# HARBORING DOUBTS ABOUT THE EFFICACY OF § 512 IMMUNITY UNDER THE DMCA

*By Jennifer Bretan*

Even as the Internet continues to evolve, Internet Service Providers ("ISPs") largely remain the gateway through which end users access the vast flow of digital content traveling throughout cyberspace. ISPs also host web pages, forward and process listserv messages, newsgroups and email, provide online chat venues, and link users to the infinite array of sites and services which, together, comprise the Internet.[1] End users themselves, however, do not uniformly comply with copyright laws. Users can make and post digital reproductions of copyrighted works with ease, and access to those infringing materials acts as a magnet, drawing traffic to specific sites and service providers.[2] In hosting, routing, and linking to such sites or services, ISPs themselves become vulnerable to charges of copyright infringement, whether direct, contributory or vicarious.[3]

Without some measure of protection against potentially crushing liability, ISPs could no longer afford to provide the technological backbone that now supports the Internet.[4] Rather than continue its progression, absent structured immunity, the growth of the Internet might falter as bankrupted ISPs slowly disappear from the digital landscape.[5] In § 512 of the



1. *WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2180 Before the Subcomm. on Courts and Intellectual Prop., House Comm. on the Judiciary*, 104th Cong. (1997) (statement of Roy Neel, President and Chief Executive Officer, United States Telephone Association) (discussing access and content provided by Telco ISPs).

2. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001); *See also* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.01[C] (2002) (discussing the ease with which works can be pirated and distributed on the internet).

3. *See* NIMMER, *supra* note 2, § 12B.01[A] (discussing the difficulty in determining which party should be liable for copyright infringment on the internet: the poster, the user accessing the material, or the service provider making access possible).

4. Neel, *supra* note 1 ("[W]hile USTA members are committed to the Internet, the threat of copyright lawsuits is becoming an increasingly salient consideration in offering the service at all.").

5. *See* NIMMER, *supra* note 2, § 12B.01[C] ("[H]aving a profusion of copyrighted works available will not serve anyone's interest if the Internet's backbone and infrastructure are sued out of existence for involvement in purportedly aiding copyright infringe-

Digital Millennium Copyright Act ("DMCA"), Congress explicitly carves out a number of safe harbors to shield ISPs from such liability.[6] The intent was to strike an appropriate balance between "securing copyright in the global, digital environment," and the need to provide protective limitations on liability for ISPs "in order to attract the substantial investments necessary to continue the expansion . . . of the Internet."[7]

Part I of this Note briefly describes how the pre-DMCA case law necessitated ISP immunity and how the decision in *Religious Technology Center v. Netcom On-Line Communication Service, Inc.*[8] ultimately provided the basis for structuring such immunity under the DMCA. Part II discusses the basic framework of § 512, as enacted, and how courts have begun to erode the intended protections of its safe harbors. Part III analyzes recent judicial decisions applying the § 512 provisions and uses them to illustrate what seem to be fast-developing statutory reinterpretations of the ISPs' responsibilities under the DMCA.[9] Lastly, Part IV attempts to reconcile the decisional erosion of the safe harbors and provide some guidance for ISPs who still hope to garner the valuable, but perhaps fleeting, protections of § 512.

## I. THE HISTORICAL NEED FOR ISP IMMUNITY

### A. The Ease of Copyright Infringement in the Digital Age Necessitates Legislative Intervention

The Internet opened a digital floodgate through which millions of reproductions of "movies, music, software, video games and literary and graphic works that are as good as the originals" travel daily from end user to end user.[10] Given the sheer volume of this information, traditional notions of policing copyright became outmoded. ISPs cannot monitor or judge copyright validity with even a modicum of efficacy given the "explosion of new ways to use wires, cables or other communication chan-

---

ment. Without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet.").

6. 17 U.S.C. § 512 (2000).

7. 144 CONG. REC. S11,887-92 (daily ed. Oct. 8, 1998) [hereinafter CONG. REC. S11,887-92] (statement of Sen. Hatch) (discussing the need for clarification and limitation on liability for ISPs in the DMCA).

8. 907 F. Supp. 1361 (N.D. Cal. 1995).

9. *See* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002); Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002); Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

10. CONG. REC. S11,887-92, *supra* note 7.

nels."[11] Moreover, although ISPs built the infrastructure of the Internet, they still function in large part as mere conduits for content originating with and driven by users.[12] Unable to police effectively and, by design, likely unaware of the infringing nature of the great balance of content, ISPs would face unlimited liability if courts decided to impute the infringing acts of users to the ISP.[13]

### B. The *Netcom* Decision: A New Direction on Liability Analysis and a Move Toward Safe Harbors for ISPs

In a prescient opinion, the district court in *Netcom*[14] recognized that "carried to its natural extreme," imputing acts of direct infringement to ISPs based on third party conduct "would lead to unreasonable liability."[15] In *Netcom*, a user posted copyrighted material of the Church of Scientology on a Usenet newsgroup that was connected to the Internet through the ISP.[16] The *Netcom* court rejected the liability analysis previously undertaken by courts in *Playboy Enterprises, Inc. v. Frena*[17] and *Sega Enterprises, Ltd. v. Maphia*[18] that found ISPs responsible for the infringing conduct of their users. *Frena* installed a strict liability regime and held a computer bulletin board (BBS) operator guilty of direct infringement where users had uploaded and downloaded copyrighted photographs without its knowledge.[19] Similarly, in *Sega*, liability attached where a BBS operator provided the venue for trading copyrighted computer games.[20] The deci-

---

11. *See* NIMMER, *supra* note 2, § 12B.01[A] (analogizing the liability of Internet ISPs to that previously feared by telephone companies as passive conduits).

12. *See generally id.* § 12B.01[C][1] (discussing how ISP fear of liability for user driven piracy over the Internet infrastructure drove the need for immunity).

13. *See generally id.* § 12B.01[B][2] (discussing ISP concern over duty to police the Internet for infringement and how "it would be unreasonable to expect the ISPs to act as the 'Internet Police' with respect to the copyright materials owned by everyone on earth").

14. 907 F. Supp. 1361 (N.D. Cal. 1995).

15. *Id.* at 1369.

16. *Id.* at 1365-66.

17. 839 F. Supp. 1552 (M.D. Fla. 1993).

18. 857 F. Supp. 679 (N.D. Cal. 1994).

19. 839 F. Supp. at 1554. The court held that the BBS engaged in public distribution and display of the infringing photos and, in denying a fair use defense, noted that Frena, the BBS provider, derived a commercial benefit from the subscription based service. Even though takedown was immediate, a monitoring policy to prevent future abuses was implemented, and the ISP was wholly unaware of the offending conduct and content. *Id.* at 1556-59.

