating a subscriber's account." Invoking the *Verizon* decision, Charter insists that because Congress purportedly used the two phrases to mean different things in another provision of the DMCA (§ 512(j)), they must have mutually exclusive meanings. Charter Br. at 19 (citing 351 F.3d at 1235). Charter thus relies on the canon of construction that different words in a statute are presumed to have different meanings. That canon is, however, inapposite.

Courts have routinely recognized that even distinct statutory terms can have an overlapping or common meaning. *See, e.g., Natural Res. Def. Council, Inc. v. EPA*, 907 F.2d 1146, 1163 (D.C. Cir. 1990) (rejecting argument that terms cannot have overlapping meaning where Congress "d[id] not explicitly indicate that they are to be mutually exclusive"); *Carson Harbor Vill., Ltd. v. Unocal Corp*., 270 F.3d 863, 882 (9th Cir. 2001) (concluding that "there is at least substantial overlap between" two terms and "reject[ing] the interpretation that the difference in the definitions requires us to . . . make the terms mutually exclusive"), *cert. denied*, 535 U.S. 971 (2002); *United States v. Hill*, 79 F.3d 1477, 1482-83 (6th Cir. 1996) (noting that two terms in the same provision "must have different meanings," but concluding nonetheless "that there is considerable overlap between the two terms"). Indeed, as the Supreme Court has said, "Congress . . . is permitted to use synonyms in a statute." *Tyler v. Cain*, 533 U.S. 656, 664 (2001).

Charter, like the D.C. Circuit, reaches the wrong result because it never considers that "disable access" and "terminate" might have overlapping meanings. Section 512 makes clear that Congress intended those terms to have such an overlap. The objective of "disabling access" to infringing material is to prevent the outside world from gaining access to it. Terminating a subscriber's account is one way to do that. In this regard, it is crucial to understand that termination is a *remedy* for the copyright owner to prevent others from gaining access to infringing material (either by accessing the subscriber's computer or receiving a transmission from the subscriber), thus bringing ongoing infringement to a halt. Terminating a subscriber's account is *not* merely a punishment to prevent the infringer from accessing the Internet to surf the World Wide Web. It is, therefore, fully consistent with both the statutory text and structure of § 512, and with Congress's purposes, to recognize that an ISP can disable access to infringing material on a subscriber's computer by terminating the account of that subscriber.

Indeed, it is clear from § 512(j) (the very provision on which Charter and the D.C. Circuit rely) that "disabling access" and "terminating a subscriber's account" have overlapping meanings. Section 512(j) specifies the injunctive relief available against ISPs. The purpose of such injunctions is to "prevent or restrain" copyright infringement. 17 U.S.C. § 502. Pursuant to § 512(j)(1)(A), a copyright owner may obtain an order to "restrain[]" a service provider storing infringing material "from

providing access to infringing material or activity residing at a particular online site" or an order to "restrain[]" such a provider "from providing access to a subscriber . . . by terminating the accounts of the subscriber." § 512(j)(1)(A). Although the two remedies are not wholly congruent, an ISP under an injunction to prevent access to infringing material at an online site would obviously satisfy its obligation by terminating the Internet connection of that "online site." More generally, § 512(j) makes clear that the point of injunctive relief is to disable the access of other Internet users to infringing material (not merely to punish the infringer), that this can be accomplished by terminating the Internet connection of an infringing user, and that this remedy is available when an ISP is engaged solely in the conduit functions covered by § 512(a). § 512(j)(1)(B)(i); § 512(j)(1)(B)(ii).

Charter counters by asserting that terminating a subscriber's account is a "broader sanction" that is not required in this circumstance. Charter Br. at 19 n.1. That is beside the point. Section 512(h) obliges an ISP only to identify infringing subscribers. It does not obligate an ISP receiving a subpoena and accompanying notification to terminate the subscriber whose identity is sought, or to disable access to infringing material. If the infringing material does not reside on the ISP's network, then the notification accompanying the § 512(h) subpoena requires nothing of the ISP beyond responding to the subpoena. Congress made that quite clear in § 512(h)(5), which requires ISPs to respond to subpoenas "regardless of

whether" the ISP otherwise responds to the notification accompanying the subpoena.

Thus, even accepting Charter's flawed statutory premises, the question is *not* whether Charter *must* "disable access" by terminating the subscriber's account, but whether it *is capable of doing so*. Applying a common-sense understanding of "disable access," Charter plainly is capable of doing so. Even read in isolation, therefore, the text of § 512(c)(3)(A) provides no basis for restricting the scope of § 512(h) subpoenas to material stored on the ISP's network. That conclusion is fatal to Charter's position.

C. The Legislative History Demonstrates That Congress Enacted the DMCA to Combat Infringement from Home Computers.

Interpreting the text with its purpose in mind leaves no doubt that § 512(h) applies to all ISP functions, regardless of where infringing material is stored. If, however, the Court finds the text of the DMCA ambiguous, it must nonetheless reject Charter's interpretation, because it conflicts with the purpose of the DMCA and its legislative history. Indeed Charter's interpretation would preclude the use of DMCA subpoenas in the vast majority of situations in which they are needed and in the vast majority of situations discussed in the congressional record.

