Save the Slip for the Service Providers: Courts Should Not Give Short Shrift to the Safe Harbors of the Digital Millennium Copyright Act

By RAPHAEL A. GUTIÉRREZ*

IN 1998, CONGRESS passed the Digital Millennium Copyright Act ("DMCA"),[1] with the hope that its provisions would bolster the development of the Internet. In particular, Title II granted service providers immunity from any type of copyright infringement to encourage them to develop their services freely, without fear of liability for acts of infringement that might occur on their systems.

To date, there have not been many cases in which entities have claimed the protection of the safe harbors. However, in the cases that have been decided, courts have interpreted the requirements very strictly, thereby denying service providers the protection to which they are entitled. Title II is extremely long and complicated, and courts that have tackled it seem to have had a difficult time determining exactly what is required of service providers. The result has been that they are erring on the side of granting too much copyright protection.

This article suggests that to give effect to the intentions of Congress, courts should read the safe harbors more liberally, in order to grant the service providers protection and incentives to keep developing Internet related services. A step by step framework is also suggested to help courts analyze claims of safe harbor protection by entities that claim to be service providers.

I. Introduction to the Digital Millennium Copyright Act

The Digital Millennium Copyright Act of 1998 was a mammoth piece of legislation that added a number of sections to the Copyright

* J.D. 2001, University of San Francisco School of Law; B.A. 1996, University of California, Los Angeles. The author is an associate at Knobbe, Martens, Olson & Bear, LLP.

1. Pub. L. No. 105–304, 112 Stat. 2860 (Oct. 28, 1998) (codified in various sections of 17 U.S.C. (Supp. IV 1999).

Act. The stated purpose of the DMCA was to "facilitate robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[2]

The DMCA is divided into four titles; each has its own purpose. Title I implemented the new World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty. Title II was designed to address safe harbor provisions for service providers. Title III created a specific exemption in the copyright act regarding rights of a computer owner or lessee. Title IV was intended to update the United States' copyright laws concerning library, archive, and educational use of copyrighted works in the digital age.

This article will focus solely on Title II, describing the elements of its various subsections and analyzing how certain of those subsections have been interpreted by the courts. Courts, in most circumstances, have been overly cautious in applying Title II to service providers. At the time of publication, no court has granted a service provider the protection to which it is entitled under Title II. For sections that have not been addressed by the courts, courts should give them a liberal interpretation in order to further Congress's purpose in enacting Title II of the DMCA.

II. The Purposes of Section 512

Congress designed Title II of the DMCA ("Title II") to "preserve[ ] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[3] Congress also intended Title II to give service providers more certainty as to their liability for copyright infringement that occurred during their provision of Internet services.[4]

Title II created a new section under Chapter 5 of the Copyright Act, adding 17 U.S.C. Section 512.[5] Congress wanted Section 512 to limit service providers' liability for copyright infringement "for five general categories of activity set forth in subsections (a) through (d) and subsection (g)."[6] These limitations on liability are often referred

2. S. REP. NO. 105-190, at 1 (1998), *reprinted in* MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT: *Congressional Committee Reports on Amendments* (2000) [hereinafter SENATE REPORT].

3. *Id.* at 20.

4. *See id.*

5. *See id.*

6. *Id.* at 19.

to as "safe harbors."[7] The first four safe harbors limit liability for any qualifying "service provider"[8] while the fifth provides immunity in certain circumstances for "good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent."[9] The Senate Report makes clear that the safe harbors only apply if the service provider would otherwise be found liable under existing copyright principles.[10] In other words, the DMCA does not create any new standards to determine liability (or a lack thereof) for copyright infringement.

