Order Code RL32037

CRS Report for Congress
Received through the CRS Web

Safe Harbor for Service Providers Under the Digital Millennium Copyright Act

Updated January 9, 2004

Brian Yeh
Law Clerk
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 examines the recent decision of the D.C. Circuit Court of Appeals in *RIAA v. Verizon Internet Services*, holding that service providers may not be subpoenaed to identify peer-to-peer music-file sharers.

Contents

Background 1
Safe Harbor Provisions 2
Eligibility Threshold for Safe Harbor 5
Subpoena to Identify Infringer 11
Conclusion 14

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

---

[1] P.L. 105-304, 112 Stat. 2860 (1998).

[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.

[6] In re Verizon Internet Services, Inc., 240 F. Supp.2d 24, 37 (D.D.C.), *rev'd sub nom.* Recording Industry Association of American v. Verizon Internet Services ,___F.3d___, (continued...)

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.
- 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

---

[6] (...continued)
2003 WL 22970995 (D.C.Cir. 2003).

[7] Ellison v. Robertson, 189 F. Supp.2d 1051, 1064 (C.D. Cal. 2002).

[8] 17 U.S.C. § 512(a)-(d).

[9] 17 U.S.C. § 512(n).

[10] 17 U.S.C. § 512(a).

[11] *Id.*

[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).

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 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]

- 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.

---

[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).

[17] 17 U.S.C. § 512(c)(1)(A)(ii).

- 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 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

---

[18] "The Register of Copyrights is directed to maintain a directory of designated agents available for inspection by the public, both on the web site 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).

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

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.

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."[24] 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."[25] For example, this definition encompasses providers offering "Internet access, e-mail, chat room and web page hosting services."[26]

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:[27]

1. 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.
2. The provider must accommodate and not interfere with "standard technical measures"[28] 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."[29] 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

---

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

[24] 17 U.S.C. § 512(k)(1)(A).

[25] 17 U.S.C. § 512(k)(1)(B).

[26] H.R. CONF. REP. NO. 105-551, pt. 2 at 64.

[27] 17 U.S.C. § 512(i)(1)(A)-(B).

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

[29] 17 U.S.C. § 512(m)(1).

infringing activity–service providers are under no such duty."[30] 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.[31] These judicial interpretations of the termination requirements in section § 512(i)(1)(A), discussed below, arguably may be contrary to Congress' 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.[32]

Judicial Interpretation of the Safe Harbors. Several court cases have considered the safe harbor provisions to determine whether certain service providers met the statutory requirements for protection from copyright 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.*[33] and *In re: Aimster Copyright Litigation*,[34] 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 stored on their users' computer hard drives. Using peer-to-peer software offered by Napster and Aimster,[35] 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.

---

[30] In re: Aimster Copyright Litigation, 252 F.Supp.2d 634, 657 (N.D. Ill. 2002).

[31] *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).

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

[33] 239 F.3d 1004 (9th Cir. 2001).

[34] 252 F.Supp.2d 634, 648 (N.D. Ill. 2002), *aff'd,* 334 F.3d 643 (7th Cir. 2003).

[35] The Aimster service was renamed "Madster" in January 2002, after a ruling by the National Arbitration Forum panel that the Internet domain name "aimster.com" violated the trademark for America Online (AOL)'s 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].

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."[36] 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.[37] 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 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.[38] 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 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 obtain shelter under § 512."[39] 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).[40] 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."[41]

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."[42] 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

---

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

[37] *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)."

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

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

[40] *Id.*

[41] *Id.*

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

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.[43] 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).[44] 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.[45]

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).[46] ALS Scan holds the copyrights to over 10,000 "adult" photographs which were posted on newsgroups[47] 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 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.[48] 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 web site addresses where RemarQ could find pictures and names

---

[43] *Id.* at 659. (Emphasis in original.)

[44] *Id.*

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

[46] 239 F.3d 619, 620 (4th Cir. 2001).

[47] 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].