Seeking to paper over this weakness, Charter (again relying on the D.C. Circuit) suggests that § 512(h) does not cover P2P piracy because the 1998 Congress which enacted the DMCA did not foresee the risk of infringement by ISP

subscribers using their home computers to disseminate infringing material. *See Verizon*, 351 F.3d at 1238 ("the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works"). On this view, the narrow scope of 512(h) is just an unfortunate oversight resulting from Congress's failure to anticipate P2P systems. Charter's argument is, however, both irrelevant and wrong.

To begin with, that Congress did not foresee a particular technology provides no basis for narrowing § 512(h). The circumstances that serve as a catalyst for legislative action "do[] not define the outer limits of [a] statute's coverage." *New York v. FERC*, 535 U.S. 1, 21 (2002). To the contrary, "the fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth." *PGA Tour, Inc. v. Martin*, 532 U.S. 661, 689 (2001) (internal quotations omitted). That principle applies here. At the insistence of ISPs, Congress drafted the DMCA broadly to ensure that it would not be immediately outmoded by changes in technology. *See The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 25-26 (Sept. 4, 1997) (Vradenburg). The DMCA was enacted to establish broad, enduring rules for the future, and thus to avoid the necessity of ongoing legislative revision.

In all events, the DMCA's plain text refutes Charter's contention. Section 512(a) was designed to address situations in which the ISP serves only as a "conduit" for Internet users directly exchanging infringing files. The provision proves in the clearest terms that Congress was aware of ISP subscribers making infringing material available on their home computers and using ISPs merely as conduits. The point of § 512(a) is to limit ISP liability in precisely that circumstance. Similarly, § 512(j)(1)(B) expressly provides for injunctive relief against ISPs to block infringement by subscribers where the ISP is providing only the conduit function described in § 512(a) and where infringing material resides on the subscriber's computer – once again showing that the 1998 Congress was aware of, and legislated against, piracy committed by ISP subscribers from their home computers.

The legislative history further refutes Charter's claim. As discussed above, *see* supra at 5-10, Congress knew in 1998 that FTP sites and BBS services on home computers were engines of copyright piracy, and that such piracy would increase.[20] The cases cited most prominently in hearings and in the House and Senate reports all involved BBS services operated from home computers. *See*

[20] The D.C. Circuit erred in concluding that Congress was concerned only with FTP sites and BBSs *stored* on the systems of ISPs, and with rogue ISPs. 351 F.3d at 1238. *See supra*.

supra. Congress also knew that infringers were exchanging copyrighted works directly through electronic mail. *Id*.

In each of these situations, direct infringers use the conduit facilities of ISPs to disseminate infringing material over the Internet, and only the ISP providing access to the Internet is likely to know the identity of the infringers. Congress therefore knew about, considered at length, and legislated against the very risk that Charter now claims was unforeseen in 1998.

There is thus no reason for failing to interpret § 512(h) in accord with its text as well as Congress's clear purposes.

II. THE DMCA TRUMPS THE CABLE ACT BY REQUIRING ISPs TO COMPLY WITH DMCA SUBPOENAS "NOTWITHSTANDING ANY OTHER PROVISION OF LAW."

Charter next asserts that the DMCA and the Cable Act "impose two directly conflicting burdens on cable operators." Charter Br. at 30. Under 47 U.S.C. § 551(c)(1) of the Cable Act, a cable operator must obtain a subscriber's consent before "disclos[ing] personally identifiable information," whereas under § 512(h), an ISP must disclose such information in response to a DMCA subpoena regardless of the subscriber's consent. Charter, based on a lengthy analogy to an

inapposite statute,[21] asserts that the Cable Act's "more restrictive" requirements override the DMCA. Charter Br. at 30-36.

The plain language of the DMCA – *which Charter never mentions* – resolves the alleged conflict between the statutes. An ISP must comply with a DMCA subpoena "notwithstanding any other provision of law." § 512(h)(5). Such "'notwithstanding' language . . . supersede[s] all other laws." *Cisneros v. Alpine Ridge Group*, 508 U.S. 10, 18 (1993) (internal quotation omitted); *Campbell v. Minneapolis Pub. Hous. Auth. ex rel City of Minneapolis*, 168 F.3d 1069, 1075 (8th Cir. 1999) (concluding that "notwithstanding" language trumps federal and state laws concerning disclosure of medical records); *Liberty Maritime Corp. v. United States*, 928 F.2d 413, 416 (D.C. Cir. 1991) ("a clearer statement" that Congress intended to override other laws "is difficult to imagine") (internal quotation omitted).

The presence of a statutory "notwithstanding" clause "signals that [an act] supersedes other statutes that might interfere with or hinder the attainment" of the act's objectives. *Campbell*, 168 F.3d at 1075. In such situations, the Court "need not consider the appropriate interaction" between statutes. *Id*. The statute containing the "notwithstanding" clause trumps.

