Safe Harbors Against the Liability Hurricane: the Communications Decency Act and the Digital Millennium Copyright Act

Jonathan Band and Matthew Schruers[1]

I. Introduction

Congress has enacted two provisions limiting the liability of Internet Service Providers (ISPs) for the activities of their subscribers. First, Congress adopted Section 230(c)(1) of the Communications Decency Act (CDA)[2] to address the liability of ISPs in defamation cases. Since its enactment in 1996, courts have interpreted the CDA broadly, in essence providing "interactive computer services" with blanket immunity from civil liability for all claims except for intellectual property infringement, to which the CDA by its terms does not apply.[3] Second, two years after the CDA's enactment, Congress partially filled this intellectual property gap in the CDA with Title II of the Digital Millennium Copyright Act (DMCA).[4] This provision offers "safe harbors" from copyright liability to ISPs that comply with certain conditions. Taking a markedly different path from CDA jurisprudence, courts have construed the DMCA narrowly.

This divergence between the CDA and the DMCA is both ironic and disturbing. It is ironic in that Congress and industry spent relatively little time crafting the simple provisions of the CDA, but invested several years in intense negotiations drafting the DMCA's detailed provisions, yet the hastily drafted CDA has afforded ISPs far more protection than the DMCA.

---

[1] Jonathan Band is a Partner in the Washington, D.C. office of Morrison & Foerster LLP. Matthew Schruers is a student at the University of Virginia Law School and a summer associate at Morrison & Foerster LLP. The views expressed in this article are those of the authors and do not reflect the views of any clients of Morrison & Foerster LLP.

[2] Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 133 (codified at 47 U.S.C. § 230(c) (2001)).

[3] 47 U.S.C. § 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.").

[4] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C. (2001)).

The divergence is disturbing in that it suggests that the courts believe that copyrighted works deserve more protection than the individuals harmed by the torts falling within the scope of the CDA.

Part II of this article explores how courts have interpreted the CDA's provisions broadly, limiting ISP liability in circumstances far removed from its roots in defamation. Part III, in contrast, discusses how courts have interpreted the DMCA's provisions narrowly, and cautions that future courts may erroneously interpret the DMCA as simply providing ISPs with "one free pass."

II. ISP Liability Limitations under the Communications Decency Act

A. Cases Predating the CDA

Prior to the CDA, the standing authority on ISP tort liability had been *Cubby, Inc. v. CompuServe, Inc.*[5] CompuServe was sued over allegedly defamatory statements appearing in a subcontractor's forum. *Cubby* treated ISPs as distributors of third party content, rather than as publishers. Accordingly, *Cubby* held the ISP to a constructive knowledge (knew or should have known) standard, instead of the higher, strict liability standard to which publishers are held. Thus, as distributors, ISPs were not liable for statements about which they did not know and had no reason to know.[6]

This standard was upset by *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[7] which imposed a publisher standard on ISPs which monitored their services.[8] The case concerned allegedly defamatory statements about Stratton Oakmont posted on a Prodigy computer bulletin

[5] 776 F. Supp. 135 (S.D.N.Y. 1991).

[6] *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113, at 811 (5th ed. 1984) (noting that distributors cannot be liable "in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published").

[7] 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

[8] *Stratton Oakmont,* 23 Media L. Rep. at 1798, 1799.

board. The court ruled that having held itself out as a "family oriented computer network" that monitored the content of bulletin board postings for conformity with standards set forth in its "content guidelines," Prodigy was not a mere distributor but rather a publisher. Since publishers are strictly liable for their publications, the *Stratton Oakmont* holding meant that by monitoring its service, an ISP increased its exposure to liability for third party content.

B. Adoption of Section 230 of the CDA

Congress quickly recognized that the *Stratton Oakmont* holding led to anamolous result: that an ISP could be penalized for its efforts to rid the Internet of inappropriate content. This result, of course, was contrary to the objectives of the CDA, then under consideration, which prohibited the online distribution of indecent material to minors. Moreover, some legislators who questioned the constitutionality and efficacy of regulating the Internet preferred a self-regulatory approach where ISPs were given an incentive to eliminate objectionable content. Thus, a legislative compromise was reached concerning Section 230 of the CDA. Section 230(c)(1) provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230, therefore, immunized ISPs from liability as content publishers even if they monitored their service. When the U.S. Supreme Court overturned the CDA as unconstitutionally vague in *Reno v. American Civil Liberties Union*,[9] Section 230 was one of the few provisions of the CDA left undisturbed.

C. Cases Applying Section 230 of the CDA.

Congress adopted Section 230 in response to a specific defamation decision, but courts have it construed it broadly in a wide range of contexts. Section 230 has been held to immunize

[9] 521 U.S. 844, 887 (1997).

ISPs from a variety of state law claims, including negligence, business disparagement, waste of public funds, and infliction of emotional distress.

The first case decided under Section 230 was *Zeran v. America Online, Inc.*[10] In *Zeran*, a plaintiff sought to hold America Online (AOL) responsible for the harassment that followed the libelous posting on an AOL bulletin board of his name, telephone number, and false information glorifying the then-recent Oklahoma City bombing. AOL had removed the first posting upon Zeran's request, but the libelous information was re-posted to the same board under a slightly different alias. Because of this posting, Zeran received hostile and threatening telephone calls for several weeks. Zeran argued that having received notice of the postings, AOL could be liable as a common-law distributor. The Fourth Circuit rejected this argument, holding that notice-based liability would frustrate the purpose of the CDA.[11] In effect, the Fourth Circuit interpreted Section 230 as precluding the treatment of an ISP as either a publisher or a distributor, thus giving ISPs complete immunity.

Later cases expanded on *Zeran*, immunizing ISPs from liability for a variety of content-related injuries.[12] In *Blumenthal v. Drudge*,[13] White House aide Sidney Blumenthal and his wife sued the author of the popular gossip column "The Drudge Report" over unsubstantiated allegations of spousal abuse. At the time, AOL had contracted with Drudge Report creator Matt Drudge, paying a fee for the rights to make the report available to AOL subscribers.[14] The

---

[10] 129 F.3d 327 (4th Cir. 1997).

[11] *See Zeran*, 129 F.3d at 333 (citing *Auvil v. CBS "60 Mins."*, 800 F. Supp. 928, 931 (E.D. Wa. 1992); *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986) (recognizing the adverse effect of economic considerations on speech).

