Order Code RL32037

CRS Report for Congress
Received through the CRS Web

Safe Harbor for Service Providers Under the Digital Millennium Copyright Act

Updated November 4, 2005

Brian T. Yeh
Legislative Attorney
American Law Division

Robin Jeweler
Legislative Attorney
American Law Division

Safe Harbor for Service Providers Under the Digital Millennium Copyright Act

Summary

Congress passed the Digital Millennium Copyright Act (DMCA) in 1998 in an effort to adapt copyright law to an evolving digital environment. The expansive legislation is divided into five titles, the second of which is the focus of this report. Title II of the DMCA amended chapter 5 of the Copyright Act, 17 U.S.C. § 501 *et seq.*, and created a new § 512 to limit the liability of service providers for claims of copyright infringement relating to materials on-line. This "safe harbor" immunity is available only to parties that qualify as a "service provider" as defined by the DMCA, and only after the provider complies with certain eligibility requirements.

In exchange for immunity from liability, the DMCA requires service providers to cooperate with copyright owners to address infringing activities conducted by the providers' customers. Subsection 512(h) obligates service providers to divulge to copyright owners the identity of a subscriber suspected of copyright infringement. The subsection provides a detailed procedure that a copyright owner must follow in order to obtain a subpoena from a federal court compelling the service provider to reveal the identity of the suspected infringing user.

This report describes the safe harbor and subpoena provisions, along with the responsibilities and obligations of service providers under 17 U.S.C. § 512. In addition to highlighting specific aspects of the statutory text, the report examines case law to date interpreting and applying the DMCA's safe harbors and subpoena procedure. With respect to the latter, the report discusses court decisions, including the opinion of the D.C. Circuit Court of Appeals in *RIAA v. Verizon Internet Services*, which have held that certain types of service providers may not be subpoenaed under § 512(h) to identify peer-to-peer music file-sharers.

This report will be updated if events warrant.

Contents

Safe Harbor for Service Providers Under the Digital Millennium Copyright Act

Background

Online service providers (OSPs) and Internet service providers (ISPs) provide critical infrastructure support to the Internet, allowing millions of people to access on-line content and electronically communicate and interact with each other. The potential for computer users to infringe intellectual property copyrights using the Internet could expose service providers to claims of secondary liability, such as contributory and vicarious copyright infringement. Concerned about this significant legal vulnerability of service providers, Congress passed the "Online Copyright Infringement Liability Limitation Act," Title II of the Digital Millennium Copyright Act (DMCA) of 1998,[1] which created limitations on the liability of OSPs and ISPs for copyright infringement arising from their users' activities on their digital networks.[2] The act's legislative history indicates that Congress wanted to provide service providers with "more certainty ... in order to attract the substantial investments necessary to continue the expansion and upgrading of the Internet."[3] At the same time, Congress desired to preserve "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."[4] The DMCA therefore includes several conditions that the service provider must satisfy in order to qualify for liability protection, and requires that the service providers' activities be encompassed within one of four specified categories of conduct.[5] One federal district court assessed the "dual purpose and balance" of the DMCA in the following manner:

> Congress ... created tradeoffs within the DMCA: service providers would receive liability protections in exchange for assisting copyright owners in identifying and dealing with infringers who misuse the service providers' systems. At the same time, copyright owners would forgo pursuing service providers for the copyright

---

[1] P.L. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. § 512).

[2] The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, 8 (Dec. 1998) at [http://www.copyright.gov/legislation/dmca.pdf]. [Hereinafter *Copyright Office Summary*].

[3] 144 CONG. REC. S11,889 (daily ed. Oct. 2, 1998) (statement of Sen. Hatch).

[4] H.Rept. 105-796, 105th Cong., 2d Sess. 72 (1998).

[5] *Id.* at 73.

infringement of their users, in exchange for assistance in identifying and acting against those infringers.[6]

Safe Harbor Provisions

Limitations on liability, often called "safe harbors," shelter service providers from copyright infringement suits. The DMCA's safe harbor provisions, codified at 17 U.S.C. § 512, do not confer absolute immunity, but they do greatly limit service providers' liability based on the specific functions they perform.[7] The safe harbors correspond to four functional operations of a service provider: 1) transitory digital network communications, 2) system caching, 3) storage of information on systems or networks at direction of users, and 4) information location tools.[8] Qualification for any one of these safe harbors is limited to the criteria detailed in each provision, and qualification under one safe harbor category does not affect the eligibility determination for any of the other three.[9]

§ 512 (a) Transitory digital network communications. When a service provider acts as a data conduit at the request of a third party by "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider," it will be shielded from liability for copyright infringement.[10] This safe harbor also protects the service provider for any intermediate and transient storage of the material in the course of conveying the digital information. However, qualification for this safe harbor is subject to several conditions, including:[11]

- Data transmission occurs through an automated technical process without selection of the material by the service provider.
- The service provider does not determine the recipients of the material.
- Intermediate or transient copies stored on the provider's system or network must not be accessible to anyone other than the designated recipients, and such copies must not be retained on the system longer than is reasonably necessary.

---

[6] In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 37 (D.D.C.2003), *rev'd sub nom.* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

[7] Ellison v. Robertson, 189 F. Supp. 2d 1051, 1064 (C.D. Cal. 2002), *aff'd in part and rev'd in part*, 357 F.3d 1072 (9th Cir. 2004). Service providers who qualify for safe harbor are protected from all monetary and most equitable relief that may arise from copyright liability. In such a situation, "even if a plaintiff can show that a safe harbor-eligible service provider has violated her copyright, the plaintiff will only be entitled to the limited injunctive relief set forth in 17 U.S.C. § 512(j)." Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1098-99 (W.D. Wash.2004) (citations omitted).

[8] 17 U.S.C. § 512(a)-(d).