---

[21] Charter's detour on the Electronic Communications Privacy Act, 18 U.S.C. § 2701, is irrelevant. That the Patriot Act addressed a potential conflict between ECPA and the Cable Act says nothing about how Congress intended the Cable Act and the DMCA to interact.

Thus, Charter did not "face[] an untenable situation." Charter Br. at 29. The DMCA contains a plain statement that responding to a § 512(h) subpoena is of paramount importance when compared to other obligations that might limit such disclosure by ISPs.[22] Charter therefore was required to comply.

In any event, Charter concedes that the Cable Act, 47 U.S.C. § 551(c)(2)(B), allows disclosure of personal information pursuant to a court order. Charter Br. at 37. Here, the district court entered such an order, thus satisfying the Cable Act. As discussed in Part III, Charter's argument that the district court lacked authority to enter such an order is meritless.

III. THE DMCA DOES NOT VIOLATE ARTICLE III.

Charter's Article III challenge to § 512(h) is meritless.[23] Charter asserts that Article III prohibits Congress from authorizing the issuance of a subpoena unless there is "a case or controversy within the federal court's jurisdiction pending

---

[22] The DMCA was enacted after the Cable Act. If the two statutes conflict, the later-enacted DMCA is controlling. *See Posadas v. National City Bank of New York*, 296 U.S. 497, 503 (1936); *United Family Farmers, Inc. v. Kleppe*, 552 F.2d 823, 825-28 (8th Cir. 1977).

[23] If this Court invalidates § 512(h) for any reason, it would have to invalidate the entirety of §512. Severance is improper if an unconstitutional provision is an integral part of the legislation, as § 512(h) is here. *See Mille Lacs Band of Chippewa Indians v. Minnesota*, 124 F.3d 904, 917-18 (8th Cir. 1997), *aff'd*, 526 U.S. 172 (1999); *Alaska Airlines, Inc. v. Brock*, 480 U.S. 678, 685 (1987) (requiring consideration of "the importance of the [unconstitutional provision] in the original legislative bargain"). If § 512(h) were severed, it would destroy Congress's careful legislative balance. *See MD/DC/DE Broadcasters Ass'n v. FCC*, 253 F.3d 732, 734-36 (D.C. Cir. 2001).

somewhere." Charter Br. at 25. As the district court in *Verizon* held, however, Congress may, consistent with Article III, authorize issuance of subpoenas in advance of the filing of a complaint. *See In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244 (D.D.C. 2003) ("*Verizon II*"), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003).[24]

A. Congress Has the Power to Authorize Pre-Litigation Discovery.

Even if one construes the ministerial issuance of a subpoena by the clerk as an exercise of Judicial Power, § 512(h) raises no conceivable Article III problem. In contending otherwise, Charter confuses the existence of an Article III "case or controversy" with the existence of a pending judicial action. It is plain, however, that the former can exist even if the latter does not. Congress thus has the power to authorize discovery prior to the filing of a complaint with respect to any controversy cognizable in the federal courts. *See Verizon II*, 257 F. Supp. 2d at 252-54. Laws such as Fed. R. Civ. P. 27 and § 512(h) date back to the Framers, and no court has ever suggested they raise constitutional concerns.[25]

---

[24] In a second lengthy and well-reasoned opinion, the district court in *Verizon* rejected Article III and First Amendment arguments identical to those raised by Charter. The D.C. Circuit did not address those issues in its opinion.

[25] *See* Judiciary Act of 1789, 1 Stat. 88, 90; *see also* 18 Rev. Stat. § 866 (1878) (continuing the practice in chancery of allowing certain pre-litigation depositions relating to matters cognizable in federal court). Federal courts sitting in equity frequently sustained "the right to file a bill of discovery to ascertain the proper persons to make defendants in a proposed suit at law." *Brown v. McDonald*, 133

Section 512(h) functions much like Rule 27. Both are preludes to a possible federal court action, but neither requires the filing of a complaint at the time they are invoked or any time thereafter. Under Rule 27, a party must show "a sufficient likelihood that the expected litigation will eventuate." *De Wagenknecht v. Stinnes*, 250 F.2d 414, 417 (D.C. Cir. 1957). Similarly, under § 512(h), the copyright holder must declare, under penalty of perjury, that the information is being sought to protect rights under the copyright laws, *i.e.*, a possible infringement action. If anything, § 512(h) has a more clear nexus with later litigation than does Rule 27. Under § 512(h), a copyright owner must attest to all the elements of a copyright claim – ownership of, or license to, a copyright and violation of its exclusive rights. Although Rule 27 petitions are often filed before the future case is ripe, *see De Wagenknecht*, 250 F.2d at 416-17, § 512(h) subpoenas are sought only after the infringement has occurred.