[12] *See, e.g., Doe v. America Online, Inc*., 718 So.2d 385 (Fla. Dist. Ct. App. 1998), *aff'd,* 783 So. 2d 1010 (Fla. 2001), *also available at* 2001 Fla. LEXIS 449, petition for cert. filed, 70 U.S.L.W. 3090 (July 14, 2001) (No. 01-125); *Ben Ezra, Weinstein & Co. v. America Online, Inc*., 206 F.3d 980 (10th Cir. 2000), *cert. denied,* 531 U.S. 824 (2000).

[13] 992 F. Supp. 44 (D.D.C. 1998).

[14] *Id* at 47. Drudge was responsible for all aspects of the *Drudge Report*. AOL's contract reserved the right to remove content that violated AOL standard terms of service. *Id.*

Blumenthals sued AOL and Drudge. The court reluctantly granted AOL's motion for summary judgment, in spite of the contractual relationship between Drudge and AOL, citing the authority of Section 230 and *Zeran*.[15] The court found this to be an obtuse result, stating that "[i]f it were writing on a clean slate, this Court would agree with plaintiffs."[16]

Though early cases decided under Section 230 pertained primarily to defamation, the scope of its protection soon spread to other areas of state law. In *Doe v. America Online, Inc.*,[17] a mother filed a negligence suit against AOL for her minor son's emotional injuries. The boy had been victimized by a man, also named as a defendant, who had lured the plaintiff and two other minors into engaging in sexual acts. The defendant later marketed photographs and videotapes of these activities through AOL chat rooms.[18] The plaintiff alleged that but for AOL's negligence, these transactions would not have taken place. The trial court granted AOL's motion to dismiss, and the dismissal was affirmed on appeal.[19] The Supreme Court of Florida also affirmed, declaring that state law remedies inconsistent with Section 230 were unequivocally preempted by that provision.[20]

A recent decision, *Kathleen R. v. City of Livermore*,[21] expanded Section 230 well beyond the area of tort liability. In *Kathleen R.*, the plaintiff's son employed an Internet connection at his public library to downloaded sexually explicit images on numerous occasions. Upon discovering this, the plaintiff sued her municipality and the library trustees, arguing that the

---

[15] *Id*. at 52-53. Though AOL was dismissed from the suit, the Blumenthals continued to pursue their claim against Drudge. *See Blumenthal v. Drudge*, 286 F.R.D. 386 (D.D.C. 1999) (procedural decisions); *Blumenthal v. Drudge*, 29 Media L. Rep. 1347 (D.D.C. 2001) *available at* 2001 U.S. Dist. LEXIS 1749 (motion to dismiss denied as untimely).

[16] *Blumenthal*, 922 F. Supp. at 51.

[17] 718 So.2d 385 (Fla. Dist. Ct. App. 1998), *aff'd,* 783 So.2d 1010 (Fla. 2001) *also available at* 2001 Fla. LEXIS 449.

[18] *Id*. at 386.

[19] *Id*. at 387-390.

[20] *Doe v. America Online, Inc*., 2001 Fla. LEXIS 449, *24, cert. denied (U.S., Oct. 1, 2001).

library should have prevented this practice.[22] The plaintiff's complaint alleged waste of public funds, nuisance, premises liability, and a civil rights claim.[23] The court affirmed the lower court's dismissal, finding that Section 230 preempted the plaintiff's state law claims.[24] By applying Section 230, the court appears to have engaged in an exercise of economy, dismissing a host of dubious state law claims designed to plead around Section 230.[25] In discarding the plaintiff's argument that Section 230 did not prohibit her claim for waste of public funds, the court noted that Section 230's preemption language, "no cause of action may be brought and no liability may be imposed under any State law that is inconsistent with this section,"[26] prohibited all remedies, be they tort claims or otherwise, damages or injunctive relief. While the court obviously wanted to prevent the plaintiff from circumventing the statute through creative pleading, the result in *Kathleen R.* allows defendants to apply Section 230 to an even broader scope of claims.

Similarly, in *Stoner v. eBay, Inc.*,[27] a California court held that nothing in the history of Section 230 prevented its application to allegations of unfair business practices. In *Stoner*, the auction site eBay was sued over bootlegged audio recordings appearing on its service. The plaintiff asserted various violations of Californian civil and penal codes, alleging that by engaging in the sale of "infringing" recordings, eBay was dealing with the public and its users in an unfair and misleading manner.[28]

---

[21] 87 Cal. App. 4th 684 (2001).
[22] *Kathleen R.*, 87 Cal. App. 4th at 690-691.
[23] *Id.* at 690.
[24] *Id.* at 698. The § 1983 civil rights cause of action was also dismissed for failure to state a claim. *Id.*
[25] The court noted that permitting the plaintiff's claims would place libraries in a "damned if you do, damned if you don't" situation. *Id.* at 691-692 (citing *Mainstream Loudoun v. Board of Trustees of Loudoun*, 24 F. Supp. 2d 552 (E.D. Va. 1998) (use of filtering software violates First Amendment)).
[26] 47 U.S.C. § 230(e)(3).
[27] 56 U.S.P.Q.2d 1852 (Cal. Sup. Ct. 2000), *available at* 2000 WL 1705637, 2000 Extra LEXIS 156.
[28] *Id.* at *2.

The court applied factors enumerated in *Zeran*, and found that because: 1) eBay fell within the scope of Section 230; 2) it was not a content provider with respect to the bootlegged recordings; and 3) the plaintiff sought to hold eBay liable for third party content, eBay was therefore protected by Section 230.[29] The court granted summary judgment to eBay, and suggested in dicta that an ISP remained immune until it reached the point of "aiding and abetting" criminal activity.[30] *Stoner* is noteworthy in that it involves intellectual property. Had the plaintiff's claim been cast as a cause of action arising under federal copyright law, it may have yielded a different result because the CDA would not have applied.

D. State of § 230 Today

ISPs pleading Section 230 immunity must establish three factors, originally laid out in *Zeran*. An ISP must demonstrate: 1) that it is an interactive computer service provider as defined by § 230(f)(2);[31] 2) that it is not an information content provider under § 230(f)(3) with respect to the injurious content;[32] and 3) that the plaintiff seeks to hold the ISP responsible for content originating from third parties. The statute precludes all state law remedies, regardless of the underlying theory. Once thought to limit only damages,[33] it is now clear that Section 230 also precludes injunctive relief.[34]

In sum, federal and state courts alike have applied Section 230 liberally and without

---

[29] *Stoner*, 2000 Extra LEXIS 156 at *3-*4.