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

of ALS Scan's adult models.[49] 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.[50]

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.*[51] 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."[52] 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.[53] The plaintiff refused to provide this information and proceeded to file copyright infringement suits against eBay. At trial, Hendrickson did "not dispute that he has not strictly complied with Section 512(c)(3)."[54] 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 17 U.S.C. § 512 (c)(3)(A)(v)-(vi).[55] In addition, the plaintiff failed to provide eBay with sufficient information to allow the service provider to identify the auction listings that allegedly offered pirated copies of "Manson" for sale. This failure further rendered Hendrickson's notice improper under the DMCA.[56] Therefore, the court ruled, eBay was under no obligation to remove the allegedly infringing material on its system.[57] The court went on to consider eBay's eligibility for safe harbor under § 512 (c), and determined that it satisfied all the statutory

---

[49] *Id.* at 624-625. 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.

[50] *Id.* at 620. (Emphasis in original.)

[51] 165 F. Supp.2d 1082 (C.D. Cal. 2001).

[52] *Id.* at 1085.

[53] *Id.*

[54] *Id.* at 1089.

[55] *Id.* at 1089-1090.

[56] *Id.* at 1090-1092.

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

conditions. The DMCA thus having shielded eBay from liability, the court granted eBay summary judgment on the copyright infringement claim.[58]

Ellison v. Robertson is another case that granted safe harbor to the defendant service provider.[59] Without authorization by the copyright owner, Stephen Robertson electronically scanned and converted into digital "binary" files[60] several science fiction novels written by Harlan Ellison. Robertson then uploaded and copied the files onto USENET newsgroups that are carried by several ISPs, including American Online, Inc. (AOL).[61] AOL's retention policy provided that USENET messages containing binary files remain stored on the company's servers for fourteen days.[62] 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 contributory copyright infringement suit against AOL and other parties. The *Ellison* court found that AOL's failure to receive the plaintiff's e-mail notification was due to its own fault in not promptly updating its "designated agent" contact e-mail address with the Copyright Office.[63] Due to this error, the e-mail sent by the plaintiff was routed to a defunct e-mail account. The court refused to permit AOL to disclaim knowledge of the infringement[64] on account of its own carelessness: "If AOL could avoid the knowledge requirement through this oversight or deliberate action, then it would encourage other ISPs to remain willfully ignorant in order to avoid contributory copyright infringement liability."[65]

After finding a triable issue of fact as to AOL's liability for contributory copyright infringement, the *Ellison* court proceeded to consider AOL's safe harbor defenses. As a threshold determination, the court held that AOL had complied with § 512(i) in adopting and implementing a termination policy for repeat infringers.

---

[58] *Id.* at 1094.

[59] *Ellison*, 189 F.Supp.2d 1051 (C.D.Ca. 2002).

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

[61] "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." 189 F.Supp.2d at 1053.

[62] 189 F.Supp.2d at 1054.

[63] *Id.* 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@aol.com" in fall 1999, but waited until April 2000 to notify the Copyright Office of the change.

[64] 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).

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

Despite the plaintiff's argument that no AOL user has ever been terminated for being a repeat infringer and therefore AOL's termination policy was inadequate, the court referred to the legislative history of the DMCA to find that § 512(i) "does not require AOL to *actually terminate* repeat infringers" but rather "requires AOL to put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights."[66]

The *Ellison* court then examined AOL's claim to safe harbor under both § 512 (a), the transitory digital network communications subsection, and § 512(c), information residing on systems or networks at direction of users. The court found that AOL's fourteen-day retention of Robertson's posts on its USENET servers "constitute[d] 'intermediate and transient storage' that was not 'maintained on the system or network ... for a longer period than [was] reasonably necessary for the transmission, routing or provision of connections."[67] The court was satisfied that AOL met the remaining criteria under § 512(a).[68] Emphasizing that § 512(n) explicitly provides that each of the four safe harbors "describe separate and distinct functions for purposes of applying this section [§ 512]," the court did not feel the need to analyze AOL's § 512(c) eligibility.[69] Once the *Ellison* court found that AOL qualified for a § 512 (a) liability limitation defense, it granted summary judgment for the service provider.