Indeed, § 512(h) is narrower that Rule 27. Section 512(h) authorizes only subpoenas to identify an infringer. In contrast, Rule 27 authorizes a wide range of discovery, including the production of documents, an inspection of land, and physical examinations. Fed. R. Civ. P. 27(a)(3). Finally, like Rule 27 discovery, § 512(h) subpoenas are critical to the perpetuation of evidence because ISPs

---

F. 897, 898 (3d Cir. 1905); *see* Joseph Story, *Equity Jurisprudence* § 1483, at 811 (13th ed. 1886).

generally maintain the information that copyright owners seek for only a limited period of time. 314A; s*ee Verizon II*, 257 F. Supp. 2d at 254.

Rule 27 and its precursors demonstrate that Congress has authority, consistent with Article III, to authorize discovery prior to the filing of a complaint. At the time a copyright owner seeks a DMCA subpoena, it obviously has a cognizable controversy with a copyright infringer. Article III requires nothing more.

B. Issuance of a § 512(h) Subpoena Does Not Implicate the Judicial Power.

In any event, the issuance of a DMCA subpoena – as distinct from its enforcement – is not the exercise of Judicial Power. Indeed, it has been the law for more than a century that Congress may authorize subpoenas in the exercise of its Article I powers, and that Article III courts can enforce such subpoenas even absent a pending judicial proceeding.

That is the precise holding of *ICC v. Brimson*, 154 U.S. 447 (1894). In *Brimson*, the Supreme Court rejected the claim Charter makes here, holding that Congress had Article I authority to provide for the issuance of subpoenas backed by judicial enforcement even if the subpoenas did not seek evidence for a judicial proceeding, and that Article III courts acted within their "case or controversy" authority in adjudicating disputes over such subpoenas. *Id.* at 478, 485.

Brimson and its progeny recognize that issuance of a subpoena, whether by a clerk, a private party, or an administrative agency, is not itself an exercise of the Judicial Power. *Verizon II*, 257 F. Supp. 2d at 249. Indeed, subpoenas backed by the threat of federal court enforcement are issued every day, in the absence of any pending judicial proceeding, by administrative agencies,[26] clerks or federal courts themselves,[27] and private parties.[28] Federal courts regularly enforce such subpoenas, *see, e.g., In re Arbitration between Security Life Ins. Co. of Am.*, 228 F.3d 865, 870-71 (8th Cir. 2000) (enforcing subpoena issued by private arbitrators), and those provisions have never been thought to raise constitutional concerns.

Charter suggests that such statutes are valid only because a controversy exists "somewhere," even if that "somewhere" is not an Article III *court*. *See* Charter Br. at 25. That concession is fatal to Charter's Article III challenge because, as demonstrated (*infra* at 51), a cognizable controversy exists between a

---

[26] *E.g.*, 29 U.S.C. § 657(b) (granting OSHA the power to issue judicially enforceable subpoenas); 29 U.S.C. § 161(1) (same for NLRB investigating unfair labor practices).

[27] *E.g.*, 35 U.S.C. § 24 (subpoena issued by clerk at behest of private party for patent validity proceeding); 7 U.S.C. § 2354(a) (subpoenas related to Plant Variety Protection Office proceedings); 45 U.S.C. § 157(h) (subpoenas at request of arbitrator under the Railway Labor Act); 28 U.S.C. § 1782(a) (subpoenas in aid of foreign judicial proceedings). Prosecutors routinely issue grand jury subpoenas *ex parte*, absent a "case" or "controversy," and courts enforce those subpoenas.

[28] *E.g.*, 9 U.S.C. § 7 (subpoenas issued by private arbitrators).

copyright owner and a subscriber at the time a § 512(h) subpoena issues. In all events, Charter's purported statement of Article III law is insupportable. Proceedings pending before an administrative agency, an arbitration tribunal, or a foreign court, by definition, do not invoke the exercise of Article III authority. Indeed, subpoenas issued in anticipation of foreign court proceedings under foreign law necessarily involve non-Article III proceedings outside the jurisdiction of the federal courts. *See* 28 U.S.C. § 1782(a); *see In re Letters Rogatory from the First Court of First Instance in Civil Matters, Caracas, Venezuela,* 42 F.3d 308, 310 (5th Cir. 1995) (allowing discovery prior to commencement of foreign proceedings). The statutes discussed above are valid *not* because there is a proceeding pending "somewhere" but because the mere issuance of subpoenas does not constitute the exercise of Judicial Power.[29]

Lacking valid arguments, Charter resorts to misconstruing cases, beginning with *Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792) and *United States v. Ferreira*, 54 U.S. (13 How.) 40 (1851). Charter claims that *Hayburn's Case* invalidated a law requiring judges to take pension applications because it imposed duties "not of a judicial nature." Charter Br. at 26. *Hayburn's Case*, however, stands for the

[29] Under Charter's view, attorneys issuing subpoenas pursuant to Fed. R. Civ. P. 45 are exercising Judicial Power. Yet Charter fails to recognize that virtually all subpoenas are issued without "judicial supervision." In this regard, § 512(h) is no different from other types of subpoenas – they are issued without judicial supervision, and Article III judges act only when a party raises an objection or fails to comply.