20. 857 F. Supp. 679, 686-87 (N.D. Cal. 1994). Direct infringement was established under a strict liability scheme akin to that discussed in Frena. In Sega, the court additionally held that "even if Defendants do not know exactly when games will be uploaded to

sions were illustrative of the need for some measure of ISP protection in the new digital paradigm. Although the ISP in *Sega* was arguably more culpable than in *Frena*, appearing to have actively encouraged users to share copyrighted material, the larger implication of the decision caused alarm for ISPs. Carried to its logical conclusion, any ISP providing services capable of significant infringing use could be found liable.[21]

Despite *Frena* and *Sega*'s portent of debilitating liability for ISPs, *Netcom*'s policy reasoning and analysis of legal accountability created a significant limit on ISP liability.[22] Because a finding of direct infringement would "result in liability for every single Usenet server in the worldwide link of computers transmitting [the infringing] message to every other computer," the *Netcom* court held liability better resolved under "the rubric of contributory infringement," a schema more capable of addressing the complex relationship between ISPs and subscribers[23] In stark contrast to *Frena*'s direct infringement regime, under *Netcom*, a claim for contributory infringement is made out if the ISP knew or should have known of the infringement and had substantially induced, caused, or contributed to that conduct.[24] A claim of vicarious liability could likewise be sustained where the right or ability to control the infringing conduct exists and financial benefit, directly attributable to the infringing content, accrues to the ISP.[25]

---

or downloaded from the MAPHIA bulletin board, their role in the copying, including provision of facilities, direction, knowledge and encouragement, amounts to contributory copyright infringement."

21. *See* NIMMER, *supra* note 2, § 12B.01[A] (raising the hypothetical scenario of a BBS which is largely used for noninfringing purposes, but with the same level of infringing activity as in Sega).

22. Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1369 (N.D. Cal. 1995).

23. *Id.*

24. *Id.* at 1382.

25. *Id. But see* David L. Hayes, *Copyright Liability of Online Service Providers (pt. 2)*, 19 THE COMPUTER & INTERNET LAW. Nov. 2002, at 15, 19. Although Hayes notes that at least one court relied on Netcom to establish no direct financial benefit where an ISP charged a flat fee for its services, Hayes suggests that the Netcom holding, which heavily relied on the district court ruling in Fonovisa, has been imperiled by subsequent findings. Namely, the Ninth Circuit's reversal on the issue of financial benefit in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (establishing sufficient benefit to auction owners based on admission fees and concession sales) and a similar result in A&M Records Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (establishing financial benefit based on the draw that infringing content has on users of the service) make any future reliance by ISPs on Netcom to establish no financial benefit a more risky proposition.

## II. THE BASIC FRAMEWORK AND APPLICATION OF § 512

In 1998, Congress adopted § 512 of the DMCA, a legislative attempt to formalize structured immunities for ISPs, clarify the rights of copyright holders, and otherwise react to infringing content and conduct plaguing the Internet's new digital regime.[26] Section 512 creates safe harbor provisions to safeguard ISPs operating in their ordinary functions, a move to protect service providers from the type of liability that could have led them to "hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet."[27]

### A. The Provisions of § 512

Section 512 "clearly define[s] the conditions under which" ISPs may be held liable for copyright infringement and creates four safe harbor provisions to shield ISPs from damages.[28] Each provision provides protection for a distinct ISP function.[29] Congress adapted the basic structure of *Netcom*'s policy analysis on direct infringement, exempting providers for the automated transmission of third party infringement, as the first safe harbor in § 512(a).[30] As codified, it grants immunity where ISPs "[take] no 'affirmative action that [directly results] in copying . . . works other than by installing and maintaining a system whereby software automatically forwards messages received from subscribers . . . and temporarily stores copies on its system.'"[31] *Netcom*'s analysis of contributory and vicarious liability were similarly formalized and clarified within § 512, though without reference to specific technologies.[32] The enumerated safe harbors describe distinct functions and their application requires separate analyses

26. 17 U.S.C. § 512 (2000); *see also* Perfect 10, Inc. v. Cybernet Ventures, Inc, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002); Hayes, *supra* note 25, at 21-24 (discussing the legislative history which lead to the codification of ISP immunity in § 512 of the DMCA).

27. *See* NIMMER, *supra* note 2, § 12B.01[C][1] (discussing the need for § 512's limitations on liability so that ISPs would continue to build out of the Internet).

28. Hayes, *supra* note 25, at 22.

29. *Id.*

30. H.R. REP. NO. 105-551, pt. 1, at 26 (1998) ("Section 512(a)(1) . . . codifies the result of Religious Technology Center v. Netcom On-line Communications Services, Inc. . . . with respect to liability of providers for direct infringement.").

31. *Id.* (quoting Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1368 (N.D. Cal. 1995)).

32. 144 CONG. REC. E160-61 (daily ed. Feb. 12, 1998) (statement of Rep. Coble) (the elements of vicarious infringement are set out in § 512(c)(1)(B) and the actual or constructive knowledge requirement of contributory infringement in § 512(c)(1)(A)(i)-(ii)).

according to the criteria of the relevant subsection.[33] Failure to gain immunity for a function detailed by one safe harbor does not preclude a finding of immunity under another provision for ISPs performing more than one functional role.[34] Importantly, safe harbor disqualification does not make out a prima facie case of infringement, so service providers may still defend under applicable copyright law.[35]

*1. The Eligibility Threshhold of § 512*

To qualify for immunity under any safe harbor, § 512(i) obligates ISPs to meet two threshold requirements.[36] First, the ISP must "[adopt] and reasonably [implement]" a termination policy for repeat infringers and inform its subscribers of that policy.[37] Second, the ISP must accommodate and refrain from interfering with the standard technical measures copyright holders utilize in protecting works in the digital environment.[38] Though seemingly innocuous, the § 512(i) eligibility requirements have become a point of contention in recent caselaw, a development that this Note addresses more thoroughly throughout.

*2. The Four Functions Immunized Under § 512*

Once eligible, § 512 allows ISPs to function generally unfettered in four main operative roles. Under the statutory scheme, an ISP garners protection from damages for: a) transitory digital network communications; b) system caching; c) information residing on systems or networks at [the] direction of users; and d) providing information location tools.[39]

a) Transitory Digital Network Communications

ISPs provide the basic infrastructure of the Internet and, in that capacity, are shielded from liability under § 512(a), the first safe harbor provision.[40] Simply put, this section immunizes ISPs that are acting as mere

33. 17 U.S.C. § 512(n) (2000) ("Whether a service provider qualifies for the limitation on liability in any one of the [safe harbor] subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other.").

34. *Id.*

35. *See* NIMMER, *supra* note 2, § 12B.06[B] (noting that ISPs may still defend conduct under the Copyright Act of 1976 such as through the affirmative defense of fair use).

36. § 512(i)(1)(A)-(B).

37. *Id.* § 512(i)(1)(A).

38. *Id.* § 512(i)(1)(B).

39. *Id.* § 512(a)-(d).

40. Section 512(a) protects those "entit[ies] 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

conduits for information.[41] A "transitory digital network [communication]" refers to "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider" at the initiation of third parties, including the ISP's intermediate or transient storage of that material.[42] The transmission of infringing works must occur automatically, cannot be selectively routed to specific recipients by the ISP, and may neither be retained on the system longer than is "reasonably necessary for the transmission, routing, or provision of connections" or have had its content modified by the ISP.[43] For example, an ISP would be protected when delivering email with infringing content.

b) System Caching

Section 512(b) and the remaining safe harbor provisions cover providers who deliver "online services or network access, or [operate] facilities therefor."[44] "System caching" refers to the process by which ISPs temporarily "[store] material on a system or network," as part of managing network performance, in order to "reduce network congestion generally" and speed access to popular sites.[45] The transmission must be initiated by a third party, transmitted through the system to a second user, and stored via automatic processes.[46] However, unlike protection for transitory communications, this subsection only limits liability for those service providers who, upon notification, "[respond] *expeditiously* to remove, or disable access to, the material that is claimed to be infringing."[47]

---

of the material as sent or received." § 512(k)(1)(A) (Definition as applied specifically to subsection 512(a) on Transitory Digital Network Communications). America Online and Earthlink are two paradigmatic service providers in this narrow category and garner the codified Netcom protection against direct infringement.