[30] *Id.* at *14.

[31] Section 230(f)(2) defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

[32] Section 230(f)(3) defines an information content provider as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Providing content in general will not provide grounds for liability. *See e.g., Blumenthal v. Drudge*, 992 F. Supp. at 46-47.

[33] *Mainstream Loudoun v. Board of Trustees of Loudoun*, 2 F. Supp. 2d. at 790.

[34] *See Ben Ezra*, 206 F.3d at 983-984; *Kathleen R.*, 87 Cal. App. 4th at 698.

qualification. CDA jurisprudence is, if nothing else, predictable.[35]

III. ISP Liability Limitations Under the DMCA

In dramatic contrast to the CDA jurisprudence, the DMCA jurisprudence provides little certainty to ISPs. Indeed, the appellate decisions applying the DMCA arguably have weakened its provisions, thereby raising serious questions about the future utility of its safe harbors.[36]

A. Secondary Liability Under Copyright Law

Copyright infringement may take three forms. Direct or primary infringement occurs when a party knowingly or unknowingly infringes upon the exclusive rights of the copyright holder.[37] The other two forms of infringement are secondary: for either to occur, a third party must commit a primary infringement. Vicarious liability results when the defendant: 1) had the right and ability to supervise the infringing activity; and 2) had an obvious and direct financial interest in the exploitation of copyrighted materials.[38] Contributory infringement occurs when the defendant: 1) had knowledge of the primary infringement; and 2) induced, caused, or materially contributed to the infringing conduct.[39] While direct liability is created by the Copyright Act, contributory and vicarious liability have been created by courts interpreting the Copyright Act.

B. Cases Predating the DMCA

---

[35] Other recent CDA cases include *Schneider v. Amazon.com*,[cite], where the Washington Court of Appeals affirmed a lower court's ruling that the CDA sheltered Amazon.com from liability for allegedly defamatory book reviews posted on its site; *Barrett v. Clark*, No. 833021-5 (Cal. Super. Ct., July 25, 2001), where the court held that the CDA protected a user from liability for posting on an Internet forum the contents of an article written by another person; and *Patentwizard v. Kinko's*, D. S.D., No. Civ. 00-4143, 9/27/01, where the court held that the CDA sheltered a commercial copy shop that made Internet accessible computers available to its customers.

[36] Two recent district court decisions appear more favorable to ISPs than the appellate decsions: *Hendrickson v. eBay Inc*., 2001 U.S. Dist. LEXIS 14420 (C.D. Cal. Sept.4, 2001), and *CoStar Group v. Loopnet*, 2001 U.S. Dist. LEXIS 15401 (D. Md., Sept. 28, 2001). While the DMCA protected the defendant in these cases, the opinions contain some troubling language, as discussed below.

[37] *See* MELVILLE B. NIMMER, 2 NIMMER ON COPYRIGHT § 8.01[A] (2001); 2 PAUL GOLDSTEIN, COPYRIGHT: PRINICIPLES AND PRACTICE § 6.0 (2000).

[38] *See* 3 NIMMER, *supra* note 37, § 12.04[A][1] at 12-68 (citing *Shapiro, Bernstein, & Co. v. H.L. Green Co*., 316 F.2d 304, 307 (2d Cir. 1963)). Knowledge is not a requirement for vicarious liability. *See Shapiro*, *id*. at 307.

Some cases preceding the DMCA, most notably *Playboy Enterprises v. Frena*,[40] had imposed direct liability on ISPs for the infringing conduct of users. The direct liability finding was based on the notion that servers operated by the ISP made at least temporary copies of the infringing material when the subscriber uploaded it onto the Internet.[41]

Later courts, particularly *Religious Technology Center v. Netcom On-Line Communication Services*[42], rejected *Frena*'s approach, concluding that "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system for the function of the Internet…. The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred."[43] In *Netcom*, the plaintiffs held copyrights on works posted to a Usenet group, which were automatically disseminated through the defendant ISP's server. The court dismissed the claims of direct and vicarious infringement against the ISP, finding that the requisite participation for direct infringement and the requisite benefit for vicarious infringement were lacking. The court did not dismiss the contributory infringement claim, however, because the pleadings left a factual question about the extent of the ISP's knowledge.[44]

Cases following *Netcom* accepted the proposition that direct infringement required a deliberate "volitional" act by the defendant ISP with respect to the specific work in question.[45]

---

[39] *See Gershwin Publ'g. Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

[40] 839 F. Supp. 1552 (M.D. Fla. 1993)

[41] *See Frena*, 839 F. Supp. at 1556. The law on liability for digital copies had been a troubling issue since *MAI Systems Corp. v. Peak Computer, Inc*., 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994), when the court held that unlicensed computer users violated the operating system copyright simply by turning the computer on, since copying between the hard drive and the computer's RAM would occur.

[42] 907 F. Supp. 1361 (N.D. Cal. 1995).

[43] *Id*. at 1372.

[44] *Id.* at 1374.

[45] *See Sega Enters. v. Maphia,* 948 F. Supp. 923, 932 (N.D. Cal. 1996) (holding defendant not directly liable, imposing contributory liability); *Sega Enters. v. Sabella*, Copy. L. Rep. (CCH) ¶ 27,648, *also available at* 1996 U.S.

Additional cases have limited direct liability to those who directly provide infringing material for profit.[46] Nonetheless, the earlier cases such as *Frena*, combined with the continuing potential for secondary liability, caused sufficient concern in the ISP community that it sought relief from Congress.

C. Title II of the DMCA: Conditions for Eligibility for the Section 512 Safe Harbors

Title II of the DMCA, enacted in 1998, serves the dual purpose of limiting the liability of ISPs for copyright infringement and protecting intellectual property from unauthorized online distribution.[47] The DMCA's legislative history makes clear that Congress intended to overturn *Frena* and codify and extend the effect of *Netcom*.[48] To this end, the DMCA provides "safe harbor" protection to "service providers" -- a broad term which would seem to encompass virtually every Internet or intranet provider or intermediary, including portal sites, search engines, universities, and intranet providers, as long as the operator does not modify or create the content at issue.[49] The safe harbors, appearing in § 512 of the DMCA, limit ISPs' liability for regularly conducted Internet activities including: 1) providing digital network communications services; 2) system caching; 3) hosting information on service provider servers; and 4) providing information location tools, *e.g.*, search engines.[50] If a service provider meets the safe harbor requirements, it is immune from monetary relief, and subject to limited injunctive relief.