irrelevant proposition that a federal court cannot render initial decisions on matters subsequently reviewed and decided by Executive Branch officials – because such initial decisions would be advisory opinions. Indeed, in *Hayburn's Case* the Circuit Court for New York specifically held that the judges could hear pension claims in their individual capacities as commissioners. 2 U.S. at 410.[30]

Charter also cites a series of cases for the proposition that courts lack inherent authority to issue subpoenas. *See* Charter Br. at 27. Those cases, however, lack the feature recognized as dispositive in *Brimson* and present here: express congressional authorization. In *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), the Court rejected the claim that the FTC's investigation of compliance with a judicial decree intruded on the judicial power. The Court noted in *dicta* that federal courts lack *inherent* authority to undertake investigations on their own. That unremarkable proposition has no relevance here because Congress has authorized issuance of subpoenas at the behest of private parties, not at the

[30] The same is true for *Ferreira*. There, a statute required federal judges to decide certain claims subject to revision by other branches of government. The Supreme Court held that the judges' decisions did not constitute the exercise of judicial power. The Court did not, however, invalidate the delegation of authority; rather the Court held that there was no subject matter jurisdiction to consider the judges' actions on appeal. *See Mistretta v. United States*, 488 U.S. 361, 403-04 (1989) (explaining *Ferreira*). The Supreme Court in *Brimson* expressly considered both *Hayburn's Case* and *Ferreira* and concluded that upholding the power of federal courts to enforce subpoenas authorized by Congress outside the context of a judicial case or controversy is "not inconsistent with anything said or decided in those cases." 154 U.S. at 485.

instigation of the judiciary. *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72 (1988), and *Houston Business Journal, Inc. v. Office of Comptroller of Currency*, 86 F.3d 1208 (D.C. Cir. 1996), are also inapposite. In those cases, the *only* source of authority for the subpoena was a pending federal case. Because the court lacked jurisdiction over the underlying dispute, it lacked power to enforce Rule 45 subpoenas.

At bottom, Charter's argument confuses issuance of a subpoena with its subsequent enforcement. The former does not "implicate Article III judicial power" or "involve[] federal judges in an investigation of the sort properly relegated to one of the other branches." *Verizon II*, 257 F. Supp. 2d at 250. The latter is undoubtedly a case or controversy. "In a real-world sense, no Article III judge takes any action with respect to a § 512(h) subpoena until the copyright holder moves to enforce the subpoena or the ISP moves to quash it – at which time there is a concrete controversy sufficient to confer jurisdiction under Article III." *Id*.

C. The Clerk's Issuance of Subpoenas Does Not Violate Article III.

Nor does Congress's delegation of the task of issuing § 512(h) subpoenas to the clerk of court violate Article III. As the Supreme Court has repeatedly held, ministerial actions by the clerk of court do not constitute the exercise of Judicial Power. *E.g., Custiss v. Georgetown & Alexandria Turnpike Co.*, 10 U.S. (6

Cranch) 233 (1810) (Marshall, C.J.); *Elliot v. Lessee of William Peirsol*, 26 U.S. 328 (1828); *Ex parte Virginia*, 100 U.S. 339 (1879); *Central Loan & Trust Co. v. Campbell Comm'n Co.*, 173 U.S. 84 (1899). Indeed, Congress has repeatedly authorized clerks to issue subpoenas in the absence of a pending case or controversy. *See supra* n.27.

Placing the ministerial duty of issuing subpoenas on the clerk does not unlawfully expand the powers of the judiciary, as *amici* contend. *See* SBC Amici Br. at 18. An enactment violates the separation of powers only if it poses an actual "threat of undermining the integrity of the Judicial Branch or of expanding the powers of the Judiciary beyond constitutional bounds by uniting within the Branch the political or quasi-legislative power . . . with the judicial power." *Mistretta*, 488 U.S. at 380-81, 393. Congress may delegate to judicial branch actors a variety of tasks, such as overseeing the independent counsel process, *see Morrison v. Olson*, 487 U.S. 654, 681 n.20 (1988), serving on the sentencing commission, *Mistretta*, or conducting extradition proceedings, *see Lo Duca v. United States*, 93 F.3d 1100 (2d Cir. 1996), without violating Article III. *See Ex Parte Siebold*, 100 U.S. 371 (1879) (rejecting argument that inferior officers appointed by judges can perform only judicial functions); *Morrison*, 487 U.S. at 676 & n.13.

Section 512(h) is no different from these delegations. It does not authorize the judiciary to spearhead an investigation on its own initiative. Rather, issuance

of a DMCA subpoena is a "ministerial" task that requires no exercise of discretion. S. Rep. at 51 (describing issuance of subpoena as a "ministerial function"). Clerks have issued subpoenas under the Federal Rules and pursuant to numerous other statutes for over a century. Assigning the task of issuing DMCA subpoenas to the clerk thus neither undermines nor aggrandizes the authority of the Judiciary.