41. *See* NIMMER, *supra* note 2, § 12B.02[B] (identifying the first safe harbor provision as protecting those ISPs engaging in ". . . essentially conduit only functions.").

42. 17 U.S.C. § 512(a); *id.* § 512(a)(1).

43. *Id.* § 512(a)(2)-(5).

44. *Id.* § 512(k)(1)(B) (Definition of providers as applied to safe harbor categories other than (a), but inclusive of those as defined in subparagraph (A) above). Included within this class of service provider is a search engine such as Google or a multi-purpose content and linking service such as Yahoo.

45. *See* NIMMER, *supra* note 2, § 12B.03[A].

46. § 512(b)(A)-(C).

47. *Id.* § 512(b)(E) (emphasis added).

c) Information Residing on Systems or Networks at the Direction of Users

The safe harbor provision of § 512(c) for "information residing on systems or networks" limits ISP liability for content posted or hosted at the direction of end users.[48] Examples of functions covered within this safe harbor category include the storage of user home pages, Usenet and auction site postings, and chat rooms.[49] This provision protects those ISPs that receive no financial benefit "directly attributable to the infringing activity," where the provider has neither the right nor ability to control the activity and where, if properly notified, the ISP suppresses access to the infringing content.[50] However, it does not protect ISPs with actual or constructive knowledge of infringing content who do not, on their own initiative, move quickly to disable access.[51] Section 512(c) additionally details the need for ISPs to provide agents charged with handling infringement notifications on their behalf and enumerates the elements constituting notification sufficient to shift the liability burden back on to the ISP.[52]

d) Information Location Tools

Lastly, under § 512(d), ISPs are granted immunity for the "information location tools" that provide links to "online location[s] containing infringing material or infringing activity . . . including a directory, index, reference, pointer, or hypertext link."[53] Again, actual or constructive knowledge of the infringement proves fatal, though, as § 512(c) makes clear, takedown upon notification and the absence of direct financial benefit preserves the immunity.[54]

*3. Notice and Takedown*

Despite its explicit purpose of sheltering ISPs from unreasonable liability, § 512 also contains substantial protection for the rights of copyright holders. In order to reap the benefits of immunity, ISPs must institute systems of notice and takedown by which copyright holders can identify infringing material for ISP removal. First, the ISP must designate an agent

48. *Id.* § 512(c); *see* NIMMER, *supra* note 2, § 12B.04[B] (noting that the material may not appear by action or by decision of the service provider, but must be user directed).

49. *See* NIMMER, *supra* note 2, § 12B.04[B] (describing the types of functions covered).

50. § 512(c)(1)(B)-(C).

51. *Id.* § 512(c)(1)(A)(i).

52. *Id.* § 512(c)(1)(C)(2)-(3).

53. *Id.* § 512(d).

54. *Id.* § 512(d)(1)-(3).

to handle infringement claims.[55] To ease the burden on the copyright owner, the agent's contact information must be made readily available both through conspicuous placement on the ISP's own site and through registration with the Copyright Office.[56] Second, a written communication to the designated agent containing specific identifying elements constitutes effective notice.[57]

Once the copyright holder effects notice under the scheme, § 512 requires an ISP to remove or otherwise disable access to the allegedly infringing material identified in the claim.[58] To balance the risks of such pre-adjudicated termination, § 512 also ensures that the ISP cannot be held liable for taking the identified material down and provides an analogous counter notification procedure whereby a subscriber can challenge the infringement claim.[59]

*4. No Affirmative Duty to Police the Internet*

Section 512 imposes no affirmative duty on ISPs to police their vast systems in search of copyright infringement.[60] Section 512 also ensures that voluntary efforts to monitor do not result in forfeiture of the safe harbor limitations on liability.[61] However, the vagueness of the "reasonable implementation" standard may prove to be a back door requirement for ISPs to police. As noted earlier, the termination policy is a threshold to eligibility under § 512. Failure to implement that policy might lead a court to deny the ISP the benefit of the safe harbors. If strictly construed, the requirement of reasonable implementation may begin to look like an affirmative duty to both monitor and *actively* terminate infringers. As discussed in Part III infra, the recent decision in *Perfect 10, Inc. v. Cybernet*

---

55. *Id.* § 512(c)(2).

56. *Id.* § 512(c)(2)(A)-(B).

57. *Id.* § 512(c)(3)(i)-(vi). The elements of effective notification include: 1) a signature of a person authorized to act on behalf of the owner of the copyright allegedly infringed; 2) identification of the work infringed or a representative list of such works if multiple works exist at a single site; 3) identification of the infringing material and information sufficient to allow the ISP to locate it; 4) contact information of the complaining party; 5) a statement of good faith; 6) a statement of accuracy of the claim under penalty of perjury.

58. *Id.* § 512(c)(1)(C).

59. *Id.* § 512(g)(1)-(3).

60. *Id.* § 512(m)(1).

61. *See* NIMMER, *supra* note 2, § 12B.09[B] n.26 (discussing the Congressional desire not to discourage ISPs from undertaking monitoring for fear of losing the safe harbor immunities).

*Ventures, Inc.*,[62] where a court found that the ISP had not sufficiently acted on its termination policy, appears to suggest that active policing has become a virtual prerequisite to immunity within § 512's safe harbors.

### 5. *Remedies and Subpoena Powers Under § 512*

Once a service provider qualifies for safe harbor, monetary relief is not available to the copyright holder,[63] and the crushing liability ISPs anticipated prior to the DMCA is eliminated.[64] The court may, however, still award equitable relief even where the safe harbor provision has shielded the provider from damages.[65] Under § 512(j), injunctive relief may take the form of orders to restrict access to infringing material or particular sites on a system, orders to deny access or terminate subscribers "engaging in infringing activity," and any other injunctive action the court finds necessary to effectuate relief, so long as it is the "least burdensome to the service provider" of the available equitable remedies.[66]

While ISPs may qualify for immunity, the safe harbor provisions do not protect those end users "who take advantage of [the service provider's] facilities" to infringe copyrighted works.[67] Thus, § 512 allows the copyright owner to ask a district court to issue a subpoena requiring the ISP to reveal the identity of the alleged primary infringer.[68] The request must include a copy of 512(c) notification, a proposed subpoena, and a sworn declaration that the information sought is for the sole purpose of protecting copyright.[69] Upon subpoena, an ISP must quickly disclose the identity of the alleged infringing subscriber, whether or not it has determined that the content in question actually violates copyright.[70] Commentators note that the § 512 subpoena provisions are ripe for abuse, "particularly in circumstances involving competitors or critics" where copyright holders might use the subpoena powers to "investigate and gather information

---

62. *See* Perfect 10, Inc. v. Cybernet Ventures, Inc, 213 F. Supp. 2d 1146, 1179 (C.D. Cal. 2002) ("Because the Court finds that there is a strong likelihood that Cybernet cannot establish that it has "reasonably implemented" a policy directed at terminating repeat infringers . . . there is little likelihood that it can avail itself of § 512's safe harbors.").