Furthermore, section 512 is only a limitation on liability for claims of copyright infringement. In *Universal City Studios, Inc. v. Reimerdes*,[11] the plaintiff brought suit under Title I of the DMCA, alleging that the defendants had circumvented a technological measure designed to control access to its copyrighted works.[12] One of the defendants argued that he was a service provider and attempted to rely on section 512 of the DMCA to immunize himself from liability.[13] The court rejected this argument for two reasons. The first was that the defendant offered no proof he was a service provider.[14] But that was unimportant in light of the court's second reason: "Section 512(c) provides protection only from liability for copyright infringement. [P]laintiffs seek to hold defendants liable . . . for a violation of section 1201(a)(2), which applies only to circumvention products and technologies."[15] Therefore, the court concluded that section 512 was inapplicable.[16]

The first four safe harbors, which will be described in more detail below, limit liability for copyright infringement for different activities, and will be referred to as the conduit safe harbor,[17] the system caching safe harbor,[18] the system storage safe harbor,[19] and the informa-

7. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).
8. *See* 17 U.S.C. § 512(a)–(d) (Supp. 1998).
9. 17 U.S.C. § 512(g)(1).
10. *See* SENATE REPORT, *supra* note 2, at 40.
11. 82 F. Supp. 2d 211 (S.D.N.Y. 2000).
12. *See id.* at 215.
13. *See id.* at 217.
14. *See id.*
15. *Id.*
16. *See id.*
17. *See* 17 U.S.C. § 512(a) (Supp. IV 1998). *See also* SENATE REPORT, *supra* note 2, at 41 (1998): "Subsections (a)(1) through (5) limit the range of activities that qualify under this subsection to ones in which a service provider plays the role of a 'conduit' for the communications of others."
18. *See* § 512(b).
19. *See* § 512(c).

tion location tools safe harbor.[20] Each safe harbor has its own set of requirements that must be met before it can be used. Subsection (n) indicates the separate and independent functioning of each safe harbor. It states that a service provider's eligibility for one subsection shall be based solely on the requirements of that particular subsection, and shall not affect a determination of whether it qualifies for another subsection.[21] One district court gave effect to subsection (n) by ruling that the potential applicability of one safe harbor would not completely preclude application of another.[22]

III. Safe Harbor Protections Offered Service Providers

A. Protection from Monetary Damages

Any entity that qualifies for protection under one of the first four safe harbors is immunized against monetary relief for any type of copyright infringement: direct, vicarious, and contributory. This is evident from the language in the Senate Report[23] and the fact that each of the four sections begins with the language "[a] service provider shall not be liable for monetary relief . . . ."[24] The only definition provided by the statute, other than "service provider," is for "monetary relief," which, for the purposes of section 512 means "damages, costs, attorneys' fees, and any other form of monetary payment."[25]

B. Limited Protection from Injunctions: Section 512(j)

The first four safe harbors also protect qualifying service providers, to a limited extent, from injunctive or any other type of equitable relief.[26] Subsection (j) of the statute sets out specific forms of injunctive relief that a court may issue. Generally, a court may require a service provider to either block access to an infringing site, or to terminate the account of an infringing subscriber.[27] If the entity qualifies for a safe harbor other than section 512(a), the court may also grant such injunctive relief as it considers necessary to prevent or re-

20. *See* § 512(d).
21. *See* § 512(n).
22. *See* A&M Records, Inc. v. Napster, Inc., 54 U.S.P.Q.2d (BNA) 1746, 1751 (N.D. Cal. 2000).
23. *See* SENATE REPORT, *supra* note 2, at 40 (1998).
24. § 512(a)-(d).
25. § 512(k)(2).
26. *See* §512(k).
27. *See* § 512(j)(1)(A)-(B).

strain copyright infringement, so long as that relief is the least burdensome to the service provider.[28]

Subsection (j)(2) gives the court considerations to take into account in issuing an injunction. Subsection (j)(3) lays out the requirement of notice that must be given to the service provider before an injunction can be issued. A discussion of these subsections, however, is beyond the scope of this paper.

IV. Two Definitions of "Service Provider" in Section 512(k)(1)

Before a party can argue that its actions meet the requirements of one of the safe harbors, it must first meet the definition of "service provider," as service providers are the only entities protected under section 512.[29] Subsection (k)(1) defines "service provider" in two ways, depending on which safe harbor is used.