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 (RIAA)'s highly publicized efforts to take legal action against individual computer users who use peer-to-peer software to share copyrighted music files.[70] 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."[71] The clerk's issuance of the subpoena depends on the filing of the specified information in the subpoena request:[72]

---

[66] *Id.* at 1065-1066. (The court referred to H.Rept. 105-551, pt. 2 at 61.)

[67] *Id.* at 1070.

[68] *Id.* at 1071-1072.

[69] *Id.* at 1072, citing 17 U.S.C. § 512(n).

[70] 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.

[71] 17 U.S.C. § 512(h)(3)-(4).

[72] 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.

- 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.[73] 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.[74] Indeed, Congress' intent is expressly reflected in the statutory language itself, where the word "expeditiously" appears twice in the subpoena procedure section.

In re Verizon. 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.[75] 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, but rather on its subscribers' computers.[76] 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.[77] 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,[78] and that the DMCA subpoena power was constitutional.[79] 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.[80] A day later, Verizon revealed the names of four subscribers suspected of copyright infringement.[81]

---

[73] 17 U.S.C. § 512 (h)(5).

[74] H.R. CONF. REP. NO. 105-551, pt. 2, at 61.

[75] *Verizon*, *supra* note 6; In re Verizon Internet Services, Inc., 257 F. Supp.2d 244 (D.D.C.), *rev'd sub nom.* Recording Industry of American v. Verizon, ___F.3d___, 2003 WL 22970995 (D.C.Cir. 2003).

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

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

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

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

[80] 2003 WL 21384617 (D.C.Cir. Jun 04, 2003) (NO. 03-7015, 03-7053).

[81] *See* Christopher Stern, *Verizon Identifies Download Suspects*, WASHINGTON POST, June

(continued...)

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."[82] 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."[83] 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."[84] 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."[85] 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)."[86]

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.[87] Armed with this information, the RIAA promised to file what could be thousands of lawsuits against particularly egregious P2P swappers of copyrighted music.[88] 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,[89] as did several universities that were recipients of RIAA

---

[81] (...continued)
6, 2003, at E05.

[82] 240 F. Supp.2d at 40-41.

[83] *Id.* at 41, footnote 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..."

[84] *Verizon,* 257 F. Supp.2d at 260-261.

[85] *Id.* at 263.

[86] *Id.* at 265-266.

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

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

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

subpoenas.[90] 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."[91] Congress has expressed interest and concern over the issue as well. Several hearings were held.[92]

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 upholding the RIAA subpoenas.[93] The reversal was predicated on the 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

---

[90] On Aug. 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 PATENT, TRADEMARK & COPYRIGHT J. 458 (Aug. 15, 2003).

[91] *Letter from Kevin S. McGuiness, Exec. Director of NetCoaliton.com to Cary Sherman, Pres., RIAA* (Aug. 11, 2003) at [http://www.netcoalition.com/keyissues/2003-08-11.453.pdf]

[92] *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,* 108th Cong. 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.

[93] Recording Industry Assoc. of American v. Verizon Internet Services, ___F.3d___, 2003 WL 22970995 (D.C.Cir. 2003).

locate the material[.]"[94] 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.[95]

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.[96] "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 web site stored in the ISP's server, or as an information locating tool hosted by an ISP,[97] but *not* when it is routing infringing material to or from a personal computer owned and used by a subscriber.[98] 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 engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others."[99]

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.

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' attempt to address the liability concerns of service providers that operate the infrastructure of the Internet, as well as specify means by which service providers can cooperate with copyright owners to identify and deal with infringing users.

---

[94] 17 U.S.C. § 512(c)(3)(A)(iii) as referred to in subsection (h)(2)(A). (Emphasis added.)

[95] RIAA v. Verizon, 2003 WL 22970995 at *5.

[96] *Cf.* § 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 subscriber's account.

[97] § 512(b)-(d).

[98] § 512(a).

[99] RIAA v. Verizon, 2003 WL 22970995 at *6.

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 no where 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.[100] But P2P file-sharing technology developments raise far more serious privacy issues with a much wider sweep.

---

[100] *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).