D. The Dispute Between RIAA and Charter Is a Case or Controversy.

Finally, even if a dispute must be pending "somewhere" at the time a DMCA subpoena is issued, *see* Charter Br. at 27, that requirement is met here. Like other federal statutes, § 512(h) gives copyright owners a federal right to information from ISPs and makes that right enforceable in federal court. *See* 29 U.S.C. § 1132(c)(1) (ERISA); 5 U.S.C. § 552(a) (FOIA). By filing its notification of infringement (rather than a complaint) and a form subpoena (rather than a summons), a copyright holder or its agent asserts its rights in the manner established by Congress. *See Aetna Life Ins. Co. of Hartford v. Haworth*, 300 U.S. 227, 240 (1937) ("Congress is not confined to traditional forms or traditional remedies."). The dispute with Charter over the information is ripe and neither hypothetical nor advisory. The parties are adverse, and the remedy is within the competence of the courts. Thus, there is a "case or controversy" pending at the time the subpoena is issued.

IV. SECTION 512(H) DOES NOT VIOLATE THE FIRST AMENDMENT.

Charter contends that § 512(h) violates the First Amendment by interfering with subscribers' "anonymity." Charter Br. at 39-44. The conduct at issue in this case, however, is theft, not protected expression. Moreover, the Constitution provides no right to prevent disclosure of records pursuant to lawful process. Section 512(h) therefore does not violate the First Amendment.

A. There Is No First Amendment Interest At Stake.

Charter's subscribers have no First Amendment right to steal copyrighted sound recordings, anonymously or otherwise. *See Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555-60 (1985); *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562, 574-78 (1977). Charter's repeated claim that RIAA has provided nothing more than "suspicion" or "speculation" of infringement is demonstrably false. Charter Br. at 18, 40. RIAA does not merely suspect the Charter subscribers whose identities are at issue: RIAA has hard evidence that they have committed copyright infringement. RIAA provided Charter with specific allegations against each infringer. *See* 103-287A. RIAA also provided sworn testimony to the district court describing its evidence against each infringer. That testimony explained that RIAA downloaded and listened to files being disseminated by each of the subscribers, and determined that they were copyrighted sound recordings being disseminated without authorization. *See* 309-

10A. RIAA identified the IP addresses the subscribers were using to commit this infringement, as well as the date and time of the infringement, *see* 103-287A, 309-310A. Moreover, RIAA identified specific copyrighted works that each subscriber was disseminating. *See* 310-11A.

This evidence is undisputed. Charter notified each of the subscribers whose identity is at issue, and each had an opportunity to move to intervene in the district court. None, however, came forward to dispute RIAA's evidence or claim a First Amendment interest.

Because there is no constitutional interest at stake in this case, this Court need look no further to deny Charter's First Amendment challenge.[31]

B. There Is No Right to Anonymity in an ISP's Records.

Even if First Amendment interests were at stake, § 512(h) is constitutional because it neither restricts speech by users of the Internet, nor penalizes them after speaking. By allowing copyright owners to obtain information essential to the vindication of their rights, § 512(h) is no different from Rule 45, grand jury subpoenas, or administrative subpoenas issued without judicial involvement and

[31] Charter has made no effort to meet the heavy burden of establishing an overbreadth claim. *See New York v. Ferber*, 458 U.S. 747, 769 (1982). A court will invalidate a statute only if its overbreadth is "real" and "substantial as well, judged in relation to the statute's plainly legitimate sweep." *Broadrick v. Oklahoma*, 413 U.S. 601, 615 (1973). Charter's and its *amici's* speculation about possible misuse of § 512(h) is plainly insufficient to support an overbreadth challenge. *See Whalen v. Roe*, 429 U.S. 589 (1977).

without notice to potential targets. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 742 (1984) (concluding that the Due Process Clause is not "offended when a federal administrative agency, without notifying a person under investigation, uses its subpoena power to gather evidence adverse to him").

Charter's subscribers have no right to prevent disclosure of information they have provided to Charter. "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435, 442-45 (1976). Just as telephone users forfeit the expectation that the telephone company will conceal records of their calls, *see Smith*, 442 U.S. at 742, and just as Western Union users have no privacy interest in records of their wire transfers, *see In re Grand Jury Proceedings*, 827 F.2d 301, 302-03 (8th Cir. 1987), ISP subscribers have no legitimate expectation that ISPs will conceal their identities in response to legal process. *See Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) ("[C]omputer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person – the system operator."); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507-09 (D. W. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (table).

This is especially true here. As the *Verizon II* court explained, where an ISP subscriber "opens his computer to permit others, through peer-to-peer filesharing,

to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world." 257 F. Supp. 2d at 267; *see also United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (activation of file sharing mechanism shows no expectation of privacy).

Charter's effort to cloak its argument in the First Amendment does not change the result. The Supreme Court has made clear that the assertion of a First Amendment interest does not compel application of a heightened standard prior to compliance with a subpoena. *See Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 192-93, 208-11 (1946); *University of Pa. v. EEOC*, 493 U.S. 182, 199-200 (1990).