Dist. LEXIS 20470 at * 19-20 (holding that whether [the defendant] knew her BBS users were infringing on Sega's copyright or encouraged them to do so ha[d] no bearing on whether [she] directly caused the copying to occur.").

[46] *See*, *e.g.*, *Playboy Enters. v. Webbworld*, 968 F. Supp. 1171 (N.D. Tex. 1997) (imposing direct and vicarious liability for direct online sale of infringing photographs gathered by BBS from newsgroups); *Playboy Enters. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997) (imposing direct and contributory liability on BBS).

[47] *See* S. REP. NO. 105-190 at 2, 19 (1998).

[48] *See* H.R. REP. NO. 105-551, pt. 1, at 24-25 (1998). *See also id.* at 11(stating that the DMCA overruled *Frena* to the extent that *Frena* allowed for direct liability).

[49] 17 U.S.C. § 512(k)(1) (2001). The definition of a service provider for purposes of the safe harbor for providing digital network communications services is somewhat narrower.

[50] *Supra* note 47, at 40.

In order to receive safe harbor protection, the provider must satisfy several general requirements. It must adopt, implement, and inform users of a policy providing for the termination of repeat infringers.[51] The provider must also accommodate "standard" technical measures used by copyright owners to identify and protect copyrighted works.[52]

Additional conditions are required for an ISP to qualify for the hosting and information location tool safe harbors in §§ 512(c) and (d). The provider must: 1) lack actual knowledge or awareness of facts or circumstances from which infringing activity is apparent; 2) not receive a financial benefit directly attributable to the infringing activity, if the provider has the right and ability to control such activity; and 3) respond expeditiously to remove or disable allegedly infringing material if it receives sufficient notice.[53] Significantly, eligibility for a safe harbor is not contingent on the ISP monitoring its service for infringing material.[54]

D. The Courts' Interpretation of the DMCA: Ignoring Congress' Intent?

The DMCA adopted a different approach for limiting ISP liability from the CDA. While the CDA established a simple blanket immunity, the DMCA created several complex safe harbors which are subject to certain conditions, particularly with respect to the hosting and information location safe harbors. Besides the fact that injunctive relief is still available under the DMCA, the most obvious difference between the DMCA and the CDA in the hosting and information location contexts involves "notice and takedown." If an ISP does not respond expeditiously to an adequate notification, it falls out of the DMCA safe harbor. On the other hand, as the *Zeran* decision made clear, an ISP's failure to respond to notification has no impact whatsoever on its CDA immunity.

---

[51] 17 U.S.C. § 512(i) (1)(2001).
[52] *Id*. § 512(i)(2).
[53] *Id*. §§ 512(c)(1), (d).
[54] Section 512(m).

Additionally, as noted above, the DMCA imposes two conditions which closely mirror the judge-made standards for vicarious and contributory liability. This similarity creates the possibility of a Catch-22: if the safe harbors from vicarious and contributory liability were available only to providers that were not vicariously or contributorily liable, a service provider could only qualify for the safe harbor when it didn't need one, and any provider needing the safe harbor would be ineligible.[55] If this were the case, then the only tangible benefit of the DMCA would be its grant of direct liability immunity. To be sure, such immunity would not be insignificant, but it would be far less valuable than immunity from direct *and* secondary liability. A threshold question, then, is whether these conditions are mere restatements of the tests for contributory and vicarious liability.

The legislative history indicates that the tests were not intended to be identical -- that Congress did not intend to create a Catch-22. Rather, Congress made subtle modifications to the prevailing tests to make them "clearer, and somewhat more difficult [for the plaintiff] to satisfy."[56] The courts, in contrast, appear to have collapsed some of the distinctions between traditional secondary liability and the DMCA, thereby creating the potential for a Catch-22.[57] One court has also interpreted the notice requirement in a manner which could significantly diminish protection for ISPs.

1. Constructive Knowledge and Red Flags

Courts historically have imposed contributory copyright liability when the defendant knows or should have known of the primary infringement and materially contributes to the

---

[55] Charles S. Wright, *Actual Versus Legal Control: Reading Vicarious Liability for Copyright Infringement Into the Digital Millennium Copyright Act of 1998*, 75 WASH. L. REV. 1005, 1007 (July 2000).

[56] H.R. REP. NO. 105-551, pt. 1, at 11. *See also* 3 NIMMER, *supra* note 37, § 12.06[B] at 12B-55 n.22 (noting equivocally that "[t]he elements for proving traditional copyright infringement may be less onerous for a plaintiff than the factors that disqualify an ISP from its Section 512 defense.").

[57] The ambiguous status of the "vicarious liability" prong is dicussed in Section III, *infra*.

infringing conduct.[58] The DMCA's hosting and information location provisions require that the ISP lack "actual knowledge" or awareness "of facts or circumstances from which infringing activity is apparent."[59] Calling this "awareness of facts and circumstances" prong a "red flag" test, the Congressional committee reports on the DMCA sought to distinguish it from the mere constructive knowledge, "should have known," standard typically applied in contributory liability cases. The committee reports specifically provide that the DMCA's knowledge standard "differs from existing law, under which a defendant may be liable for contributory infringement if it knows or should have known that the material was infringing."[60]

The committee reports describe the "red flag" test as having both a subjective and objective element. The subjective element tests the service provider's subjective awareness of the facts or circumstances in question. The objective element questions whether infringement would have been apparent to a reasonable person with that knowledge.[61] The reports refer to "pirate sites or similarly obvious and conspicuous circumstances" as examples of facts which would impute "awareness of infringement" to a service provider. The reports underscore that the infringements must be apparent "from even a brief and casual viewing." Reading this legislative history, scholars have concluded that "the 'flag' must be brightly red indeed - and be waving blatantly in the provider's face."[62]

The courts in *A&M Records v. Napster, Inc.,* 239 F. 3d 1004 (9th Cir. 2001) (*Napster),* *ALS Scan v. RemarQ Communities, Inc.*, 239 F. 3d 619 (4th Cir. 2001) (*ALS Scan),* and

---

[58] *See Gershwin*, 443 F.2d at 1162.
[59] 17 U.S.C. §§ 512(c)(2)(A) and (d)(1).
[60] H.R. REP. NO. 105-551, pt. 1, at 25. *See also* David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC'Y 449 (1999) (noting that "courts must advert carefully to the differences" between the varying standards required in the DMCA).
[61] H.R. REP. NO. 105-551, pt. 1, at 26; S. REP. NO. 105-190 at 44.
[62] *See* 3 NIMMER, *supra* note 37, § 12B.04[A][1] at 12B-37.