[9] 17 U.S.C. § 512(n).

[10] 17 U.S.C. § 512(a).

[11] *Id.*

- The provider must not have modified the content of the transmitted material.

§ 512 (b) System Caching. The second safe harbor category limits ISP liability when its engages in "caching" of on-line content for purposes of improving network performance. Caching[12] helps to reduce the service provider's network congestion and increase download speeds for subsequent requests for the same data. For example, subscribers to a service provider may transmit certain material to other users of the provider's system or network, at the direction of those users. The service provider may, via an automated process, retain copies of this material for a limited time "so that subsequent requests for the same material can be fulfilled by transmitting the retained copy, rather than retrieving the material from the original source on the network."[13] Immunity for service providers that utilize system caching is provided on the condition that the ISP complies with the following:[14]

- The content of cached material that is transmitted to subsequent users is not modified by the service provider.
- The provider complies with industry standard rules regarding the refreshing, reloading, or other updating of the cached material.
- The provider does not interfere with the ability of technology that returns "hit" count information that would otherwise have been collected had the website not been cached to the person who posted the material.
- The provider must impose the same conditions that the original poster of the material required for access, such as passwords or payment of a fee.
- The provider must remove or block access to any material that is posted without the copyright owner's authorization, upon being notified that such material has been previously removed from the originating site, or that the copyright owner has obtained a court order for the material to be removed from the originating site or to have access to the material be disabled.

§ 512 (c) Information residing on systems or networks at direction of users. This safe harbor protects against copyright infringement claims due to storage of infringing material at the direction of a user on ISP systems or networks. Such storage includes "providing server space for a user's website, for a chat room, or other forum in which material may be posted at the direction of users."[15] The conditions placed on receiving the benefit of this safe harbor are as follows:[16]

---

[12] Caching is defined as "intermediate and temporary storage of material on a system or network operated by the service provider." 17 U.S.C. § 512(b).

[13] *Copyright Office Summary*, 10.

[14] 17 U.S.C. § 512(b)(2)(A)-(E).

[15] H.Rept. 105-551, pt. 2, 105th Cong. 2d Sess. 53 (1998).

[16] 17 U.S.C. § 512(c).

- The service provider lacks actual knowledge of the infringing material hosted or posted on its system or network.
- In the absence of actual knowledge, the service provider is "not aware of facts or circumstances from which infringing activity is apparent."[17]
- Where the provider has the right and ability to control the infringing activity, it must not derive a financial benefit directly attributable to that activity.
- Upon receiving proper notification of claimed infringement, the service provider must act "expeditiously" to remove or block access to the material.
- The service provider must designate an agent to receive notifications of claimed infringement. The contact information for this agent must be filed with the Register of Copyrights[18] and also be displayed to the public on the service provider's website.

Copyright owners must adhere to a prescribed procedure to inform the provider's designated agent of claimed infringement. To constitute effective notification, the copyright owner must "comply substantially" with the statutory requirements of § 512 (c)(3):[19]

- The notification is in writing, signed physically or electronically by a person authorized to act on behalf of the owner of the copyright allegedly infringed.
- The notification identifies the material that is claimed to have been infringed and provides sufficient information allowing the service provider to locate the material.
- The complaining party includes a statement, under penalty of perjury, that the party has a "good faith belief" that the use of the material is not authorized by the copyright owner, and that the information in the notification is accurate.

§ 512 (d) Information location tools. The fourth safe harbor classification immunizes service providers that provide users access to websites that contain infringing material by using "information location tools" such as hypertext links, indexes, and directories.[20] The conditions attached are substantially similar to those that apply to the "system storage" safe harbor provision discussed above, § 512 (c), including lack of actual or constructive knowledge requirements, notice and take-down procedures, and absence of direct financial benefit.[21] The rationale for protecting service providers under this provision is to promote development of the

---

[17] 17 U.S.C. § 512(c)(1)(A)(ii).

[18] "The Register of Copyrights is directed to maintain a directory of designated agents available for inspection by the public, both on the website of the Library of Congress, and in hard copy format on file at the Copyright Office." H.Rept. 105-551, pt. 2 at 55.

[19] 17 U.S.C. § 512(c)(3)(A)(i)-(vi).

[20] 17 U.S.C. § 512(d).

[21] 17 U.S.C. § 512(d)(1)-(3).

search tools that make finding information possible on the Internet.[22] Without a safe harbor for providers of these tools, the human editors and cataloguers compiling Internet directories might be overly cautious for fear of being held liable for infringement.

Notice and Take-down Procedure. One condition common to three of the four categories is the requirement that upon proper notification by the copyright owner of on-line material being displayed or transmitted without authorization, a service provider must "expeditiously" remove or disable access to the allegedly infringing material.[23] This "notice and take-down" obligation does not apply when the service provider functions as a passive conduit of information under § 512(a), but is a condition that must be met to obtain shelter under the remaining three safe harbor provisions. As indicated by the eligibility conditions in each subsection of § 512(b)-(d), the notice and take-down procedure varies slightly for each.

To prevent abuse of the notice and take-down procedure, § 512(f) provides damages, costs and attorneys' fees to any service provider that is injured by a knowing, material misrepresentation that an item or activity is infringing.[24] For example, any person who sends a "cease and desist" letter to a service provider, with the knowledge that the claims of copyright infringement are false, may be liable to the accused infringer for damages.

Eligibility Threshold for Safe Harbor. For protection under any of the exemptions, a party must first meet the statutory definition of a "service provider." The DMCA provides two distinct definitions, one applicable to the first provision and the second applicable to all of the others. Under § 512(a), the transitory communications provision, "service provider" is narrowly defined as "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."[25] The remaining three subsections utilize a broader definition of "service provider," applicable to "a provider of online services or network access, or the operator of facilities therefor."[26] For example, this definition encompasses providers offering "Internet access, e-mail, chat room and web page hosting services."[27]

---

[22] H.Rept. 105-551, pt. 2 at 58.