C. The DMCA Provides Significant Procedural Protections.

Charter and its *amici* mischaracterize or ignore the significant procedural protections Congress imposed in enacting § 512(h). The DMCA, however, contains far greater procedural protections than are available under Rule 45, which Charter concedes can be used to obtain exactly the same information. *See* Charter Br. at 43 (noting that copyright owners can bring John Doe suits and issue Rule 45 subpoenas).

As the *Verizon II* court found, the DMCA's "subpoena provision contains a number of substantial procedural requirements aimed at preventing abuse, fraud,

and mistakes, without chilling expressive or associational rights." 257 F. Supp. 2d at 270. First, a copyright owner or its agent must possess a "good faith belief" that the use of copyrighted material is unauthorized. § 512(c)(3)(A)(v). Second, the party seeking the subpoena must swear under penalty of perjury that it owns the copyrighted works or is authorized by the copyright owner. § 512(c)(3)(A)(vi). Third, the party must identify the works being infringed and the material claimed to be infringing. § 512(c)(3)(A)(ii)-(iii). Fourth, the party must swear that information "will only be used for the purpose of protecting rights under this title." § 512(h)(2)(C). These measures minimize the risks of mistake and misuse. *See Ingraham v. Wright*, 430 U.S. 651, 678 (1977) (threat of sanction for misuse minimizes risk of erroneous deprivations). Indeed, a copyright owner alleges the equivalent of a prima facie case of copyright infringement prior to obtaining the subpoena. *See Verizon II*, 257 F. Supp. 2d at 270. Moreover, pursuant to a DMCA subpoena, a copyright owner may obtain only limited information. *See infra* Pt. V. Finally, the statute expressly provides for judicial review, if desired, before compliance. *See* § 512(h)(6).

Charter cites several cases to support its view that "courts have carefully scrutinized . . . [non-DMCA] subpoenas to insure that they are proper and not abusive." Charter Br. at 42 n.8. As the district court in *Verizon II* observed with regard to the same cases, the DMCA provides "precisely the type of procedural

requirements other courts have imposed – in non-copyright cases – to compel a service provider to reveal the identity of anonymous Internet users." 257 F. Supp. 2d at 263 n.22. In those few cases, courts looked to whether the information was sought in good faith to prove a claim under federal or state law, was directly related to a claim or defense, and was otherwise unavailable. *See* Charter Br. at 42 n.8. RIAA has more than met those standards in this case.[32]

V. THE DMCA AUTHORIZES DISCLOSURE OF AN INFRINGER'S E-MAIL ADDRESS.

Pursuant to § 512(h)(3), a copyright holder is entitled to "information sufficient to identify the alleged infringer." The district court correctly held that such information includes the subscriber's e-mail address.

Charter concedes that the DMCA authorizes disclosure of names and physical addresses, but claims that it prohibits disclosure of e-mail addresses. Charter Br. at 45-48. Charter, however, points to no text in § 512(h) to support this distinction, relying instead on the fact that § 512(h) does not expressly require disclosure of e-mail addresses. Charter Br. at 45. That argument fails because

[32] The Consumer and Privacy *Amici* argue that § 512(h) violates the Due Process Clause. *See* Consumer and Privacy *Amicus* Br. at 13. This is Charter's First Amendment argument dressed in different clothing. Because the so-called "liberty interest" in anonymous expression is wholly derivative of the right to free speech, the proper constitutional framework is the First Amendment, not the Fifth Amendment. Moreover, the infringers in this case received the very process that *amici* seek – notice that RIAA was seeking their identities and the opportunity to challenge the disclosure. *See* Consumer and Privacy *Amicus* Br. at 17-18.

Congress did not specify *any* particular pieces of information to which a copyright owner is entitled. Rather, Congress used broad language in describing the information that copyright owners may obtain in response to a subpoena.

Charter's argument also ignores the underlying purpose of § 512(h). Congress authorized DMCA subpoenas so that copyright owners can "protect[] rights" under the copyright laws. *See* § 512(h)(2)(C). The statutory right would be hollow if it did not authorize disclosure of sufficient information to contact infringers and demand that they cease infringing. As the district court recognized,

> when you look behind the reason for identifying the alleged infringer, then it's clear that something more than just the name is contemplated. If the purpose of identifying the infringer is to enable a company or organization like the RIAA to contact these individuals and . . . put them on notice. . . what they're doing is wrong and it is a violation of copyright and they better stop or else, or if the purpose is to identify them so they can obtain service of process on them, obviously, an address -- a residence address -- is essential to that purpose. But in today's world, communication is made in a number of different ways; not simply in writing through the U.S. mail.

Appellee's Appendix 57-58.

A subscriber's e-mail address will often be the quickest way to contact infringers. Given "the ease with which digital works can be copied and distributed worldwide virtually instantaneously," S. Rep. at 8, copyright pirates can unlawfully disseminate thousands of sound recordings in a matter of seconds. This infringement constitutes irreparable harm as a matter of law. *See Taylor Corp. v.*

Four Seasons Greetings, LLC, 315 F.3d 1039, 1041-42 (8th Cir. 2003). For that reason, Congress emphasized the need for expedition in the DMCA itself. *E.g.*, § 512(h)(5). Requiring an e-mail address is thus consistent with Congress's intent.