63. 17 U.S.C. § 512(a)-(d) ("A service provider shall not be liable for monetary relief . . .").

64. Hayes, *supra* note 25, at 22.

65. § 512(j)(1).

66. *Id.* § 512(j)(1)(i)-(iii).

67. *See* NIMMER, *supra* note 2, § 12B.09[A] (noting that an end user engaging in copyright infringement remains fully liable).

68. § 512(h)(1).

69. *Id.* § 512(h)(2)(A)-(C).

70. *Id.* § 512(h)(5).

. . . that would not generally be available in the off-line world."[71] Both Wal-Mart's recent abuse of the subpoena power to obtain noncopyrightable price information and a recent subpoena asking the ISP Verizon to reveal the identity of an infringing subscriber despite the copyright holders' failure to conform with the requisite notification clearly justify those concerns.[72]

### B. Courts Block Easy Entry to the Safe Harbors: *Napster* and *ALS Scan*

Following the enactment of the DMCA, caselaw quickly began to erode the protections of § 512's safe harbors. In analyzing whether ISPs may avail themselves of those limitations on liability, courts in two recent cases failed to interpret the statutory protections so as to afford protection to service providers. In *Napster*,[73] the Ninth Circuit put the question of liability ahead of safe harbor defense consideration in forestalling protection and, in *ALS Scan Inc. v. RemarQ Communities, Inc.*,[74] the Fourth Cir-

---

71. *See* NIMMER, *supra* note 2, at § 12B.09[A] (quoting the Hearing Before the Subcommittee on Telecommunications, Trade, and Consumer Protection, Serial No. 105-102 (June 5, 1998), at 16 (statement of Electronic Privacy Information Center)).

72. *See* AScribe Newswire, *FatWallet Victorious in Challenge to Wal-Mart's Frivolous Digital Millennium Copyright Act Subpoena*, *available at* http://www.nyfairuse.org/dmca/wallmart.fw.xhtml (Dec. 5, 2002) ("Wal-Mart had sought the identity of the individual who posted Wal-Mart Day After Thanksgiving sales information on the FatWallet site . . . Wal-Mart obtained a subpoena from federal court under the DMCA after submitting a declaration under penalty of perjury that its sales prices were protected by copyright law. FatWallet.com objected to the subpoena on the grounds that the Supreme Court has ruled that facts cannot be copyrighted."); *see also* Declan McCullagh, *Music Body Presses Anti-Piracy Case*, CNET News.com, *at* http://news.com.com/2100-1023-954658.html (Aug. 21, 2002); Declan McCullagh, *Verizon, RIAA in Copyright Showdown*, CNET News.com, *at* http://news.com.com/2100-1023-960838.html (Oct. 4, 2002); Reuters, *Verizon Questioned Over File Swapping*, CNET News.com, *at* http://news.com.com/2100-1023-960935.html (Oct. 5, 2002). On January 21, 2003, Verizon was ordered by the district court to turn over the subscriber information as per the subpoena. U.S. District Judge John D. Bates ruled that Congress could not have intended that the DMCA would "enable a copyright owner to obtain identifying information from a service provider storing the infringing material on its system, but would not enable a copyright owner to obtain identifying information" from an ISP merely transmitting such information. *See* Jonathan Krim, *Recording Firms Win Copyright Ruling*, *at* http://www.washingtonpost.com/wpdyn/articles/A24577-2003Jan21.html (Jan. 22, 2003); *see also* Amy Harmon, *Verizon Ordered to Give Identity of Net Subscriber*, *at* http://www.nytimes.com/2003/01/22/technology/22MUSI.html (Jan. 22, 2003). Verizon is appealing the decision. *See* Declan McCullagh, *Verizon Appeals RIAA Subpoena Win*, CNET News.com, *at* http://news.com.com/2100-1023-982809.html (Jan. 30, 2003).

73. 239 F.3d 1004 (9th Cir. 2001).

74. 239 F.3d 619 (4th Cir. 2001).

cuit rendered a substantially relaxed reading of the notification requirements under § 512(c) in a decision that shifts a good deal of the copyright holder's infringement burden back onto the ISP.[75]

In common law copyright, the elements of vicarious liability are met if a defendant has the right and ability to supervise infringing activity from which it receives a direct financial benefit.[76] In finding vicarious liability likely, despite § 512(m)'s "no affirmative duty to police," the *Napster* court looked upon the peer-to-peer provider's ability to block access to material, or to otherwise terminate infringing users, as evidence that it had the right and ability, and ultimately, the responsibility, to control the infringement.[77] Although the legislative intent of § 512 was to encourage ISPs voluntarily to engage in monitoring,[78] *Napster* reveals the peril faced by ISPs who demonstrate an ability to do just that. The Ninth Circuit grounded its vicarious liability analysis of Napster's services by analogy to the *Fonovisa* swap-meet, in which the "'ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise,"[79] and direct financial benefit adheres where "the availability of infringing material 'acts as a "draw" for customers.'"[80]

Rather than defaulting to an analysis of limitation on liability under § 512, the appeals court in *Napster* put the likelihood of liability first, leaving any significant consideration of the safe harbor defenses for development at trial, and remanded to the district court for modification of the preliminary injunction.[81] To the extent that the Ninth Circuit did consider § 512, it suggested Napster might not fit the categories of providers covered, questioned the need for § 512(c) official notice, and raised doubt about Napster's threshold eligibility because it failed to comport with the court's notion of a reasonably implemented termination policy for recidi-

---

75. Alan S. Wernick, ISP's Could Not Rely on Immunity in Two Cases, 23 NAT'L L.J. 38 (2001).

76. *Napster*, 239 F.3d at 1022 (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

77. *Id.* at 1027 ("Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. . . . Napster . . . also bears the burden of policing the system within the limits of the system.").

78. *See* NIMMER, *supra* note 2, § 12B.01[C][[1] (noting that an end user engaging in copyright infringement remains fully liable).

79. *Napster*, 239 F.3d at 1023 (citing Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996)).

80. *Id.* at 1023 (quoting *Fonovisa*, 76 F.3d at 263-64).

81. *Id.* at 1029.

vist infringers.[82] It remains unclear why both the district court and the Ninth Circuit chose to bypass the DMCA safe harbors, where injunctive remedies are clearly available, and to order equitable relief outside the § 512 regime.