A. The Broad Definition of Service Provider

The more broadly worded definition can be used to immunize from liability entities that may not traditionally be thought of as service providers.[30] The Senate Judiciary Report states that the definition was meant to cover providers of "services such as . . . Internet access, e-mail, chat room and web page hosting," as well as "universities and schools to the extent they perform the functions identified in subsection ([k])(1)(B)."[31] Thus, providers of e-mail (such as Hotmail)[32] or providers of web page hosting (such as GeoCities)[33] would be eligible for protection from liability for copyright infringement.

B. The Narrow Definition of Service Provider

If an entity wants to claim the protections of the conduit safe harbor (section 512(a)), a provision that limits liability for transitory digital network communications, that entity's activities must fall within the scope of the "narrow definition" of service provider: "an entity offer-

28. *See* § 512(j)(1)(A)(iii).

29. *See* § 512(a)-(d), (g).

30. *See* Casey Lide, *What Colleges and Universities Need to Know About the Digital Millennium Copyright Act, available at* http://www.educause.edu/ir/library/html/cem9913.htm (last visited Apr. 29, 2001).

31. SENATE REPORT, *supra* note 2, at 49.

32. *See, e.g.*, Hotmail, *available at* http://www.hotmail.com (last visited Aug. 13, 2002).

33. *See, e.g.*, Geocities, *available at* http://geocities.yahoo.com/home/ (last visited Aug. 13, 2002).

ing the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of material as sent or received."[34] For all of the other safe harbors, however, the "broad definition" of "service provider" applies, which is defined as "a provider of online services or network access, or the operator of facilities therefore, and includes any entity described in [the narrow definition of service provider]."[35]

The narrow definition was crafted in such a way as to recognize that section 512(a) is a narrow limitation on liability, intended to protect only conduit activities. "This . . . definition is derived from the definition of 'telecommunications' found in 47 U.S.C. § 153(48) in recognition of the fact that the functions covered by this definition are conduit activities."[36] The legislative history demonstrates the limited scope of the definition by stating that while "hosting a World Wide Website does not fall within the subsection ([k])(1)(A) definition; providing connectivity for a [W]orld [W]ide [W]eb site does fall within that definition."[37] While the definition may be narrow, a provider which performs functions that fall both within and without the narrow definition does not lose its eligibility for the safe harbor.[38] It can still claim the limitation on liability for the activities that fall within the narrow definition.

To use an example from the Senate Report, imagine there is a service provider, called SP, which *provides connectivity* for a World Wide Web ("WWW") site, called Site A. This activity would allow SP to come within the narrow definition of service provider. Imagine that SP also *hosts* some WWW sites, including Site B. This activity would fall outside the narrow definition of service provider. Imagine further that SP then becomes a defendant in a suit for copyright infringement regarding material that appears on Site A. SP would still be able to use the narrow definition of service provider and claim the conduit safe harbor since the activities in question allow it to meet that definition. Thus, the fact that it does perform some activities that fall outside the narrow definition, such as hosting Site B, is irrelevant, as long as those activities do not involve the alleged copyright infringement at issue.

34. § 512(k)(1)(A).

35. § 512(k)(1)(B).

36. SENATE REPORT, *supra* note 2, at 49.

37. *Id.*

38. *See id.*

C. Application of the Narrow Definition of Service Provider in *A&M Records, Inc. v. Napster, Inc.*[39]

In *A&M Records, Inc. v. Napster, Inc.* ("*Napster SJ*"), the defendant, Napster, attempted to rely on the conduit safe harbor in its motion for summary judgment by asserting it was a service provider.[40] In order to use this safe harbor, Napster would have had to meet the narrow definition of service provider. The plaintiffs never challenged Napster's ability to meet the narrow definition of service provider, and instead only argued that Napster did not fulfill the requirements of the safe harbor.[41] Judge Patel thus assumed, without holding, that Napster was a service provider under the narrow definition, since plaintiffs "appear[ed] to concede that Napster is a 'service provider' within the meaning of subparagraph 512(k)(1)(A)."[42]

The plaintiffs moved for a preliminary injunction against Napster, which Judge Patel issued in a decision that will be referred to here as *Napster I*.[43] The Ninth Circuit reviewed the grant of the preliminary injunction in an opinion that will be referred to as *Napster II*.[44] In their brief to the Ninth Circuit, the plaintiffs challenged Napster's status as a service provider.[45] The plaintiffs' argument, however, rested on the fact that Napster did not provide access to the Internet, like AT&T, nor did it function as a generalized search engine, like Yahoo!.[46] The plaintiffs made no effort to show that Napster did not fit one of the definitions of service provider under section 512(k).