Hendrickson v. eBay, Inc., 2001 U.S. Dist. LEXIS 14420 (C.D. Cal. Sept. 4, 2001)*(Hendrickson)* seem to have disregarded the distinction between constructive knowledge and the "red flag" test. On the contrary, the courts' opinions could be read as treating these standards as one and the same. In granting the plaintiffs' injunction, the district court in *Napster* stated that certain conduct by Napster executives "satisfie[d] the objective test for constructive knowledge - defendant had reason to know about infringement by third parties." The court's footnote to this text held that this finding put "an end to defendant's persistent attempts to invoke the protection of the Digital Millennium Copyright Act . . . [as it] expressly excludes from protection any defendant who… 'is aware of facts or circumstances from which infringing activity is apparent.'"[63] While Napster may have known of circumstances which constituted "red flags," the district court did not identify them. Rather, it assumed that "reason to know" was equivalent to "awareness of facts and circumstances." While the Ninth Circuit did not accept the district court's holdings about the degree of protection the DMCA affords secondary infringers ("We do not agree that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se"),[64] it did not specifically correct the district court's misreading of the "awareness of facts or circumstances" language.

Similarly, the Fourth Circuit in *ALS Scan* noted that § 512 immunity was "not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or *constructive* knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1)."[65] This statement could be interpreted by subsequent courts as indicating that the court read the "awareness of facts and circumstances" language of § 512(c)(1)(A)(ii) as

[63] *Napster*, 114 F. Supp. 2d at 919 & n.24 (citing 17 U.S.C. § 512(d)(1)(B)).
[64] *Napster*, 239 F.3d at 1025.
[65] *ALS Scan*, 239 F.3d at 625 (emphasis supplied).

describing a "should have known" standard, rather than the strict "red flag" test intended by Congress.

Likewise, the district court in *Hendrickson v. eBay*[66] referred to the "awareness of facts and circumstances" language of Section 512(c)(1)(A)(ii) as "constructive knowledge" no fewer than five times, including in a section heading: "The First Prong of the Test: Actual or Constructive Knowledge." Id. at *29.[67]

In the future, courts looking to *Napster, ALS Scan,* and *Hendrickson* for guidance may interpret these decisions' use of the label "constructive knowledge" for "awareness of facts and circumstances" as a substantive determination that "awareness of facts and circumstances" is equivalent to "should have known," and may ignore the "red flag" test set forth in the committee reports. Of course, these decisions do not have to be read as reaching this conclusion (although the district court in *Napster* clearly did). Nonetheless, their ambiguity on this point helps blur the distinction between the "red flag" test and the traditional constructive knowledge standard.

2. Vicarious Liability.

Courts traditionally have found vicarious liability when a person has the right and ability to supervise the infringing conduct, and receives a direct financial benefit from it. Under Sections 512(c)(1)(B) and (d)(2), a service provider is eligible for a safe harbor only if it "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity." Given the similar wording of these two tests, an obvious question is whether Congress intended courts to apply the traditional standards of vicarious liability, or whether it had different standards in mind.

[66] Hendrickson, a movie producer, sued eBay because infringing copies of his movie were auctioned through the auction site. The court found that the notice sent by theHendrickson did not satisfy the DMCA's requirements, and therefore did not trigger a takedown obligation.

The Committee reports suggest that Congress intended the direct financial benefit prong to be applied very narrowly:

> In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate business would not be considered to receive a 'financial benefit directly attributable to the infringing activity' where the infringer makes the same kind of payment as non-infringing users of the provider's service. Thus, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity.' Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would, however, include any such fees where the value of the service lies in providing access to infringing material.

S. Rep. No. 105-190 at 44-45 (1998).

Significantly, this test is narrower than that applied in some vicarious liability cases, notably *Napster*. *Napster* states in the vicarious liability context that a "[f]inancial benefit exists where the availability of infringing material acts as a draw for customers," and "where infringing performances enhance the attractiveness of a venue." Thus, while *Napster* sees a "financial benefit" where the infringing activity merely contributes to the attractiveness of a site, the Committee report's approach likely would find financial benefit only when the infringing activity was the primary attraction of the site.

Similarly, the *Hendrickson* court suggests that the phrase "right and ability to control" in the DMCA context has a different meaning from the one ascribed to "right and ability to supervise" by other courts in the vicarious liability context:

> "[T]he right and ability to control" the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored on its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of a claimed infringement. *See* 17 USC Section

---

[67] In contrast, the *CoStar* decision specifically refers to the "red flag" test, and implies that it is different from the traditional knowledge standard for contributory infringement. *See Costar* at *35.

> 512(c)(1)(C). The DMCA also provides that the limitation on liability only apply to a service provider that has adopted and reasonably implemented … a policy that provides for the termination in appropriate circumstances of [users] of the service provider's system or network who are repeat infringers." *See* 17 USC 512(i)(1)(A). Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.

Hendrickson at *32. In particular, this conclusion that "right and ability to control" in the DMCA cannot simply mean "the ability of a service provider to remove or block access to materials posted on its website" differs sharply from the *Napster* court's interpretation of "right and ability to control" in the traditional vicarious liability context. The *Napster* court stated: "The ability to to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise." The court then notes that Napster expressly reserved the right to refuse service and terminate accounts for any reason. Further, Napster had the ability to locate infringing material through the use of search indices.[68]

In sum, the Committee report and the *Hendrickson* decision suggest that there is a difference between traditional vicarious liability and the parallel provisions of the DMCA. The court *CoStar v. Loopnet*,[69] on the other hand, found that no difference exists: "Basically, the DMCA provides no safe harbor for vicarious infringement because it codifies both elements of vicarious liability." CoStar at 41. In this one sentence, the *CoStar* court appears to reduce dramatically the scope of the DMCA's safe harbors by eliminating protection from vicarious liability.

---

[68] *Napster*, 239 F.3d at 1023.