Access to safe harbor protections continued to erode in *ALS Scan* when the Fourth Circuit took a less stringent view of compliance with § 512(c)'s notification procedures.[83] In that case, users of the ISP RemarQ posted and accessed newsgroup listings containing hundreds of infringing copies of pornographic photos owned by copyright holder ALS Scan.[84] Technically, ALS Scan failed to comply with § 512(c) notice and did not specify the "identity of the pictures forming the basis of the copyright claim."[85] Rather, the court based liability on the mere provision of what it considered information sufficient to locate infringing content, reasoning that the safe harbor immunities are "not presumptive, but granted only to 'innocent' service providers who can prove that they do not have actual or constructive notice."[86] In holding that the copyright owner need not identify infringing content with specificity, *ALS Scan* suggests ISPs may shoulder a much greater burden than originally contemplated in § 512.[87] Where ISPs are forced to determine which works might infringe, chilling effects may follow. Unsure of copyright status, ISPs will likely take down questionably infringing content.[88] Ultimately, the court's denial of the safe harbor in *ALS Scan* shows that "failure to respond properly and expeditiously to even an *imperfect* DMCA notification can be perilous."[89]

Together, *Napster* and *ALS Scan* illustrate the trend toward dismantling the legislative safe harbors and imposing a duty to police the Internet

---

82. *Id.* at 1025. (questioning Napster's ability to invoke § 512 because it believed significant questions existed as to: "(1) whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give a service provider "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with § 512(i), which requires a service provider to timely establish a detailed copyright compliance policy.").

83. ALS Scan, Inc. v. Remarq Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001).

84. *Id.* at 620-21.

85. *Id.* at 622.

86. *Id.* at 625 (noting the knowledge prongs of secondary liability).

87. *See generally* NIMMER, *supra* note 2, § 12B.04[B][[4] (discussing notification procedures and the Fourth Circuit's departure in ALS Scan from strict adherence to the statutory requirements under § 512(c)).

88. *ALS Scan*, 239 F.3d at 624 (ALS Scan's notice directed RemarQ to two newsgroups containing infringing copies of its images, but "not all materials at the offending sites contained material to which ALS Scan held the copyrights.").

89. Wernick, *supra* note 75, at 39 (emphasis added).

for infringement where § 512 demands none. Against a growing storm of adverse adjudication, it is questionable whether § 512 ultimately provides the kind of protection ISPs originally sought.

## III. TRENDS: COURTS INTERPRET AND APPLY § 512

The DMCA is a relatively new statute and a major body of caselaw has yet to develop to help guide courts in interpreting and applying its provisions. As this Note demonstrates, every case that analyzes, provides insight, or otherwise clarifies how courts should treat § 512 is therefore significant. In this light, three recent cases in which ISPs defended under § 512 immunity contribute to the ever-evolving picture of how the safe harbor provisions function under the DMCA.[90] In part, each case either relies on or makes reference to decisions that precede it. This Note addresses some of the more salient developments contained in the opinions.

### A. Hope for the Specific Notice Requirements of § 512(c)

A recent judicial reiteration of the burden of copyright holders to notify with specificity contains encouraging signs that *ALS Scan*'s relaxed notice standard may yet prove to be an anomaly. In *Hendrickson v. eBay*,[91] a copyright owner sought damages from the Internet auction site, claiming that "pirated DVD copies of [his documentary film] 'Manson' . . . were being offered for sale on eBay."[92] Prior to suit, plaintiff sent eBay a general cease and desist letter, but "did not explain which copies of 'Manson' . . . were infringing copies [and did not] fully describe [Hendrickson's] copyright interest."[93] Following the letter, eBay described its termination procedure to Hendrickson and requested proper notice under the DMCA, including the need for him to "identify the exact items" believed to infringe his rights.[94] Hendrickson "refused to fill out eBay's Notice of Infringement form" and never provided eBay with the identifying information it sought.[95] After analyzing eBay's potential liability under the

90. *See* Perfect 10, Inc. v. Cybernet Ventures, Inc, 213 F. Supp. 2d 1146 (C.D. Cal. 2002); Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002); Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

91. 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

92. *Id.* at 1084-86. Three suits were filed and later consolidated.

93. *Id.*

94. *Id.* at 1085. (noting that the request for identification was possible because "each listing on eBay's website has its own item number").

95. *Hendrickson*, 165 F. Supp. 2d at 1085.

DMCA safe harbors, the court granted summary judgment in favor of the auction site provider.[96]

Although eBay argued for functional immunity under both §§ 512 (c) and (d), the court limited the factual analysis to § 512(c) alone because it believed that the functions at issue qualified as "infringement . . . by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."[97] The court identified three requirements for invocation of § 512(c): 1) that the ISP has neither actual nor constructive knowledge of the infringement or, if it did have knowledge, it disabled access to the material;[98] 2) that the ISP has not directly benefited, where it had the right or ability to control the infringing activity;[99] and, most relevant here, 3) that the ISP quickly removed the allegedly infringing material "upon notification . . . as described in [§ 512(c)(3)]," the subsection that defines the elements of proper notification.[100]

The *Hendrickson* court considered a copyright holder's failure to satisfy the requirements of proper notification by identifying infringing material insufficient to trigger the ISP's duty to act.[101] Unlike the result in *ALS Scan*, in *Hendrickson*, deficient notice could not be used to impute legal knowledge, so as to shift the liability burden back onto the ISP.[102] In concluding that the rigors of the DMCA's notification procedure had not been substantially met, the court cited the lack of a good faith statement and failure to identify the pirated goods with a high degree of specificity as the key missing elements.[103] *Hendrickson* also departs from *ALS Scan*'s presumption that a copyright holder may point to the infringement in a general manner, holding that absent communication that *all* Manson DVDs infringe, specific item numbers are "necessary to enable eBay to identify problematic listing."[104]

---

96. *Id.* at 1086.

97. *Id.*

98. *See id.* at 1088.

99. 17 U.S.C. §§ 512(c)(1)(A)-(C) (2000) (the vicarious liability codification).

100. *Id.* § 512(c)(1)(C).

101. *Hendrickson*, 165 F. Supp. 2d at 1089 (listing the six elements of proper notification contained in § 512 (c)(3)).

102. *Id.*

103. *Id.* at 1089-92.

104. *Id.* at 1090. The court noted that although the plaintiff claimed to have communicated that all "Manson" DVDs infringed his copyright, his failure to put the claim in writing, as required by § 512(c)(3)(A), prevents court consideration of that evidence. The decision stands in contrast to the ALS Scan court's allowance that a representative list of infringing material would suffice.

Having concluded that eBay had no duty to act by reason of notification, the court turned to the knowledge prong of § 512(c)'s safe harbor. Though the *ALS Scan* court might not have concluded eBay had actual or constructive knowledge of the infringing activity, the *Hendrickson* court quickly disposed of the issue, emphasizing that under § 512, failed notification "shall not be considered . . . in determining whether a service provider has actual" or constructive knowledge.[105] Because Hendrickson failed to identify infringing activity with particularity, the court found the notice to be deficient and, as a result, that eBay did not have legal knowledge prior to suit.[106]

A California district court addressed § 512 immunities in *Ellison v. Robertson*.[107] Robertson scanned copies of Ellison's science-fiction novels into digital format and uploaded them to a USENET newsgroup carried through peer agreement by several ISPs, including AOL.[108] Through dicta, *Ellison* illustrates how a copyright holder may properly invoke the § 512(c) notification procedure to alert the ISP of a violation and how courts will protect the copyright interest if ISPs fail to act upon notification.[109] Upon learning of the infringing activity, Ellison researched the DMCA notification procedures and had his counsel email AOL's designated agent with the required information.[110] Receiving no response from AOL, plaintiff filed suit against Robertson, AOL, and two other ISPs on theories of direct, contributory, and vicarious infringement.[111] Prior to resolution of this action, Ellison not only settled with and dismissed defendant Robertson, the primary infringer, but more significantly, reached similar agreements with defendant RemarQ (the ISP that had provided Robertson's access to the USENET servers) and its parent company Critical Path.[112] The ISP settlements are notable primarily because they may

105. *Id.* at 1092-93.