---

39. 54 U.S.P.Q.2d 1746 (BNA)(N.D. Cal. 2000).

40. Napster "designed and operate[d] a system which permit[ted] the transmission and retention of sound recordings employing digital technology." A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011(9th Cir. 2001). Napster's system utilized software, available for free on its website, which allowed its users to copy audio compact discs ("CDs") as MP3 files on their hard drives, to search for files on other users' computers, and to transfer files to and from other users. *See id.* MP3 is a "standard file format for the storage of audio recording in a digital format." *Id.* The software also provided chat rooms and directories where artists could post information about their band or their music. The plaintiffs, who were "engaged in the commercial recording, distribution and sale of copyrighted musical compositions and sound recordings," sued Napster for contributory and vicarious copyright infringement.

41. *See Napster*, 54 U.S.P.Q.2d (BNA) at 1749 n.5.

42. *Id.*

43. *See* A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 927 (N.D. Cal. 2000).

44. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

45. *See* Brief for Plaintiffs/Appellees at 8, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)(Nos. 00-16401 and 00-16403).

46. *See id.*

In *Napster II,* the Ninth Circuit noted that the issue of whether Napster was a service provider had never been resolved.[47] The court found that "Napster's potential liability for contributory and vicarious infringement [did not necessarily] render[ ] the Digital Millennium Copyright Act inapplicable per se," because there were still significant questions regarding the applicability of the safe harbors, including whether Napster was an "Internet service provider as defined by 17 U.S.C. § 512(d)."[48] Several ambiguities inhere in the court's statement, however. The term "service provider" is not defined in section 512(d). That section lists the requirements for the information location tools safe harbor. Thus it is not clear whether the court is saying there are questions as to whether Napster is a service provider, or there are questions as to whether Napster can claim the protection of section 512(d).

D. Definitions of Service Provider Should Be Interpreted Broadly

Congress intended to give broad protection to entities whose business involves providing access to digital networks. The broad definition includes not only those entities that provide online services or network access, but also those who operate the facilities required to provide the online services or network access.[49]

Most people familiar with the Internet would probably limit what they consider to be a service provider to those entities that provide a means for accessing the Internet, like America Online ("AOL"). However, Congress obviously intended to protect more entities than the AOL-type providers. The Senate Report states that entities that provide users with e-mail or chat functions would be included in the definition as well as

> "over-the-air broadcasting, whether in analog or digital form, or a cable . . . or . . . satellite television service . . . to the extent it provided users with online access to a digital network such as the Internet, or it provides transmission, routing or connections to connect material to such a network."

By interpreting these definitions broadly, and allowing entities such as Napster to meet the definition of service provider, courts will further the goal of Congress to clarify the liability of service providers

47. *See Napster,* 239 F.3d at 1025.

48. *Id.* The court noted that these issues would be more fully developed at trial. It still affirmed the preliminary injunction, however, because the plaintiffs had demonstrated that the balance of hardships tilted in their favor.

49. *See* 17 U.S.C. § 512(k)(1)(B) (Supp. IV 1998).

so they will not hesitate to "make the necessary investment in the expansion of the speed and capacity of the Internet."[50]

V. Safe Harbor Requirements

A. Requirements for All Safe Harbors: The Basic Requirements of Section 512(i)

Before an entity is able to take advantage of any of the safe harbor provisions, section 512(i) lists two requirements that must be met, the "basic requirements." As stated in the Senate Report, "subsection (i) imposes additional requirements on eligibility for *any* DMCA safe harbor."[51]

1. Termination Policy

The first of the basic requirements is that the service provider adopt and implement a policy providing for the termination of the accounts of subscribers who engage in repeat copyright infringement.[52] The service provider must also inform its subscribers that they are subject to the termination provisions of the policy,[53] so that "flagrant or repeat infringers 'know that there is a realistic threat of losing [their] access.'"[54]