[69] CoStar, a provider of commercial real estate information services, sued Loopnet, an Internet company which runs a website on which real estate brokers post listings of commercial real estate available for lease. CoStar alleged that these listings posted by the brokers often included photographs owned by CoStar. The court found that Loopnet was a service provider and that its activities qualified for the hosting safe harbor of Section 512(c). Material factual disputes remained as to whether Loopnet responded expeditiously enough to CoStar's notices to remain within the safe harbor.

At the same time, *CoStar* relied on *Hendrickson*'s interpretations of "right and ability to control," as well as the Committee report's narrow reading of direct financial benefit. This implies that while the *CoStar* court believed that the DMCA simplify codified the elements of vicarious liability, the court also supported the most lenient possible application of the vicarious liability tests in the DMCA context. Thus, perhaps it gave back a little of what it took away.

If nothing else, the case law interpreting the DMCA's "vicarious liability" test is muddled. *Hendrickson* suggests that the DMCA vicarious liability test is different from (and more lenient than) the traditional vicarious liability test applied by courts such as *Napster*. On the other hand, *CoStar* views the tests as the same, but then interprets vicarious liability leniently in the DMCA context. Treating the tests as the same is extremely dangerous because it invites future courts to apply *Napster*'s stringent vicarious liability standards in the DMCA context.

3. Notice

The basic architecture of the DMCA's hosting and information location safe harbors is that an ISP would not incur liability for infringing activity which did not meet the red flag or vicarious liability tests, so long as the ISP complied with the notice and takedown regime. As noted above, the courts have weakened this basic architecture by appearing to replace the red flag test with the constructive knowledge/should have known standard, and perhaps eliminating altogether the safe harbor for vicarious liability. The *ALS Scan* court has further weakened the basic architecture by diluting the standards for a notice which triggers a takedown obligation.

ALS Scan was a marketer of adult photographs which were posted to unauthorized newsgroups with the extension ".als." ALS Scan notified RemarQ, an ISP, of the newsgroups and requested that RemarQ cease carrying them. RemarQ responded by offering to remove infringing images if ALS Scan identified them "with sufficient specificity." In the ensuing

litigation, the district court ruled that ALS Scan had failed to comply with the notice provisions of the DMCA set forth in § 512(c)(3)(A), and granted RemarQ's motion to dismiss.[70] On appeal, the Fourth Circuit reversed, finding that ALS Scan had "substantially complied" with the notice provisions.

In 17 U.S.C. § 512(c)(3)(A), Congress stipulated in great detail the elements that a notification of claimed infringement must contain in order to be effective. Among the six elements, Congress required that copyright owners *specifically* identify the works they claim to have been infringed.[71] If multiple works reside on a Web site, the copyright owner could provide "a representative list of such works at the site." *Id*.

A separate element required by Congress was identification of the material that is claimed to be infringing, along with "information reasonably sufficient to permit the service provider to locate the material." 17 U.S.C. § 512(c)(3)(A)(iii). "The goal of this provision is to provide the service provider with adequate information to find and examine the allegedly infringing material expeditiously."[72]

The district court held that ALS Scan's letter failed to contain either of these lists, and thus was fatally defective.[73] Accordingly, the district court found that RemarQ had no duty to remove any files from its computer system.[74]

On appeal, the Fourth Circuit held that the ALS Scan letter provided a "notice equivalent to a list of representative works that can be easily identified by the service provider," *ALS Scan*, 239 F. 3d at 625, and therefore substantially complied with Section 512(c)(3)'s requirements. In reaching this conclusion, the Fourth Circuit made two legal errors.

---

[70] *ALS Scan*, 239 F.3d at 621.
[71] *See* 17 U.S.C. § 512(c)(3)(A)(ii).
[72] H. R. REP. 105-551, pt. 2, at 55 (1998)
[73] *ALS Scan, Inc., v. Supernews, Inc.,* No. 99-2594 (D. Md. February 28, 2000)

The first legal error is that the court collapsed two distinct elements of the notification into one. Section 512(c)(3)(A)(ii) requires identification of the allegedly infringed works. When the copyright owner believes that multiple works have been infringed, a representative list is sufficient. Section 512(c)(3)(A)(iii) separately requires identification of the allegedly infringing material. Significantly, Section 512(c)(3)(A)(iii) does not permit the short cut of a representative list. Thus, the statute requires two lists: one of the alleged infringed works, the other of the allegedly infringing material, with information sufficient to locate it.

The Fourth Circuit collapsed the two list requirements into one. This is evident from its statement that "ALS Scan substantially complied with the notification requirement of providing a representative list of *infringing* material."[75] But the representative list shortcut referenced in subparagraph (ii) concerns infringed works, not infringing material. Subparagraph (iii) separately requires identification of the infringing material, and, as noted above, does not allow the representative list shortcut.

Compounding this error was a second one: that a general statement that "virtually all" the material on a site is infringing is functionally equivalent to a representative list. Congress insisted upon the six elements for effective notification for a reason; it recognized that service providers are not in a position to identify infringing content on their systems given the automated nature of much of their services, the user driven nature of the communications thereon, and the enormous volume of material they process.[76] Service providers need far more information than provided by ALS Scan to respond expeditiously.

The dearth of detail in ALS Scan's notice forced RemarQ to chose among three unpalatable alternatives. First, it could engage in a time consuming and burdensome review of

---

[74] *Id*.
[75] *ALS Scan*, 239 F.3d at 625 (emphasis supplied).

all of the hundreds of items in the newsgroup, compare these items with the thousands of pictures of ALS Scan's models on ALS Scan's Web site, attempt to determine which articles are infringing, and take down the articles that it believes are infringing. *ALS Scan*, 239 F. 3d at 625. Second, RemarQ could simply accept ALS Scan's assertion that "virtually all" the material on the site was infringing, shut it down altogether, and risk alienating its customers. Third, it could do nothing, and expose itself to copyright liability. By approving ALS Scan's skimpy notice, the Fourth Circuit ensured that future ISPs will have to make similarly difficult decisions.

To be sure, the statute only mandates that the notification "comply substantially" with the requirements set forth in Section 512(c)(3)(A). But the DMCA's legislative history makes clear that this language accommodates only the most trivial mistakes:

> The Committee intends that the substantial compliance standard in subsections (c)(2) and (c)(3) be applied so that technical errors (such as misspelling a name, supplying an outdated area code if the phone number is accompanied by an accurate address, or supplying an outdated name if accompanied by an e-mail address that remains valid for the successor of the prior designated agent or agent of a copyright owner) do not disqualify service providers and copyright owners from the protections afforded under subsection (c). The Committee expects that the parties will comply with the functional requirements of the notification provisions — such as providing sufficient information so that a designated agent or the complaining party submitting a notification may be contacted efficiently — in order to ensure that the notification and take down the procedures set forth in this subsection operate smoothly.[77]

Here, ALS Scan did not come close to complying with the notification provision's "functional requirements."