[23] *See* 17 U.S.C. § 512(b)(E), (c)(C), and (d)(3).

[24] "'Knowingly' means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations. 'Material' means that the misrepresentation affected the ISP's response to a DMCA letter." Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) (citations omitted).

[25] 17 U.S.C. § 512(k)(1)(A).

[26] 17 U.S.C. § 512(k)(1)(B).

[27] H.Rept. 105-551, pt. 2 at 64.

After a party qualifies as a service provider under one of the applicable definitions, there are still two additional threshold requirements that the provider must satisfy:[28]

- The service provider must have adopted, reasonably implemented, and informed its users of a policy for the termination of the accounts of subscribers who are repeat copyright infringers.
- The provider must accommodate and not interfere with "standard technical measures"[29] that are used by copyright owners to identify or protect their works, such as digital watermarks or digital rights management technologies.

No affirmative duty to police infringing activity. Pursuant to § 512 (m), the DMCA safe harbor provisions are not conditioned upon a service provider "monitoring its service or affirmatively seeking facts indicating infringing activity."[30] One U.S. district court has noted that this provision of § 512 "represents a legislative determination that copyright owners must themselves bear the burden of policing for infringing activity — service providers are under no such duty."[31] Yet some legal commentators suggest that courts have nevertheless created a "back door" requirement for ISPs to police their systems in search of copyright infringement by strictly construing the § 512(i) obligation to "implement" a repeat infringer termination policy as an affirmative duty to actively investigate potential infringement.[32] These judicial interpretations of the termination requirements in section § 512(i)(1)(A), discussed below, arguably may be contrary to Congress's intent in § 512(m), as indicated in committee report language accompanying the DMCA legislation:

> [T]he Committee does not intend this [termination] provision to undermine the principles of new subsection [m] ... by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing. However, those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.[33]

Judicial Interpretation of the Safe Harbors

Several courts have considered the safe harbor provisions to determine whether certain service providers met the statutory requirements for protection from copyright

---

[28] 17 U.S.C. § 512(i)(1)(A)-(B).

[29] "Standard technical measures" is defined at § 512(i)(2).

[30] 17 U.S.C. § 512(m)(1).

[31] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 657 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

[32] *See, e.g.*, Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 51-54 (2003).

[33] H.Rept. 105-551, pt. 2 at 61.

infringement claims. A survey of cases that have examined the safe harbor defense reveals that courts generally have been cautious in permitting liability limitation to service providers, closely scrutinizing compliance with the safe harbor eligibility conditions on the part of both copyright owners and service providers.

Safe harbor denied. In two copyright infringement cases involving peer-to-peer file-sharing services, *A & M Records, Inc. v. Napster, Inc.*[34] and *In re Aimster Copyright Litigation*,[35] the courts denied safe harbor protection to the companies Napster and Aimster, on the ground that those companies did not meet the eligibility requirements specified by the DMCA. Both of these companies operated peer-to-peer networking services that facilitated sharing over the Internet of music files stored on their users' computer hard drives. Using peer-to-peer software offered by Napster and Aimster,[36] MP3 song files — the majority of which were unauthorized for distribution by their copyright owners — were uploaded and downloaded freely and repeatedly to the alarm of the music recording industry.

Napster asserted that its operations were protected by the § 512(a) safe harbor provision, claiming that it offered the "transmission, routing, or providing of connections for digital online communications."[37] The district court in *Napster* found that the infringing material was exchanged over the Internet, not through Napster's servers, and therefore Napster did not provide connections "through" its system.[38] On the basis of this determination, the court ruled that Napster had failed to demonstrate that it qualified for the § 512(a) safe harbor. In addition, the court noted that even if Napster had met the criteria in §512(a), it did not satisfy the threshold eligibility requirements in § 512(i), in particular the termination policy provision. The court found that the plaintiffs in the case had raised "genuine issues of material fact about whether Napster ha[d] reasonably implemented a policy of terminating repeat infringers" when it introduced evidence that Napster had not adopted a formal termination policy until two months *after* the filing of the lawsuit against it.[39] This belated attempt to adopt a termination policy would have prevented Napster from seeking liability protection under any of the four safe harbors.

The U.S. Court of Appeals for the Ninth Circuit in *Napster* rejected "a blanket conclusion that § 512 of the [DMCA] will never protect secondary infringers," but commented that the "plaintiffs raise serious questions regarding Napster's ability to

---

[34] 239 F.3d 1004 (9th Cir. 2001).

[35] 252 F. Supp. 2d 634, 648 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

[36] The Aimster service was renamed the "Madster" in January 2002, after a ruling by a National Arbitration Forum panel that the Internet domain name "aimster.com" violated the trademark for America Online's (AOL) instant messaging service. To avoid confusion, this report will continue to refer to the file-sharing service as "Aimster." *See* [http://www.usatoday.com/tech/news/2002/02/01/aimster-now-madster.htm].

[37] A & M Records, Inc. v. Napster, Inc., 2000 WL 573136, at *3 (N.D. Cal. May 12, 2000).

[38] *Id.* at *8. The court stated, "Napster enables or facilitates the initiation of connections, but these connections do not pass through the system within the meaning of subsection 512 (a)."