2. Accommodate Standard Technical Measures

The second requirement is that the service provider must accommodate and not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.[55] Examples of such technical measures include digital watermarks or copyright management systems. However, the service providers are only bound to accommodate such technologies as long as those technologies "(A) have been developed pursuant to a consensus of copyright owners and service providers; . . . (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on the service provider or substantial burdens on its system or network."[56]

---

50. SENATE REPORT, *supra* note 2, at 8.
51. *Napster*, 54 U.S.P.Q.2d (BNA) at 1752.
52. *See* § 512 (i)(1)(A).
53. *See id.*
54. *Napster*, 54 U.S.P.Q.2d (BNA) at 1752 (quoting H.R. REP. No. 105-551 (II), 1998 WL 414916, at *154).
55. *See* § 512(i)(1)(B), (i)(2).
56. § 512(i)(2).

3. Application of the Basic Requirements: *Napster SJ*

In opposition to Napster's summary judgment motion in *Napster SJ*, the plaintiffs alleged that Napster had failed to meet the first of these basic requirements.[57]

a. Adoption of Termination Policy

The plaintiffs claimed that Napster did not adopt a written policy of which its users had notice until *after* the lawsuit was filed.[58] Napster tried to refute this allegation by noting that the statute does not specify a certain time for the service provider to adopt the policy.[59] The court noted that while this was true on its face, it would not be logical to make the copyright compliance policy a prerequisite for all safe harbors, yet allow a service provider to adopt such a policy after a lawsuit had been filed. If that were true, the defendant in a copyright suit could simply say it had developed a formal policy after the lawsuit had been filed, and thereby avoid monetary liability for copyright infringements that occurred before developing the policy.[60] Moreover, the court concluded, for summary judgment purposes Napster would have to produce some proof that it had satisfied the requirements of subsection (i), not simply state that it had done so.[61] While courts should interpret section 512 broadly, this court was correct in not interpreting the statute too broadly so as to allow the service provider to read an absurdity into the statute.

b. Implementation of Termination Policy

The plaintiffs also argued that Napster failed to meet the requirements of subsection (i) because, even after Napster did adopt a copyright compliance policy, it did not reasonably implement it.[62] Once Napster was formally notified of users engaging in infringing activity, it would block only their passwords and not their internet protocol addresses.[63] The plaintiffs alleged this was insufficient because users could easily sign on again under a new user identification and password. They claimed that Napster purposefully kept itself ignorant of

57. *See Napster*, 54 U.S.P.Q. 2d (BNA) at 1752.
58. *See id.*
59. *See id.* at 1752–53.
60. *See id.* at 1753.
61. *See id.*
62. *See id.*
63. *See id.*

its users' identities and addresses so Napster could disclaim any liability for copyright infringement.[64]

The court concluded that the plaintiffs had produced enough "evidence that Napster's copyright compliance policy is neither timely nor reasonable within the meaning of subparagraph 512(i)(A)" to defeat Napster's summary judgment motion.[65] The Ninth Circuit agreed that there were significant questions as to whether Napster fulfilled the requirements of section 512(i).[66]

4. Issues with the Basic Requirements: Websites That Do Not Require User Subscription

One issue that has been discussed with regard to the basic requirements is whether or not a website that does not require its users to subscribe would still be able to claim the protections of the section 512 safe harbor provisions. As the *Napster SJ* court noted, a debate continues over how reasonable or easy it is to block specific internet protocol addresses, i.e. specific computers, from accessing a website or a particular service.[67] Most websites visited today, such as Yahoo.com or MSNBC.com do not require passwords, or require them only for limited functions, such as accessing e-mail.

Given Congress's intent to grant a broad scope of protection, website operators that do not require passwords should be found to meet the basic requirement as long as they notify users that any infringing material they posted to the website will be removed. Website operators that actually remove infringing material upon receiving proper notice should not be held liable for copyright infringement.

B. The Conduit Safe Harbor: Section 512(a)

The conduit safe harbor insulates a service provider from copyright infringement liability for transitory digital network communications, which are comprised of "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections."[68] An entity attempting to

64. *See id.*

65. *Id.*

66. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

67. *See* A&M Records, Inc. v. Napster, Inc., 54 U.S.P.Q.2d (BNA) 1746, 1753 (N.D. Cal. 2000).