Section 512(c)(3)(A) lists, in great detail, the information that a notice must contain to trigger a service provider's duty to disable access to infringing works. This statute was intended to create a uniform notice standard and eliminate the possibility of different federal courts

---

[76] *See* S. REP. NO. 105-190 at 8.

[77] S. Rep. 105-190 at 47 (1998).

applying different tests to determine whether service providers had "knowledge" of alleged copyright infringement.[78]

The *ALS Scan* decision appears to destroy the uniformity envisioned by Congress by significantly relaxing the requirements of Section 512(c)(1)(C). The uncertainty *ALS Scan* creates is demonstrated by its inconsistency with the *Hendrickson*. In *Hendrickson*, eBay received a cease and desist letter from the plaintiff, which stated that infringing copies of a documentary film produced by the plaintiff were being offered for sale on the eBay site. The court ruled that the cease and desist letter did not substantially comply with Section 512(c)(3)(B)'s requirements because it did not provide adequate identification of the material claimed to be infringing. Specifically, the plaintiff never identified the allegedly infringing material by their eBay item numbers, and eBay had no way of distinguishing infringing from non-infringing copies of the documentary. Additionally, the cease and desist letter did not contain a statement under penalty of perjury that the information in the notice was accurate, nor that the Plaintiff had a good faith belief that the use was unauthorized. Accordingly, in contrast to *ALS Scan*, the *Hendrickson* court found that the ISP had not received adequate notice, and thus remained within the safe harbor.

Although *Hendrickson* appears to apply the DMCA's standards more rigorously than *ALS Scan*, *Hendrickson* does contain troubling *dicta* on the identification point. The court "recognizes that there may be instances where a copyright holder need not provide eBay with specific item numbers to satisfy the identification requirement. For example, if a movie studio advised eBay that *all* listings offering to sell a new movie (*e.g.*, "Planet X,") that has not yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title

[78] *See* H.R. Conf. Rep. No. 105-796 at 72 (1998), reprinted in 1998 U.S.C.C.A.N 649.

"Planet X" and identify the offensive listings." Slip. Op at 13. Thus, *Hendrickson* appears to agree with *ALS Scan* that a notice that "virtually all" items are infringing would satisfy the takedown requirement.

Even worse, this *dicta* from *Hendrickson* seems to obligate eBay to search its site for the infringing material once it receives the generic notice. In contrast, the Senate Judiciary Committee did not envision a service provider searching its site for infringing material. Rather, the Committee understood the statutory requirement of providing the ISP with "information reasonably sufficient to permit the service provider to locate the material" as including "the URL address of the location (web page) which is alleged to contain the infringing material."[79] In short, even relatively good DMCA decisions are problematic.

4. Duty to Monitor and "One Free Pass"?

During the industry negotiations leading to the adoption of the DMCA, one of the main points of contention was the issue of monitoring. The content providers insisted that the ISPs monitor their systems for infringing material in order to qualify for a safe harbor, while the ISPs argued that a monitoring requirement was economically unfeasible and would violate their subscribers' privacy. In the end, the ISPs prevailed, and Section 512(m) specifically provides that the safe harbors are not conditioned on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity…."

Unfortunately, the recent DMCA decisions could be interpreted as significantly undermining this important provision through their misinterpretation and misapplication of the DMCA's provisions. This has the potential of degrading the DMCA into a "one free pass" safe harbor. That is, the ISP would be protected from liability, and would have no ongoing

[79] Report 105-190 at 46.

monitoring obligations, until it received its first notice of infringing activity. However, once it received that first notice, a court may well conclude that it is on "notice" about the possibility of future infringements, and the ISP might be able to shield itself from liability only if it undertook an aggressive monitoring program. Such a one free pass interpretation would violate the clear intent of Congress in enacting the DMCA.

The "awareness of facts and circumstances" language of Section 512(c)(1)(A)(ii) establishes a red flag test, which is not met by knowledge of past infringement; rather, there must be a conspicuous indication of current infringement.[80] However, some courts may mistakenly have converted the awareness of facts and circumstances/red flag test into a constructive knowledge/should have known test. Thus, once a service provider receives a notice that infringing activity is occurring on its service, and responds appropriately, a court may well find that the ISP has learned that its service can be abused by its subscribers, and therefore has constructive knowledge of subsequent infringements. After the first infringement occurred, a court may reason, the ISP should have known that additional infringements could occur. The ISP would therefore be disqualified from the safe harbor pursuant to Section 512(c)(1)(A)(ii), unless it took proactive measures to prevent the infringing activity. In this scenario, an ISP could avoid liability only if monitors its service, and the monitoring fails to detect the infringing activity.[81]

---

[80] Section 512(c)(1)(A)(ii) is worded in the present tense: "is not aware of facts and circumstances from which infringing activity *is* apparent..." This suggests that the infringing activity must presently be apparent from current facts and circumstances.

[81] The *CoStar* court discussed the continuing duty to monitor issue in the context of contributory infringement. CoStar claimed that "once it gave Loopnet notice of specific infringements, Loopnet was on notice that ongoing infringements were occurring and had a duty to prevent repeat infringement." In the court's view, "there is a critical interplay between the level of knowledge possessed by Loopnet as a result of CoStar's notices and the amount of policing, deterrence and removal demanded of of Loopnet to avoid being liable for contributory infringement." CoStar at * 46. The court reasoned that at some point, Loopnet might have sufficient constructive knowledge of ongoing infringing activity that its failure to police its site and create disincentives to infringement constituted

By departing from a strict reading of the notice requirement, the *ALS Scan* decision could further hasten the DMCA's degradation. Section 512(c)(3) requires the copyright owner to identify with particularity what the infringing material is and precisely where it can be found. The *ALS Scan* court, in contrast, found that the notice requirement was satisfied by a general statement that "virtually all" the material on a particular newsgroup was infringing. The *Hendrickson* court similarly stated that if a service provider received a notice that all copies of a work infringed, it would have to search its site for that work in order to remain within the safe harbor. It is not hard to imagine that a future court might combine the constructive knowledge standard with the loosened notice requirement, and conclude that once an ISP has been notified of the presence of an infringing copy of a popular sound recording or computer program or motion picture, it must be on the lookout for future infringements of that work.