[39] *Id.* at *9-10.

obtain shelter under § 512."[40] The significant questions included whether Napster would be eligible for safe harbor under § 512(d), the information location tools provision, whether copyright owners must give service providers "official" notice pursuant to § 512(c)(3) in order for the provider to have knowledge of infringement on its system, and whether Napster had in fact complied with the termination policy requirement of § 512(i)(1)(A).[41] Nevertheless, until these issues could be addressed at trial, the district court's approval of a preliminary injunction against Napster was appropriate because the plaintiffs had "demonstrate[d] that the balance of hardships tips in their favor."[42]

In a lawsuit similar to *Napster*, record company and music publishing plaintiffs charged the peer-to-peer file-sharing service Aimster with contributory and vicarious infringement of copyrights held by the plaintiffs. In addition to distributing file-sharing software, Aimster provided on-line tutorials on its website which "methodically demonstrated how to transfer and copy copyrighted works over the Aimster system."[43] In addition, the Aimster software allowed users to encrypt all the file exchanges, a scheme that effectively prevented Aimster from gaining knowledge of the type of content being transferred. Unlike Napster, Aimster had adopted a termination policy for repeat infringers before a lawsuit was filed against it. However, the district court in *Aimster* found that the termination policy could not be *implemented* in reality because the encryption technology provided by Aimster made it impossible to determine which users were transferring copyrighted files.[44] The court thus found Aimster ineligible for any safe harbor protections because its repeat infringer policy did not meet the requirement of § 512(i)(1)(A).[45] In upholding the district court's preliminary injunction, the U.S. Court of Appeals for the Seventh Circuit noted:

> The [DMCA] provides a series of safe harbors for Internet service providers and related entities, but none in which Aimster can moor... The common element of [the DMCA]'s safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers.' Far from doing anything to discourage repeat infringers of the plaintiffs' copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement.[46]

---

[40] *Napster*, 239 F.3d at 1025.

[41] *Id.*

[42] *Id.*

[43] *Aimster*, 252 F. Supp. 2d at 643.

[44] *Id.* at 659 (emphasis in original).

[45] *Id.*

[46] *Aimster*, 334 F.3d at 655.

Ellison v. Robertson[47] is another case that denied safe harbor to the defendant service provider for failure to meet the threshold eligibility requirements under § 512(i). Stephen Robertson had electronically scanned and converted into digital binary files[48] several science fiction novels written by Harlan Ellison, without authorization of the copyright owner. Robertson then uploaded and copied the files onto USENET newsgroups that are carried by several ISPs, including American Online, Inc. (AOL).[49] AOL's retention policy provided that USENET messages containing binary files remain stored on the company's servers for fourteen days.[50] Once Ellison learned of the infringing activity, he directed his legal counsel to e-mail a notice of copyright infringement pursuant to the DMCA notification procedures. AOL, however, claimed never to have received the notice. Receiving no response, the plaintiff then filed a copyright infringement suit against AOL and other parties.

The Court of Appeals for the Ninth Circuit in *Ellison* upheld the district court's conclusion that there were triable issues of material fact concerning Ellison's contributory copyright infringement claim, on the basis that a reasonable trier of fact could find that AOL had reason to know of the potentially infringing activity and had materially contributed to it.[51] Although AOL did not have actual knowledge of the infringement, AOL's failure to receive the plaintiff's DMCA notification was due to its own fault in not promptly updating its designated agent contact e-mail address with the Copyright Office.[52] Due to this error, the e-mail sent by the plaintiff was routed to a defunct e-mail account. The district court refused to permit AOL to disclaim knowledge of the infringement[53] on account of its own carelessness: If AOL could avoid the knowledge requirement through this oversight or deliberate action,

---

[47] 357 F.3d 1072 (9th Cir. 2004).

[48] A file stored in "binary" format is computer-readable but not human-readable. *See* [http://www.webopedia.com/TERM/b/binary_file.html].

[49] "The USENET, an abbreviation of 'User Network,' is an international collection of organizations and individuals (known as 'peers') whose computers connect to each other and exchange messages posted by USENET users." Ellison v. Robertson, 189 F. Supp. 2d 1051, 1053 (C.D.Cal. 2002), *aff'd in part and rev'd in part*, 357 F.3d 1072 (9th Cir. 2004).

[50] *Id.* at 1054.

[51] *Ellison*, 357 F.3d at 1077-78.

[52] *Ellison*, 189 F. Supp. 2d at 1058. As discussed earlier in this report, 17 U.S.C. § 512(c)(2) requires service providers to designate an agent to receive notifications of claimed infringement and provide the contact information for this agent to the Copyright Office. The record showed that AOL had changed its contact e-mail address from "copyright@aol.com" to "aolcopyright@aolcom" in fall 1999, but waited until April 2000 to notify the Copyright Office of the change.

[53] To be held liable for contributory copyright infringement, a court must find that the party, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

then it would encourage other ISPs to remain willfully ignorant in order to avoid contributory copyright infringement liability.[54]

The Ninth Circuit reversed the district court's conclusion that AOL qualified for a safe harbor limitation of liability. The appellate court found "at least a triable issue of material fact" regarding AOL's threshold eligibility for safe harbor under § 512(i).[55] First, the court explained that § 512(i)(1)(A) has three separate requirements for a service provider to fulfill:

- Adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances;
- Inform users of the service policy; and
- Implement the policy in a reasonable manner.

The court determined that there was "ample evidence in the record" to suggest that AOL failed to satisfy the last of these requirements. Because AOL had changed the e-mail address to which infringement notifications were being sent and did not close the old e-mail account or forward the messages to the new address, "AOL allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded."[56] This fact alone provides a basis for a reasonable jury to find that AOL did not "reasonably implement[]" a policy against repeat infringers.[57] Thus, the appellate court remanded the case for trial on Ellison's contributory infringement claim, and if AOL is found liable, on AOL's eligibility under § 512(i) to assert the safe harbor defense.[58]

In *ALS Scan, Inc. v. RemarQ Communities, Inc.*, the U.S. Court of Appeals for the Fourth Circuit considered whether an ISP is eligible for protection when it is alerted to infringing activity by "imperfect notice" that does not strictly comply with the notification procedures specified in § 512(c)(3).[59] ALS Scan holds the copyrights to over 10,000 "adult" photographs which were posted on newsgroups[60] that were operated by the service provider RemarQ Communities. Upon discovering that RemarQ's servers contained infringing material, ALS Scan sent a "cease and desist" letter to RemarQ, requesting deletion of two specific newsgroups that contained the photographs. However, the district court in *ALS Scan* found that the notice was "fatally defective" in complying with § 512(c)(3) because ALS Scan never provided

---

[54] *Ellison*, 189 F. Supp. 2d at 1058.