68. 17 U.S.C. § 512(a)(Supp. IV 1998).

claim the protection of this safe harbor must meet the narrow definition of service provider and the five elements discussed below.

1. Five Elements

There are five elements that must be satisfied for the conduit safe harbor to apply: (1) the transmission of material must be initiated by a person other than the service provider; (2) the transitory digital network communication must be carried out through an automatic technical process; (3) the service provider must not select the recipients of the material; (4) no copy of the material made by the service provider can be available to anyone other than the intended recipients; and (5) the material is transmitted through the system or network without modification of its content.[69]

2. Application of the Conduit Safe Harbor: *Napster SJ*

In deciding Napster's motion for summary judgment, the *Napster SJ* court seemed to read a sixth element into the statute by requiring that transmitting, routing, or providing connections literally pass through Napster's servers.[70] The court relied on the fact that the prefatory language of section 512(a) states that a service provider is free from liability for "transmitting, routing, or providing connections for, material *through a system or network.*"[71] It concluded that since the narrow definition "service provider" from section 512(k)(1)(A) did not include the words "through a system or network," section 512(a) imposed an additional requirement.[72]

a. Transmitting Material

The *Napster SJ* court held that transmissions do not pass through Napster's servers because Napster admitted that transmitted files pass through the Internet, directly from one user's computer to another's.[73] Napster then tried to argue that its system consisted not only of its servers, but also of the MusicShare browsers that its users had downloaded onto their computers.[74] The court rejected this argument, but held that even if "the system includes the browser on each user's computer, the MP3 files are not transmitted 'through' the sys-

69. *See* § 512(a)(1)–(5).
70. *See Napster*, 54 U.S.P.Q.2d at 1751.
71. *Id.* (quoting 17 U.S.C. § 512(a)).
72. *See id.* at 1749.
73. *See id.* at 1751.
74. *See id.*

tem within the meaning of subsection 512(a);" instead, the court found that they are transmitted "*from* one part of the system *to* another, or *between* parts of the system."[75]

b. Providing Connections for Material

The court also held that Napster did not provide a connection "through" its servers.[76] Napster argued, and plaintiffs admitted, that Napster's central server provided requesting users' browsers with the host users'[77] Internet Protocol address information.[78] This, in turn, enabled a connection between the two computers, comprising the "'value of the system to the users and the public.'"[79] Therefore, Napster argued, a connection was made through its system. The plaintiffs did not provide any evidence to rebut Napster's assertion. "Nevertheless, the court [found] that Napster does not provide connections 'through' its system."[80]

c. Routing Material

Then, despite the fact that "[n]either party ha[d] adequately briefed the meaning of 'routing' in subsection 512(a)," and the "legislative history [did not] shed light on this issue," the court went on to hold that "routing does not occur through the Napster system."[81] The deepest the court dove into the analysis of "routing" was rejecting Napster's argument that "Napster's server *routes* the transmission by providing the Host's address to the Napster browser that is installed on and in use in User 1's computer."[82] The court's main reason for rejecting Napster's assertion was that Napster tried to make "routing" seem too much like "providing connections," and Congress would not use those phrases disjunctively if they were intended to have similar meanings.[83]

The court proceeded to extrapolate a definition of "routing" from the parties' submissions, notwithstanding its observation of de-

75. *Id.*
76. *Id.* at 1752.
77. The host is the person who has the desired file.
78. *See Napster*, 54 U.S.P.Q.2d (BNA) at 1747, 1752.
79. *Id.* at 1751–52.
80. *Id.*
81. *Id.*
82. *Id.* (quoting Brief for Plaintiffs/Appellees at 8, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)(Nos. 00-16401 and 00-16403)).
83. *Id.*

fendant's apparently contradictory uses of the word.[84] It would seem rash for the court to admit a lack of information regarding "routing" yet base its holding on what seemed to be mere speculation and conjecture drawn from the parties' briefs.

d. The Reading of the Conduit Safe Harbor Was Too Strict

(1) A Strict Interpretation Will Stifle New Technologies

Such a strict reading of the statute defeats the purpose of the statute to "facilitate the robust development . . . of electronic commerce, communications, [and] research."[85] Shawn Fanning, one of the founders of Napster, created the Napster system using peer-to-peer architecture.[86] Peer-to-peer networks allow users to transmit files directly to each other, rather than having to send them through a central server first, and are generally simpler in nature than other types of networks.[87] Fanning's purpose in designing this system was to solve the problems his roommate encountered when looking for music files on the Internet.