Finally, Charter imagines that "aggressive and extremist entities" might abuse possession of an e-mail address. *See* Charter Br. at 46-48. Possession of an e-mail address is far less intrusive than possession of a street address, which Charter concedes it must disclose. Moreover, Charter again ignores the DMCA's significant procedural safeguards, including the requirement that a copyright owner sign a declaration on penalty of perjury that information obtained can be used only to protect rights under the copyright laws.[33] Such safeguards adequately prevent the sorts of abuses Charter hypothesizes.

In sum, the district court was correct in holding that § 512(h) authorizes disclosure of e-mail addresses.

[33] The SBC *Amici* object to the inclusion of multiple subscribers in a single subpoena. SBC *Amicus* Br. at 23. Charter has not raised this argument and thus the Court cannot consider it.

CONCLUSION

For the foregoing reasons, RIAA respectfully requests that this Court affirm the District Court's order.

Respectfully submitted,

_____

Thomas C. Walsh
K. Lee Marshall
BRYAN CAVE LLP
One Metropolitan Square
211 North Broadway, Suite 3600
St. Louis, MO 63102-2750
(314) 259-2000
(Counsel of Record)

Of Counsel:

Donald B. Verrilli, Jr.
Thomas J. Perrelli
JENNER & BLOCK LLP
601 13th Street, NW
Washington DC 20005
(202) 639-6000

Matthew J. Oppenheim
Stanley Pierre-Louis
RECORDING INDUSTRY ASSOCIATION OF AMERICA
1330 Connecticut Avenue, NW
Suite 300
Washington, DC 20036

Dated: February 24, 2004

CERTIFICATE OF COMPLIANCE

The undersigned certifies that this brief complies with Federal Rules of Appellate Procedure 32(a)(5), 32(a)(6), 32(a)(7)(c) and Eighth Circuit Rules 28A(c) and 28A(d). It contains 13,952 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). It has been prepared in proportionally spaced typeface using Microsoft Word 2000 version 9.0, in 14 point Times New Roman font. A digital version of the brief in PDF format has been provided on a computer diskette.

_____

Thomas C. Walsh

CERTIFICATE OF SERVICE

The undersigned hereby certifies that two copies of the Brief of Appellee and one copy of the Appellee's Appendix were served on this 24th day of February, 2004, by First Class mail, upon the following:

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

Christopher A. Hansen
Aden J. Fine
ACLU Foundation
125 Broad Street
18th Floor
New York, NY 10004

Paul Glist
John D. Seiver
Geoffrey C. Cook
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Ave., NW
Suite 200
Washington, DC 20006

Alan E. Untereiner
Kathryn S. Zecca
Robbins, Russell, Englert, Orseck & Untereiner LLP
1801 K Street, NW
Suite 411
Washington, DC 20006

Jeffrey R. Bragalone
Matthew P. Harper
McKool Smith P.C.
300 Crescent Court
Suite 1500
Dallas, TX 75201

Cindy A. Cohn
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Douglas N. Letter
Scott R. McIntosh
Civil Division
Department of Justice
601 D Street, NW
Room 9554
Washington, DC 20530

_____
Thomas C. Walsh

ADDENDUM

Submitted pursuant to Fed. R. App. P. 28(f)

INDEX

UNITED STATES CODE ANNOTATED
TITLE 17. COPYRIGHTS
CHAPTER 5--COPYRIGHT INFRINGEMENT AND REMEDIES

§ 512. Limitations on liability relating to material online

(a) Transitory digital network communications.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if--

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System caching.--

(1) Limitation on liability.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which--

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions.--The conditions referred to in paragraph (1) are that--

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology--

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if--

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information residing on systems or networks at direction of users.--

(1) In general.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider--

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the

service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent.--The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification.--

(A) 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:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

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

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information location tools.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider--

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on liability of nonprofit educational institutions.--(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if--

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations.--Any person who knowingly materially misrepresents under this section--

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys" fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it

(g) Replacement of removed or disabled material and limitation on other liability.--

(1) No liability for taking down generally.--Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception.--Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider--

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification.--To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) 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, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability.--A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena to identify infringer.--

(1) Request.--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.

(2) Contents of request.--The request may be made by filing with the clerk--

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena.--The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner 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.

(4) Basis for granting subpoena.--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.

(5) Actions of service provider receiving subpoena.--Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena.--Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for eligibility.--

(1) Accommodation of technology.--The limitations on liability established by this section shall apply to a service provider only if the service provider--

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition.--As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and--

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions.--The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief.--(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.--The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider--

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders.--Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions.--

(1) Service provider.--(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary relief.--As used in this section, the term "monetary relief" means damages, costs, attorneys" fees,

and any other form of monetary payment.

(l) Other defenses not affected. --The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of privacy.--Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on--

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction.--Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.