[55] *Ellison*, 357 F.3d at 1080.

[56] *Id.*

[57] *Id.*

[58] *Id.* at 1082.

[59] 239 F.3d 619, 620 (4th Cir. 2001)

[60] Newsgroups are on-line discussion groups covering thousands of subjects, such as politics, social issues, sports, and entertainment. A news reader program is required to connect to the news servers on the Internet, and allows the computer user to read and post messages to the newsgroup forum.
See [http://www.webopedia.com/TERM/n/newsgroup.html].

RemarQ with a "representative list" of the infringing photographs. Nor did it identify the pornographic photographs with "sufficient detail" to enable RemarQ to locate and disable access to them.[61] In reversing the district court's ruling granting summary judgment in favor of RemarQ, the court of appeals held that ALS Scan had "substantially complied" with DMCA notification requirements because its notice letter identified by name the two RemarQ newsgroup sites "created solely for the purpose of publishing and exchanging ALS Scan's copyrighted images" and also referred RemarQ to website addresses where RemarQ could find pictures and names of ALS Scan's adult models.[62] Thus, the court of appeals held that since RemarQ was provided with a notice that *substantially* complied with the DMCA, the service provider could not rely on a claim of defective notice to maintain the safe harbor defense.[63]

Safe harbor allowed. In contrast to the *ALS Scan* court's determination of the consequences of "imperfect notice," the court in *Hendrickson v. eBay, Inc.* [64] found that the defective notice supplied by the plaintiff in its case failed to comply substantially with § 512(c)(3)'s notification requirement. In *Hendrickson*, the Internet auction service eBay was allegedly offering for sale pirated DVD copies of a documentary about the life of Charles Manson called "Manson." Prior to filing suit, plaintiff Robert Hendrickson sent a letter to eBay demanding that the auction site cease and desist "from any and all further conduct considered an infringement(s) of [plaintiff's] right."[65] eBay responded promptly to this letter, informing Hendrickson of its termination policy for repeat infringers and requesting that the plaintiff submit proper notice under the DMCA by providing more detailed information regarding the alleged infringing items, including identifying the specific eBay item numbers corresponding to the copies of "Manson" for sale.[66] The plaintiff refused to provide this information and proceeded to file copyright infringement suits against eBay.

At trial, Hendrickson did "not dispute that he ha[d] not strictly complied with Section 512(c)(3)."[67] The U.S. district court instead considered whether the plaintiff's imperfect notice satisfied the DMCA's "substantial" compliance requirement. The court noted that Hendrickson did not include in his notice a written statement attesting to the good faith and accuracy of his infringement claim, as required by § 512(c)(3)(A)(v)-(vi).[68] In addition, the plaintiff failed to provide eBay with sufficient information to allow the service provider to identify the auction

---

[61] *ALS Scan,* 239 F.3d at 624.

[62] *Id*. at 624-25. The court further explained, "[W]hen a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements." *Id.* at 625.

[63] *Id.* at 620 (emphasis in original).

[64] 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

[65] *Id.* at 1085.

[66] *Id.*

[67] *Id.* at 1089.

[68] *Id.* at 1089-90.

listings that allegedly offered pirated copies of "Manson" for sale. This failure further rendered Hendrickson's notice improper under the DMCA.[69] Therefore, the court ruled, eBay was under no obligation to remove the allegedly infringing material on its system.[70] The court went on to consider eBay's eligibility for safe harbor under § 512(c) and determined that it satisfied all the statutory conditions. The DMCA thus having shielded eBay from liability, the court granted eBay summary judgment on the copyright infringement claim.[71]

In *Corbis Corp. v. Amazon.com, Inc.*,[72] the court determined that the electronic commerce company Amazon.com had qualified for safe harbor with regard to infringing activity allegedly occurring in its zShops third-party vendor service.[73] Corbis, a company that licenses art images and celebrity photographs, had sued Amazon, claiming that several hundred images in which it had a "copyright interest" were being copied, displayed, and sold through Amazon's zShops sites.[74] Amazon sought liability protection under § 512(c), the "information residing on systems or networks at the direction of users" safe harbor.

The *Corbis* court first examined whether Amazon satisfied the DMCA's threshold conditions for safe harbor. After finding that Amazon met the statutory definition of service provider,[75] the court applied § 512(i)'s three-part test as it was set forth in *Ellison v. Robertson.*[76] The court ruled that Amazon had adopted a termination policy for repeat infringers and communicated that policy to its users.[77] In regard to the third *Ellison* prong, the court found evidence that Amazon had reasonably implemented procedures for addressing copyright infringement complaints.[78] After satisfying these threshold conditions for safe harbor, Amazon still had to meet the requirements for liability protection under § 512(c). The court

---

[69] *Id.* at 1090-92.

[70] "[T]he service provider's duty to act is triggered only upon receipt of proper notice." *Id.* at 1089.

[71] *Id.* at 1094.

[72] 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

[73] "The zShops platform allows individuals and retailers (referred to as 'vendors') to showcase their products and sell them directly to online consumers. Amazon, however, does not sell any of its own inventory on the zShops platform." Id. at 1094.

[74] *Id*. at 1096-97.

[75] *Id.* at 1100.

[76] *See* discussion of this case, *supra* pages 8-10.

[77] *Corbis*, 351 F.Supp.2d at 1100-02.