Ordinary search engines in existence at that time searched the Internet periodically, and updated their indexes maybe every hour or so to remove sites that were down or unavailable. During the time in between each search, the indexes would become out of date as sites went up or down. Fanning's purpose in creating the peer to peer network was to have a system whose index reflected only sites that were immediately available. Users all connected to the central server and chose which files they wanted to share with others. Once a user signed off the system, the index immediately reflected that by taking that user's files off the system.

Fanning's design was unique and programmed specifically to combat certain problems encountered when looking for files on the Internet. By requiring the files to literally pass through Napster's servers, the court's ruling stifles the development of new technologies whose purpose is to make searching the Internet a smoother ride.

84. *See id.* The court noted that "Napster sometimes appears to recognize a distinction between the two terms. For example, it states that 'the system provides remote users with connection to each other and allows them to transmit and route the information as they choose.'" *Id.* at n.7 (quoting defendant's reply brief).

85. SENATE REPORT, *supra* note 2, at 1.

86. Shawn Fanning's declaration, *available at* http://www.napster.com/pressroom/legal.html (last visited April 29, 2001).

87. *See* Webopedia, *at* http://www.webopedia.com/TERM/p/peer_to_peerarchitecture.html (last visited Apr. 29, 2001).

Thus, the court essentially punished Fanning for choosing a more efficient architecture for his system.

(2) A Strict Interpretation Bars Activities the Statute Should Reach

The court's strict interpretation also seems to contravene Congress's intentions as to what types of activity the statute is supposed to reach. The Senate Report states that "[s]ubsection (a) applies to service providers transmitting, routing, or providing connections for material and some forms of intermediate and transient storage of material in the course of performing these functions."[88] There is no express requirement that material pass through a server.

Additionally, the language of the fifth requirement of section 512(a), that "the material is transmitted through the system or network without modification of its content," includes the word "through."[89] Yet, the Senate Report's summary of the elements states that the fifth element requires that "the content (but not necessarily the form) of the material is not modified in the course of transmission."[90] There is no mention of the word "through," indicating Congress was more concerned about the interpretation of the word "modification." Further demonstrating that concern, the example given in the report demonstrates that altering the form of the material, such as changing bold face type to normal, will not count as a modification.[91] Again there is no reference to the "through" element the court seems to read into the statute.

The court's insertion of a requirement that the material literally pass through the system for a service provider to claim the protection of the conduit safe harbor is overly strict. It will stifle development of Internet technologies and exclude an activity Congress intended to cover with the statute.

88. SENATE REPORT, *supra* note 2, at 41.

89. 17 U.S.C. § 512(a)(5)(Supp. IV 1998).

90. SENATE REPORT, *supra* note 2, at 42.

91. *See id.*

C. Additional Requirement for the System Caching, System Storage, and Information Location Tools Safe Harbors: A Designated Agent

To claim the protection of the system caching,[92] system storage,[93] or information location tools[94] safe harbors, a service provider must have an agent designated to receive notifications of alleged infringement.[95] The service provider must submit to the Copyright Office "substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent [and] (B) other contact information which the Register of Copyright may deem appropriate."[96] The same information must also be available through its service, and posted on its website (if it has one) in a location accessible to the public.[97]

This requirement obviously applies to section 512(c), the system storage safe harbor, because subsection (2) states that the designated agent is a requirement for the "limitations on liability established *in this subsection* [to] apply to a service provider."[98] The requirement also applies to the system caching and information location tools safe harbors because each references section 512(c)(3).[99] Section 512(c)(3), discussed in greater detail below, outlines the elements a notification must substantially contain in order for it be considered "effective" notice of copyright infringement.[100] "To be effective under [§ 512(c)(3)], a notification of claimed infringement must be a written communication provided *to the designated agent* of a service provider."[101] Thus, the cross references of the statute impose an additional requirement on three of the safe harbors to make available an agent to receive complaints of alleged copyright infringement.