106. *Id.*

107. 189 F. Supp. 2d 1051 (C.D. Cal. 2002).

108. *Id.* at 1053-54. (The newsgroup in question was "alt.binaries.e-book" which appeared to carry "unauthorized digital copies of text material, primarily works of fiction by famous authors, including Ellison."). Message postings to the newsgroups are automatically transmitted to peer ISPs and, in the case of AOL, were retained on the "company's servers for fourteen days." *Id.* at 1054. Although Robertson was not an AOL subscriber, once he uploaded his infringing copies to a newsgroup, "they were then forwarded and copied throughout USENET and onto servers all over the world, including those belonging to AOL." *Id.*

109. *Id.* at 1054.

110. *Id.*

111. *Id.* AOL claimed it never received the e-mail, but shut down access to alt.binaries.e-book following service of the suit.

112. Ellison v. Robertson, 189 F. Supp. 2d 1051, 1054 (C.D. Cal. 2002).

reflect a concern, following RemarQ's experience in *ALS Scan*, that access to the safe harbors is easily obstructed by the courts. AOL remained in the case, however, and moved for summary judgment, claiming it had not infringed and invoking the § 512 defenses to shield it from liability.[113]

The *Ellison* court followed *Netcom* in first rejecting a direct infringement claim, citing "AOL's role . . . as a passive provider of USENET access . . . [that does] no more than operate or implement a system that is essential if Usenet messages are to be widely distributed."[114] The court found unworkable a theory of direct infringement holding the "entire Internet liable for activities that cannot reasonably be deterred."[115] After disposing of direct infringement, however, *Ellison* turned to the issue of contributory infringement: knowledge of, and inducement, causation, or material contribution to infringing activity.[116] In the court's opinion, AOL had reason to know of the infringement because the court found that AOL's failure to post the correct email address of its designated agent was responsible for the ISP never having received Ellison's notification.[117] The court refused to allow AOL's oversight to exempt it from knowledge, for fear of "encourag[ing] other ISPs to remain willfully ignorant in order to avoid contributory copyright infringement liability."[118] The *Netcom* court had held that a material contribution exists where an ISP providing Usenet access had knowledge of infringement but continued to carry the infringing postings.[119] The *Ellison* court refused to distinguish *Netcom* on the basis that AOL did not have actual knowledge in continuing to allow access to the infringing activity, because it reasoned that an ISP is equally culpable where it merely *would have known* of the infringement had it received the notification.[120] Accordingly, the court believed a triable issue of fact existed as to the contributory infringement claim.[121] The finding demon-

113. *Id.*
114. *Id.* at 1056-57.
115. *Id.* at 1057.
116. *Id.*
117. *Id.* at 1057-58. AOL had changed its email address from "copyright@aol.com" to "aolcopyright@aol.com" and did not notify the Copyright Office of the change until several months later. The ISP additionally failed to arrange for messages sent to the old contact address to be forwarded to the new one. Some question exists as to why this failure to abide by the notice provisions of § 512(c) alone did not prevent the ISP from invoking the safe harbors of the DMCA.
118. *Id.* at 1058.
119. *Id.* at 1059 (citing *Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc.*, 907 F. Supp. 1361, 1376 (N.D. Cal. 1995)).
120. *Id.*
121. *Id.*

strates that proper notification can defeat the safe harbor where protection is unwarranted and an ISP likely to be liable.[122]

Likewise, in a reassertion of the need for ISPs to abide by § 512(c)'s notice provisions, the recent court decision to withhold safe harbor protections in *Perfect 10, Inc. v. Cybernet Ventures*[123] rested in part on the fact that the ISP had a policy that deviated significantly from the DMCA notification and takedown requirements.[124] Because Cybernet altered the DMCA notice requirements, demanding that a copyright holder meet *all* of the service provider's stated procedures including its refusal to allow a representative list of infringing works to suffice as notice, the court found "an intent [by the ISP] to upset the Congressionally apportioned burden between copyright holder and service provider."[125]

Viewed in concert, *Hendrickson*, *Ellison,* and *Perfect 10* can be seen as a powerful judicial re-entrenchment of the need for strict adherence to § 512(c)'s notification requirement. Despite *ALS Scan*, the cases demonstrate that the burden of notice is a two way street and, if properly followed, can be used to balance ISP liability as Congress intended.

### B. The Detrimental Effect of Allowing a Liability Analysis to Precede Consideration of the Safe Harbors

Courts appear conflicted over whether a common law analysis of copyright infringement should precede analysis under the safe harbor defenses. Similar to *Napster's* reliance on the *Fonovisa* swap meet analogy, the *Hendrickson* court identified the key question on liability as "whether eBay can be held secondarily liable for providing the type of selling platform/forum and services . . . however limited or automated in nature" to third party infringers.[126] Unlike *Napster*, however, the court acknowledged that the issue of liability on the merits was a secondary consideration, and that "the Court must [first] address . . . whether the DMCA shields eBay from liability for copyright infringement."[127]

As an initial matter, the *Hendrickson* court noted that the purpose of the DMCA is to encourage and "facilitate the robust development and worldwide expansion of electronic commerce, communications, research,

---

122. *Id.*

123. 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

124. *Id.* at 1179.

125. *Id.* at 1180 ("Cybernet has failed to structure a notice system that complies with section 512.").

126. Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1087 (C.D. Cal. 2001).

127. *Id.* at 1087-88 (noting that the Napster court had put off consideration of the DMCA safe harbors).

development, and education," a goal accomplished in part by "protect[ing] qualifying Internet service providers from liability for all monetary relief for direct, vicarious and contributory infringement."[128] The court recognized that eBay fit the § 512 definition of a service provider and could therefore look to find shelter in its safe harbors.[129] The court believed that the legislative intent to shield ISPs was critical to an analysis of liability and that the analysis must therefore be undertaken only after a court first considers whether an ISP could, in fact, avail itself of those protections.

In contrast to *Hendrickson*'s mandate that consideration of a claim begins by looking to the § 512 immunities, the *Ellison* court engaged in the infringement analysis as its initial inquiry.[130] In this manner, the court relied on caselaw, rather than the statutory safe harbor provisions to frame the issues, an ordering that, as in *Napster*, allowed the court to focus on the likelihood of the ISP's liability from the outset, before ever taking the limitations of § 512 into account.[131]

In the third recent case to consider the interpretiation and application of § 512's limitations on liability, *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, the same misaligned result occurred, with liability analysis preceding and preemptively coloring consideration of the safe harbor provisions.[132] Defendant provider Cybernet Ventures ran an age verification service called "Adult Check" through which it permitted access to and collected payments for pornographic websites.[133] Plaintiff Perfect 10 discovered "more than 10,000 copies of Perfect 10 images" on websites affiliated with Cybernet's Adult Check system.[134] Perfect 10 filed for a preliminary injunction and, as in *Napster*, the first consideration of the likelihood of finding infringement informed the later assessment of whether the safe harbors might apply.[135]

---

128. *Id.* at 1088 (quoting the legislative history as contained in S. REP. NO. 105-190 (1998)).