[78] Amazon informs the listing vendor via e-mail that 'your listing may have violated the intellectual property rights of others and the Community Rules that govern our Auction, zShops, and Amazon Marketplace sites.' The e-mail also provides the vendor with the complaining party's contact information. Finally, as with other cancellations, Amazon warns vendors that repeated violations may result in permanent suspension from the Amazon site." *Id*. at 1103 (citations omitted).

found that Amazon did not have actual[79] or apparent knowledge[80] that material on its network is infringing. The court also found that Amazon did not have the right and ability to control the infringing material on zShops vendor webpages.[81] Thus, the court concluded that Amazon is entitled to safe harbor protection under § 512(c) for any copyright infringement committed by zShops vendors on the Amazon site.

The court in *Perfect 10, Inc. v. CCBill, LLC, et al.*[82] expanded the array of service providers eligible for safe harbor to include Internet businesses that provide age-verification and on-line payment services to websites that restrict user access to adult content. Perfect 10, a copyright owner of adult-oriented photographic images, had sued several age-verification and billing companies for infringement. These businesses claimed liability protection under DMCA safe harbors §§ 512(a) and 512(d). The plaintiff argued that § 512(a), the "transitory digital network communications" safe harbor, protects only ISPs that transmit infringing material, not other material such as credit card information for on-line payment purposes.[83] Perfect 10 also argued that § 512(d), the "information location tools" safe harbor, is limited to service providers such as Yahoo! and Google that provide links to millions of websites, and does not cover a service provider that links to "a relatively small" number of websites with whom the ISP has a contractual relationship.[84]

The *Perfect 10* court dismissed the plaintiff's arguments as being "without merit," noting that § 512(a) includes ISPs that provide a "connection" to infringing material. Also, nothing in § 512(d) limits its applicability only to ISPs that provide links to millions of websites with which the service provider lacks contractual relationships.[85] Thus, the court allowed the defendant third-party billing and age-verification service providers to seek shelter under the DMCA safe harbors.

Subpoena to Identify Infringer. The subpoena provision contained in Title II of the DMCA, codified at 17 U.S.C. § 512(h), has received increased attention as a result of the Recording Industry Association of America's (RIAA) highly publicized efforts to take legal action against individual computer users who use peer-to-peer

---

[79] Cobis, prior to filing the lawsuit, had never attempted to notify Amazon about the alleged infringing conduct of zShop vendors. Thus, Corbis missed its opportunity to provide "the most powerful evidence of a service provider's knowledge–actual notice of infringement from the copyright holder." *Id*. at 1107.

[80] The court stated, "[Corbis] provides no evidence from which to infer that Amazon was aware of, but chose to ignore, red flags of blatant copyright infringement on specific zShops sites." *Id*. at 1109.

[81] *Id*. at 1110. Since Amazon failed to meet the first part of § 512(c)'s third requirement, it was unnecessary for the court to determine whether Amazon receives a direct financial benefit from the allegedly infringing conduct. *Id.*

[82] 340 F. Supp. 2d 1077 (C.D. Cal. 2004).

[83] *Id.* at 1091.

[84] *Id*. at 1097-98.

[85] *Id*. at 1091, 1098.

(P2P) software to share copyrighted music files.[86] A critical component of these actions is identification of the computer user. Upon request by a copyright owner, the clerk of any U.S. district court "shall expeditiously issue" a subpoena to a service provider for disclosure of "information sufficient to identify the alleged infringer of the [copyrighted] material."[87] The clerk's issuance of the subpoena depends on the filing of the specified information in the subpoena request:[88]

- A copy of the notification of claimed infringement sent to the service provider. This notification must comply substantially with the notice requirement described in § 512(c)(3)(A).
- A proposed subpoena indicating the information that is sought.
- "A sworn declaration" that the subpoena is sought solely to obtain information revealing the identity of the alleged infringer and that the information will only be used to protect rights under the Copyright Act.

Upon receiving the subpoena, a service provider "shall expeditiously disclose" to the copyright holder the information required by the subpoena.[89] Congress intended this rapid subpoena process to be "a ministerial function performed quickly" by the clerk of a court in order to identify copyright infringers and stop the infringing activities.[90] Indeed, Congress's intent is expressly reflected in the statutory language itself, where the word "expeditiously" appears twice in the subpoena procedure section.

In re Verizon Internet Services. In two court proceedings occurring within months of each other, the RIAA sought to enforce DMCA subpoenas served on Verizon Internet Services after Verizon refused to comply with them.[91] These subpoenas requested the identities of subscribers to Verizon's Internet access service who were allegedly sharing hundreds of copyrighted songs using peer-to-peer file transfer software. Verizon argued in the first case that the subpoena was inapplicable because the allegedly infringing material was not stored on Verizon-owned servers,

---

[86] For more background on peer-to-peer software and copyright infringement issues, *see* CRS Report RL31998, *File-Sharing Software and Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd*, by Brian Yeh and Robin Jeweler.

[87] 17 U.S.C. § 512(h)(3)-(4).

[88] 17 U.S.C. § 512(h)(2)(A)-(C). In addition to these conditions placed on obtaining a subpoena, 17 U.S.C. § 512(h)(6) provides another safeguard against abuse of subpoena power: subpoenas are subject to the provisions of the Federal Rules of Civil Procedure that govern the issuance, service, and enforcement of subpoenas. For example, under FED.R.CIV.P. 45, service providers or their Internet users may object to, modify, or move to quash a subpoena.

[89] 17 U.S.C. § 512(h)(5).

[90] H.Rept. 105-551, pt. 2, at 61.