The *Napster* decision's discussion of vicariously liability makes this nightmare scenario for ISPs even more plausible. The *Napster* court stated that "[t]o escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability….Napster … has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system….Napster's failure to police the system's 'premises' … leads to the imposition of vicarious liability."[82]

> It is unlikely that courts will interpret the DMCA's vicarious liability provisions (Sections 512(c)(1)(B) and (d)(2)) as imposing this kind of policing obligation on a service provider to qualify initially for the safe harbors; doing so would flatly contradict Section 512(m)'s statement that the safe harbors are not conditioned on "a service provider monitoring its service or affirmatively seeking facts indicating infringing

---

material inducement. *See Id.* at *46-51. However, the court ruled that too many factual disputes existed for it to decide this issue on summary judgement.

Significantly, the court assumed that this policing obligation would not exist in the DMCA safe harbor context. *See Id.* at *45, *47.

[82] *Napster*, 239 F.3d at 1023.

activity….": Indeed, the *Hendrickson* court warned against interpreting the vicarious liability provisions in a manner which "would render the DMCA internally inconsistent," and implied that "right and ability to control" had different meanings in the DMCA and traditional copyright contexts.

It is conceivable, however, that a court will interpret the DMCA's vicarious liability provisions as imposing a *Napster*-style policing obligation on an ISP which wishes to remain in the safe harbor *after* it receives an initial notice of infringing activity. The *CoStar* court observed that the DMCA codified the elements of vicarious infringement, and future courts may look to *Napster* to guide their application of the vicarious infringement standards. Under this approach, the Section 512(m) prohibition on conditioning eligibility for a safe harbor on monitoring could be understood as applying only *prior* to the first notice of infringing activity. For an ISP to qualify for a safe harbor after it receives that first notice, perhaps "the reserved right to police must be exercised to its fullest extent," *Napster*, 239 F.3d at 1023.

The better approach would be to reject *CoStar's* codification theory, and instead treat traditional vicarious liability and the vicarious liability provisions of the DMCA as two different standards. Although the words are similar -- "right and ability to supervise"(*Napster*) and "right and ability to control"(DMCA) -- they have different meanings in different contexts. This approach is better because it is more consistent with the DMCA's basic structure of providing ISPs a safe harbor from direct *and* secondary liability.

Indeed, the one free pass approach itself is flatly inconsistent with the DMCA's structure. Sections 512(c) and (d) address notice and takedown in separate subsections from the red flag test or the vicarious liability test -- in Sections 512(c)(1)(C) and 512(d)(3). There is no suggestion of a crossover between receiving notice and obtaining knowledge or awareness within the meaning of Sections 512(c)(1)(A) and (d)(1). In fact, Section 512(c)(3)(B) provides that a defective notice "shall *not* be considered ... in determining whether a service provider has actual

knowledge or is aware of facts or circumstances from which infringing activity is apparent." (Emphasis supplied.)[83] Further, the one free pass approach flies in the face of Section 512(m)'s explicit prohibition on conditioning safe harbor eligibility on monitoring.

Fortunately, the courts have not yet disfigured the DMCA into a one free pass rule. So far, only four cases have squarely addressed the DMCA safe harbors, and in *Napster*, the Ninth Circuit made clear that the applicability of the DMCA would be considered at trial.[84] Further, the positions of the Fourth and Ninth Circuits concerning the red flag test are ambiguous. Additionally, the *ALS Scan* holding could be limited to its facts: a statement that "virtually all" the items on a website are infringing is sufficient notice when dealing with a pirate site dedicated to the exchange of infringing material. The *Hendrickson dicta* about an ISP searching its website for infringing material is exactly that: mere *dicta*. The *Napster* interpretation of right and ability to supervise could be limited to traditional vicarious liability, and might not apply to the DMCA itself. Finally, the *CoStar* court indicated that the DMCA did not envision a continuing duty to monitor.[85]

The situation, therefore, is not be as bleak as suggested above. Nonetheless, even considered in the most favorable light, the DMCA case law is not evolving as positively as that of the CDA. If future courts continue to overlook the DMCA's plain language and legislative

---

[83] The only exception is when the notice substantially complies with the three core notice requirements (identification of the copyrighted work, identification of the allegedly infringing material, and information sufficient for the service provider to contact the complaining party), and the service provider does not attempt to contact the person making the notification or take other reasonable steps to assist in the receipt of compliant notification. Thus, knowledge can be imputed to the service provider only when it violates the DMCA's cooperative spirit.

[84] The fact that in three years of Section 512's opeation the courts have had to intervene only four times suggests that the notice and takedown system is working well. For this reason, it is all the more important that the courts do not upset the balance Congress achieved.

[85] See note __, supra.

history, and instead build on the negative strains of *Napster* and *Als Scan*, the DMCA's safe harbors will deteriorate rapidly.

IV. Conclusion

The disparity between the protection offered by the DMCA and the CDA could not be more stark. As applied by the courts, the CDA offers ISPs significant protection against liability for defamation and other torts committed by subscribers. In contrast, if they do not become more careful, the courts may degrade the DMCA into a one free pass rule: an ISP would be immune from liability so long as it remained in a state of blissful ignorance, but once it received the first notice of infringing activity, it would be on notice concerning the possibility of future infringements. This would mean that ISPs would have to chose between exposing themselves to infringement liability or incurring significant monitoring costs. Either alternative will impede the growth of the Internet.

It is not surprising that Congress drafted the CDA's safe harbors more broadly than the DMCA's. After all, the content community was far better organized than likely victims of defamation, and thus was far better situated to lobby against broad safe harbors for ISPs. What is hard to explain is the inconsistency between the courts' generous reading of the CDA and parsimonious reading of the DMCA. Consider the rulings of the Fourth Circuit. In *Zeran*, the Fourth Circuit concluded that holding a service provider liable after it received repeated notice from a completely innocent victim of defamation would frustrate Congress' intent in enacting the CDA. By contrast, in *Als Scan*, the Fourth Circuit found that the vague notice provided by an *adult* website substantially complied with the DMCA's detailed notice requirements and triggered a takedown obligation by an innocent ISP.

In any event, unless the courts begin applying the DMCA in accordance with its plain language and its clear legislative history, Congress may have to dredge out the DMCA's safe harbors so as to restore them to their intended effectiveness.