129. *Id.* (including eBay in the broad category of providers of online services under § 512 (k)(1)(B)).

130. Ellison v. Robertson, 189 F. Supp. 2d 1051, 1056 (C.D. Cal. 2002).

131. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001). Only after allowing an injunction against Napster, having engaged in the infringement analysis, did the Ninth Circuit consider § 512, noting "We do not agree that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se. We instead recognize that this issue will be more fully developed at trial." *Id.*

132. 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

133. *Id.* at 1158.

134. *Id.* at 1162.

135. *Id.* at 1165.

The framing of the analyses in *Napster*, *Ellison*, and *Perfect 10* reveals that a finding of liability is more likely where the safe harbor provisions are not addressed first, and demonstrates that procedural clarification is imperative. An ISP should be able to access the safe harbors without courts first viewing its role through the lens of a common law infringement analysis. The cases have proven much less generous than the safe harbor provisions intended, and they dismantled the careful balance of responsibility Congress undertook in formulating § 512. *Hendrickson* alone ordered its review of liability correctly, relying on § 512 immunity as the initial inquiry.[136] Because no solid rule on the issue has developed, ISPs seeking to invoke the immunities run the risk of being tainted as infringers from the outset. In large part, as *Napster*, *ALS Scan* and *Perfect 10* make obvious, a court's inclination to view particular ISPs as bad actors seems to inform the way it chooses to engage and order its analysis.

### C. The Control Prong of Vicarious Liability Analysis under § 512 Combines with § 512(i)'s Threshold Eligibility Requirement and Begins to Look Like an Affirmative Duty to Police.

Viewed as a whole, the decisions in *Hendrickson*, *Ellison*, and *Perfect 10* illustrate the failure of § 512 to clarify ISP liability for copyright infringement in the digital domain. Emerging as the areas of greatest confusion are how the eligibility threshold of § 512(i) should be interpreted and what constitutes control so as to make out vicarious liability. Although *Ellison* concluded that § 512(i) merely requires ISPs to put customers on notice of the threat of termination for repeat infringement,[137] *Perfect 10* demonstrates that courts can also view the failure to have actually terminated infringers as a failure to reasonably implement that policy, and thereby deny ISPs the benefits of the safe harbors altogether.[138] How the *Perfect 10* holding can be reconciled with § 512(m)'s 'no affirmative duty to police' is in need of much greater development. The clear trend, however, seems to be a court expectation that ISPs are in fact monitoring and actively terminating repeat infringers, acts of control that seem to imply a backdoor duty to police.

In contrast to *Perfect 10*'s view that the ISP must exercise control, when it can, in order to pass the threshold requirements of § 512(i), the *Hendrickson* decision insists that voluntary policing by an ISP cannot be used to establish the right to control, perhaps by reason of the choice to

136. Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1087-88 (C.D. Cal. 2001).
137. Ellison v. Robertson, 189 F. Supp. 2d 1051, 1066 (C.D. Cal. 2002).
138. *Perfect 10*, 213 F. Supp. 2d at 1179.

look first at whether the safe harbor provisions are applicable.[139] Hendrickson contended that, in removing infringing listings in the past and monitoring its service daily for keywords that appear to signal infringing items, eBay demonstrates the right and ability to control that activity.[140] In addressing § 512(c)'s vicarious liability prong, the court stopped short of addressing direct financial benefit because it believed the "undisputed facts establish" that eBay was not in control of the infringement.[141] The court thus rejected plaintiff's contention as meritless.[142]

The *Hendrickson* court's analysis of the control issue clearly distinguishes *Napster*'s extension of *Fonivisa* to the Internet and contains significant language to limit that holding.[143] As contained in the DMCA, the court noted that the "right and ability to control" infringement "cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or server."[144] ISPs are required to take down infringing materials upon valid notice, and must also have implemented a policy for termination of repeat infringers under the eligibility threshold of § 512(i).[145] The court reasoned that "Congress could not have intended for courts to hold that a service provider loses immunity under the . . . DMCA because it engages in acts that are specifically required by the DMCA."[146] Moreover, the court noted that eBay's "voluntary efforts to combat piracy over the Internet" through limited monitoring cannot "lead the Court to conclude that eBay has the right and ability to control . . . within the meaning of the DMCA."[147] The court also found eBay's passive role in the "listing, bidding, sale and delivery of any item offered for sale on its website," compelling evidence that it had no control over the type of infringement at issue, namely the right to distribute.[148]

---

139. *Hendrickson*, 165 F. Supp. 2d at 1092-93.

140. *Id.* at 1093 (noting that eBay conducted searches using keywords such as "bootleg" and "counterfeit" and removed the listings if the staff determined that infringing goods were being offered").

141. *Id.*

142. *Id.*

143. *Id.* at 1093-94. Whereas Napster's ability to block or disable access was evidence of an ability to control and the basis of the ISPs likely liability, the court in Hendrickson did not consider eBay's similar acts sufficient reason to deny immunity under § 512.

144. *Id.* at 1093.

145. *Id.*

146. *Id.*

147. *Id.* (citing to the legislative history for the proposition that the DMCA is not intended to discourage such monitoring and that eligibility is not lost in the act.); *see* H.R. REP. NO. 105-796 (1998).

148. *Id.* at 1094.

*Hendrickson* illustrates how the safe harbor provisions, when properly considered, can provide great protection to ISPs. Liability ultimately turns on the court's interpretation of the DMCA provisions with regard to control. Had the court followed the Ninth Circuit's *Napster* logic, it would surely have found the safe harbor of § 512(c) unavailable and held eBay liable. Under a *Napster* analysis, it looks as though eBay had both the right and ability to control, as evidenced by its ability to police and terminate and that direct financial benefit could be easily established because eBay receives insertion fees and a cut of the final value achieved in each auction listing.[149]

The *Ellison* court similarly rejects both *Napster* and *Netcom*'s finding that an ability to block access or otherwise delete content demonstrates the ISP's right and ability to control and, instead, embraced *Hendrickson*'s analysis of the issue under the DMCA.[150] Thus the court found that "the DMCA requires more than the mere ability to delete and block access to infringing material after that material has been posted in order" to establish the right and ability to control the activity.[151] Moreover, the court further distinguished *Netcom* because, although newsgroup peers could "block users' access to the infringing postings . . . it could not do anything to restrict the infringing activity at the root level."[152] In other words, AOL had no direct control over the access of Robertson, the direct infringer in that case.[153] The court also found insignificant the financial benefit derived by the "draw" of infringing Usenet postings.[154] The court noted that "infringing activity must be at least a *substantial* draw" and that to "hold otherwise would provide essentially for limitless expansion of vicarious liability."[155] In general, the court held that direct financial benefit could

149. *Hendrickson*, 165 F. Supp. 2d at 1094-95. Worthy of some of mention was the court's extension of the safe harbor protections to employees of eBay, individually, for acts "committed in the course and scope of their employment." *Id.* In so holding, the court noted that "Congress could not have intended to shift the target of infringement actions from the [ISPs] to their employees when it enacted the safe harbor provisions." *Id.* at 1095.

150. Ellison v. Robertson, 189 F. Supp. 2d 1051, 1059-60 (C.D. Cal. 2002).

151. *Id.* at 1061.