[91] In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 37 (D.D.C.2003) ("Verizon I"); In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244 (D.D.C.) ("Verizon II").

but rather on its subscribers' computers.[92] In the second, Verizon moved to quash the subpoena, challenging the DMCA subpoena authority as a violation of its subscribers' First Amendment right to anonymous speech.[93] The U.S. district court ruled against Verizon in both cases, finding that subpoena authority extended to all types of service providers within the scope of the DMCA, not just providers that stored information on a system or network,[94] and that the DMCA subpoena power was constitutional.[95] Verizon requested a stay of the lower court's order pending appeal, but the U.S. Court of Appeals for the District of Columbia denied the request.[96] A day later, Verizon revealed the names of four subscribers suspected of copyright infringement.[97]

The federal district court in *In re Verizon Internet Services, Inc.* determined that the § 512(h) subpoena process "provide[s] substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas."[98] In particular, it noted that the DMCA "provides disincentives for false representations under the act, making it costly for anyone to seek a subpoena on the basis of intentional misrepresentations, and thereby further ensuring that subpoenas will only be used in circumstances of good faith allegations of copyright infringement."[99] Three months later, the court upheld the constitutionality of the DMCA's subpoena provision in another proceeding against Verizon, stating that the "DMCA contains adequate safeguards to ensure that the First Amendment rights of Internet users will not be curtailed."[100] The court, in dicta, claimed that owing to built-in safeguards, "it is unlikely that § 512(h) will require disclosure, to any significant degree, of the identity of individuals engaged in protected anonymous speech, as opposed to those engaged in unprotected copyright infringement."[101] The court explained that "[w]hatever marginal impact the DMCA subpoena authority may have on the expressive or anonymity rights of Internet users ... is vastly outweighed by the extent of copyright infringement over the Internet through peer-to-peer file sharing, which is the context of the legitimate sweep of § 512(h)."[102]

---

[92] *Verizon,* 240 F. Supp. 2d at 28-29.

[93] *Verizon,* 257 F. Supp. 2d at 247.

[94] *Verizon,* 240 F. Supp. 2d at 26.

[95] *Verizon,* 257 F. Supp. 2d at 275.

[96] 2003 WL 21384617 (D.C. Cir. June 4, 2003)(No. 03-7015, 03-7053).

[97] *See* Christopher Stern, *Verizon Identifies Download Suspects*, WASH. POST, June 6, 2003, at E05.

[98] 240 F. Supp. 2d at 40-41.

[99] *Id.*, at 41 n.14. *See also* 17 U.S.C. § 512(f)("Any person who knowingly misrepresents ...that material or activity is infringing...shall be liable for any damages, including costs and attorneys fees...").

[100] *Verizon,* 257 F. Supp. 2d at 260-61.

[101] *Id.* at 263.

[102] *Id.* at 265-66.

Following the district court's determination of the DMCA subpoena power's legality, the RIAA obtained over 800 subpoenas compelling several major ISPs and some universities to provide the names of computer users suspected of swapping copyrighted music files, with approximately 75 new subpoenas being approved every day.[103] Armed with this information, the RIAA promised to file what could be thousands of lawsuits against particularly egregious P2P swappers of copyrighted music.[104] In many cases, however, these enforcement efforts have been met with resistance. SBC, an ISP subsidiary of Pacific Bell, challenged the validity and legality of subpoenas,[105] as did several universities that were recipients of RIAA subpoenas.[106] Smaller ISPs, through an organization called NetCoalition.com, expressed their concerns that RIAA's enforcement campaign seeks "to achieve in court what the association has not yet been able to accomplish in Congress — to make Internet companies legally responsible for the conduct of individuals who use their systems, forcing these companies to become not only the police of the Internet but also permanent and constant watchdogs of the substance of all email traffic, instant messaging, and file sharing." [107] Congress had expressed interest and concern over the issue as well. Several hearings were held.[108]

RIAA v. Verizon. On December 19, 2003, the U.S. Court of Appeals for the D.C. Circuit handed down its opinion reversing the district court's decisions

---

[103] *See* Ted Bridis, *RIAA's Subpoena Onslaught Aimed at Illegal File Sharing*, WASH. POST, July 19, 2003, at E01.

[104] See generally, [http://www.riaa.com/news/newsletter/062503.asp].

[105] *See ISP Claim Subpoenas for Subscriber Info Not Authorized by DMCA, Unconstitutional*, 66 BNA PAT., TRADEMARK & COPYRIGHT J. 436 (Aug. 8, 2003).

[106] On August 7, 2003, the U.S. District Court for the District of Massachusetts issued an order quashing subpoenas issued in the District of Columbia against two Boston universities, MIT and Boston University. The court held that the subpoenas violate federal rules of civil procedure which limit the geographical reach of subpoenas issued by a federal court. The RIAA has indicated that, although it believes the subpoenas were properly issued, it will file them in the appropriate courts. *District of Columbia Court Lacks Authority To Issue DMCA Subpoenas to Boston Schools*, 66 BNA PAT., TRADEMARK & COPYRIGHT J. 458 (Aug. 15, 2003).

[107] *Letter from Kevin S. McGuiness, Exec. Director of NetCoaliton.com to Cary Sherman, Pres., RIAA* (Aug. 11, 2003) at [http://www.netcoalition.com/vertical/Sites/%7BF1D948CC-5797-482E-B502-743C873E2848%7D/uploads/%7B2DBDD281-1E77-45C5-ABD2-BF39728972F0%7D.DOC]

[108] *Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs*, 108th Cong., 1st Sess. (2003); *Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace: Hearing Before the Senate Committee on Commerce, Science, and Transportation*, 108thCong., 1st Sess. (2003). *See also* S. 1621, 108th Cong., 1st Sess. (2003), the "Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003" which would require, among other things, that the DMCA subpoenas be issued only in connection with pending lawsuits.

upholding the RIAA subpoenas.[109] The reversal was predicated on the appellate court's findings that under § 512, a subpoena may be issued only to an ISP engaged in storing material that is infringing or the subject of infringing activity on its servers — not to an ISP acting as a passive conduit for data transferred between two Internet users. And, an ISP acting as a conduit for P2P file sharing does not involve the storage of infringing material on the ISP's server.