152. *Id.* at 1062.

153. *Id.*

154. *Id.* at 1063 (noting that the pro rata draw of any one newsgroup on AOL was estimated to be no more than 0.00000596% of total usage).

155. *Id.* at 1063 n.11 (citing the Ninth Circuit consideration of Fonovisa requirements in Adobe Systems Inc. v. Canus Productions, Inc. 173 F. Supp. 2d 1044 (C.D. Cal. 2001) and the fear that "for ISPs, the vicarious copyright infringement doctrine might [otherwise] start to resemble strict liability for any material that somehow finds its way onto the

not be made out where infringing and noninfringing users pay a fixed fee.[156] The court accordingly granted summary adjudication on the vicarious infringement claim in AOL's favor.[157]

Having completed the infringement analysis, the *Ellison* court eventually turned to AOL's safe harbor defense, beginning with the two threshold eligibility conditions of § 512(i).[158] It was undisputed that AOL satisfied the second requirement, that it accommodate and not interfere with the standard technical measures used by copyright holders to protect their work.[159] *Ellison* suggests, however, that AOL failed to comply with the requirement that it reasonably implement a termination policy, because evidence showed that "no individual has ever been terminated for being a repeat infringer" by AOL and "AOL had not precisely defined how many times a user had to be guilty of infringement before that user could be" terminated.[160] In contrast to *Napster*, the court interpreted § 512(i) not as a mandate to police for and terminate recidivist infringers, but merely as a command that ISPs "put [their] users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights."[161] Having done so, the court ruled that AOL was eligible for protection under § 512's safe harbor provisions.[162] Had the court decided to address the safe harbor provisions as a preliminary matter, as *Hendrickson* suggests is proper, it could have disposed of much of the case on that basis alone.[163]

As was the case in both *Hendrickson* and *Ellison*, the *Perfect 10* court relied on *Netcom* to dispose of direct infringement.[164] The court found contributory infringement likely, however, not only because Cybernet had received actual notice of alleged infringement, but because it had a general knowledge of infringing activity, based on the ISPs routine review of member sites containing "disclaimers to the effect, 'we do not hold copyrights for these works.'"[165] The court followed *Napster* and *Fonovisa* in

---

ISP's servers."). The court also cites the legislative history of the DMCA as contained in H.R. REP. 105-551(II), at 54 (1998). *Id.* at 1063-64.

156. *Id.* at 1064.

157. *Id.*

158. *Id.*

159. *Id.* at 1065.

160. *Id.* at 1066.

161. *Id.*

162. *Id.*

163. Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001).

164. Perfect 10, Inc. v. Cybernet Ventures, Inc. 213 F. Supp. 2d 1146, 1167-69 (C.D. Cal. 2002).

165. *Id.* at 1169.

holding that the material contribution prong of contributory infringement was likely also satisfied.[166] Along with providing the Adult Check service, absent which access to the infringing content could not occur, the court found that Cybernet makes "steady payments to infringing sites" and thereby "materially contribute[s] to the growth and proliferation of any infringement."[167]

The *Perfect 10* court also believed that Cybernet was probably liable for vicarious infringment, having demonstrated the right and ability to control and a direct financial benefit.[168] The court analogized to *Napster* in finding that Cybernet directly benefits from the draw of infringement because its "future revenue is [similarly] directly dependent upon 'increases in user base.'"[169] The court also established that Cybernet had a right and ability to control infringement because it provided "detailed instructions regard[ing] issues of layout, appearance, and content" to its member sites.[170] Rejecting the *Hendrickson* or *Ellison* approach to the control issue, however, the court considered Cybernet's ability to block access to or otherwise monitor content or activity tantamount to an admission of control, as had the *Fonovisa* and *Napster* courts.[171]

Most significantly, when the court finally looked at the DMCA safe harbor defense, it outright rejected *Ellison*'s reading of § 512(i)'s eligibility requirement (the reasonably implemented termination policy) as mere warning and not as a backdoor requirement that ISPs actively police and terminate.[172] In so doing, the court engaged in a policy analysis and found that "making the entrance into the safe harbor too wide would allow service providers acting in complicity with infringers to approach copyright infringement on an image by image basis without ever targeting the source of these images."[173] The court believed Cybernet could not pass the eligibility threshold absent a showing that it had actually terminated recidivist infringers.[174] But the court had used that very same ability to terminate as

166. *Id.* at 1170-71.

167. *Id.* at 1171.

168. *Id.* at 1171-74.

169. *Id.* at 1171. New users who register for access to member sites pay Cybernet directly.

170. *Id.* at 1173.

171. *Id.* at 1174.

172. *Id.* at 1175-78 ("part[ing] ways with the interpretation . . . in Ellison, in order to maintain the 'strong incentive'" for service providers to prevent their services from becoming safe havens or conduits for known repeat copyright infringers.").

173. *Id.* at 1177.

174. *Id.* at 1178.

a justification for its finding of control.[175] This forces the ISP into a Catch-22: the ISP must be actively terminating recidivist offenders but, in so doing, the ISP thereby opens itself up to a finding that it demonstrates an ability to control, making it vulnerable to the vicarious liability claim.[176] Denying Cybernet shelter, the court granted a preliminary injunction against the provider.[177] The injunction that issued is of some relevance because it institutes a virtual duty to police all content to which Cybernet provides access.[178] In effect, the injunctive order in *Perfect 10* is an invocation of the kind of overwhelming liability that ISPs feared would put them out of business.

## IV. CONCLUSION

Courts are in need of further guidance on how to approach and apply the § 512 safe harbor provisions, and need clarification of their legal duties. Recent conflicting results suggest that ISPs may soon be burdened with the kinds of policing duties from which the DMCA was intended to provide relief. Specifically, as a result of *ALS Scan*, ISPs might begin to take down the good with the bad, forced to remove arguably noninfringing content in a superabundance of caution, even upon deficient notice. And, in the wake of *Perfect 10*, the duty to monitor may lead to takedown and termination, absent specific notice of infringement. Together, the post-DMCA decisions portend a future in which ISPs shoulder a greater weight of responsibility for protecting copyright in the digital era. And, if case law continues to erode or otherwise block access to the § 512 safe harbor provisions, the shelter of immunity may provide little promise of protection against what could be, in the peer-to-peer era, a gathering storm of infringement suits.[179]

---

175. *Id.* at 1174.

176. *Id.* at 1179.

177. *Id.* at 1193.

178. *Id.* at 1193-96. First, the court required Cybernet, prior to adding members to its network, to "review the content of websites to determine whether they contain any Prohibited Content." *Id.* at 1194. The court also ordered perpetual monthly reviews of any member sites that had at any time removed content based on alleged copyright infringement. *Id.* Lastly, the court ordered review within ninety days of the content of every Cybernet premium member site. *Id.*

179. There seems to be only a small logical leap from the district court holding that Verizon must turn over user information for content that never resided on its servers under § 512(k) and, the possibility that future courts could find the failure to have actively terminated users who engage in peer to peer infringement as a reason to deny protection of the § 512 safe harbor provisions. *See* Krim, *supra* note 72 ("Internet service companies fear that if the decision stands, they will be deluged by subpoenas . . . .).