The court rested its decision on a technical interpretation of § 512(h) and the overall structure of § 512. Examining closely the cross-references of subsection (h), it noted that one of the required elements in the subpoena application is that the copyright owner identifies "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[.]"[110] The court agreed with Verizon that it is impossible to comply with this requirement when an ISP is acting as a mere conduit because

> [n]o matter what information the copyright owner may provide, the ISP can neither "remove"' nor "disable access to" the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscriber's computers.[111]

The court rejected the RIAA's contention that an ISP could "disable access" by terminating the infringer's account with the ISP. Blocking access to infringing material and terminating an ISP's user account are separate remedies elsewhere under § 512.[112] "Notice and take-down" requirements of § 512(b)-(d), that is, disabling access to infringing material, apply to ISPs when they are storing infringing material — either as a temporary cache of a web page, as a website stored in the ISP's server, or as an information locating tool hosted by an ISP,[113] but *not* when it is routing infringing material to or from a personal computer owned and used by a subscriber.[114] The court reasoned that the reference to "disabling access" for purposes of issuing a subpoena is distinct from terminating service. Thus, because the ISP does not have access to material residing on a user's computer, it cannot disable access to it by others. Examining the overall structure of the statute, the court concluded that "[t]he presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) suggests the subpoena power of § 512(h) applies only to ISPs

---

[109] Recording Indus. Ass'n of Am.v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

[110] 17 U.S.C. § 512(c)(3)(A)(iii) as referred to in subsection (h)(2)(A) (emphasis added).

[111] *Verizon*, 351 F. 3d at 1235.

[112] *Cf.* 17 U.S.C. § 512(j)(1)(A)(i) with (j)(1)(A)(ii). These provisions set forth separate remedies available under an injunction to remedy copyright infringement. Specifically, blocking access to infringing material and terminating a subscribe's account.

[113] 17 U.S.C. § 512(b)-(d).

[114] 17 U.S.C. § 512(a).

engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others."[115]

The court was sympathetic to the RIAA's concerns regarding the widespread infringement of its members' copyrights and their need for legal tools to combat it. But it would not "rewrite" the DMCA to address those concerns. That prerogative rests squarely with the Congress.

In re Charter Communications. On January 4, 2005, a divided panel of the U.S. Court of Appeals for the Eighth Circuit reached the same conclusion regarding the DMCA subpoena power as the *Verizon* appellate court.[116] At issue was Charter Communications' motion to quash the RIAA's subpoenas requesting that the internet service provider produce the names, physical addresses, telephone numbers, and e-mail addresses of 200 Charter customers. The Eighth Circuit ruled that § 512(h) does not authorize a copyright owner to request a subpoena for an ISP that only acts as a conduit for copyrighted material transferred between two users.[117] In dicta, the court acknowledged the difficulties that copyright owners face in deterring unlawful P2P file-sharing without first learning of the identities of persons engaged in the activity. However, the court pointed out that this information could be discovered through alternative means such as "John Doe" lawsuits,[118] a legal device that the RIAA has been using in the aftermath of *Verizon* in order to obtain court-ordered subpoenas.[119]

Conclusion

Among the DMCA's significant changes to the Copyright Act is the creation of § 512 to protect service providers from copyright liability arising from the infringing conduct of their users. This section represents Congress's attempt to address the liability concerns of service providers that operate the infrastructure of the Internet,

---

[115] Verizon, 351 F. 3d at 1236-37.

[116] In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005).

[117] *Id*. at 777. The dissenting opinion in *Charter* argued that the right to request a subpoena pursuant to § 512(h) is not limited by the type or function of the service provider. Since a subpoena may be issued to "a service provider," and the statutory definition of "service provider" expressly includes conduit service providers, then the RIAA's subpoena to Charter should be enforced. *Id*. at 778-80 (Murphy, J., dissenting).

[118] *Id.* at 775 n.3. The dissenting judge complained that John Doe lawsuits were insufficient to help copyright holders in their efforts to stop the "massive piracy" of their works over P2P networks, since such legal actions are costly and time consuming. Relegating copyright owners to using John Doe lawsuits to protect themselves from infringement by subscribers of conduit ISPs, is contrary to legislative intent because the purpose of the DMCA subpoena power was "to obtain the assistance of ISPs in an expeditious process to stop infringement." *Id.* at 782 (Murphy, J., dissenting).

[119] *See, e.g.*, John Schwartz, *Music Industry Returns to Court, Altering Tactics On File Sharing*, N.Y. TIMES, Jan. 22, 2004, at C1 (explaining how John Doe lawsuits are used by plaintiffs to sue persons whose identities are not known. The suits "identify the suspected file traders only by a numerical tag, known as an Internet protocol number, assigned to them by their Internet service provider.")

as well as specify means by which service providers can cooperate with copyright owners to identify and deal with infringing users.

The general purposes and goals of the safe harbor statute are clear. The subpoena issue, however, is believed by many to be an excellent example of the widely-acknowledged difficulty of enacting legislation tailored to evolving technologies. Both the U.S. district court and the U.S. court of appeals in *Verizon* noted that peer-to-peer file-sharing technology was nowhere on the horizon when Congress considered and enacted the DMCA. And, as P2P technology utilizing more encryption evolves, the issues are likely to become even more complex.

Server-based Napster-like music file sharing, though very popular, was arguably not legally complicated. Traditional copyright law principles and balancing copyright owners' property interests against consumer desires for access to entertainment media clearly favored copyright owners.[120] But P2P file-sharing technology developments raise far more serious privacy issues with a much wider sweep.

[120] *See* A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).