D. The System Caching Safe Harbor: Section 512(b)

Caching occurs when a system creates a "temporary storage area for frequently-accessed or recently-accessed data . . .[to] speed[ ] up

92. *See* § 512(b).
93. *See* § 512(c).
94. *See* § 512(d).
95. *See* § 512(c)(2).
96. *Id.*
97. *See id.*
98. *Id.* (emphasis added).
99. *See* § 512(b)(2)(E), (d)(3).
100. *See* § 512(c)(3). A service provider incurs additional obligations upon receipt of effective notice. *See* § 512 (b)(2)(E), (c)(1)(C), (d)(3).
101. § 512(c)(3)(A) (emphasis added).

the operation of the computer."[102] Thus, when a service provider creates a cache file, it stores Internet material on its own servers. A service provider will usually cache Internet sites frequently visited by its users in order to speed up the transmission of information from those sites. By speeding up the transmission, congestion on the server is decreased. Systems are normally designed to update their cached files automatically.

Section 512(b) consists of eight requirement that must be met, and is divided into two parts: the first three requirements describe the actions to which the limitation on liability applies[103] and the last five requirements describe conditions that must be met to claim that limitation.[104]

1. Actions That Qualify for Limitation on Liability

A limitation on liability for copyright infringement is provided for the "intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider" in a specific situation which is described by the statute.[105]

The statute first states that the material must be made available by a person other than the service provider.[106] For simplicity's sake, this "person other than the service provider" will be referred to as the "originator." The material must then be transmitted through the system from the originator to a user (i.e., a person other than the originator) at the user's request.[107] After such a transmission, any temporary storage of the originator's material on the system must occur by means of an automatic technical process in order to make that material available to other users who request access.[108]

For example, SP is a service provider. O, an originator, posts an infringing copy of a magazine article on a website, Site A. A user of SP's system accesses Site A, and the infringing material is transmitted through SP's system to the user. Ten other users of SP's system also access Site A. In order to speed up transmissions to its users, SP designed its system to automatically make a cache file of any website that is visited by 5 or more users. Thus, in the situation just described, SP

102. Computeruser.com, *at* http://www.computeruser.com/resourcesdictionary/index.html (last visited Apr. 29, 2001).
103. *See* § 512(b)(1).
104. *See* § 512(b)(2).
105. § 512(b)(1).
106. *See* § 512(b)(1)(A).
107. *See* § 512(b)(1)(B).
108. *See* § 512(b)(1)(C).

would not be liable for copyright infringement that occurred on Site A, provided the remaining five requirements are met.

2. Conditions for Qualification

Five additional conditions apply to the system caching safe harbor. The first, and arguably most important, is that the material cannot be modified after its initial transmission.[109] Second, the service provider must comply with a generally accepted industry standard protocol regarding rules concerning refreshing, reloading, or other updating of the material.[110] Those rules, however, must not prevent or unreasonably impair the intermediate storage of the material.[111] Third, the service provider must not interfere with the ability of technology to return to the originator information that would have been collected had the material been accessed on the originating, rather than the cached, site.[112] This includes information such as the number of "hits"[113] on the site and any data entered by users of the site. Fourth, if the originator has conditions that must be met before a user can access the material, such as a password or fee, the service provider must also require that those conditions to be met.[114]

The last requirement is somewhat complicated and is best explained in two parts: as an the obligation of the service provider, and as a situation in which the service provider becomes subject to the obligation. If the service provider receives proper notice[115] from the copyright owner (or her agent) that the material posted is infringing, the service provider must remove or block access to that material.[116] However, the service provider must only do so if the party giving notification confirms[117] that the allegedly infringing material has actually been removed, or a court has ordered it to be removed, from the originating site.[118]

The following example is illustrative: Suppose "Holder" is the holder of the copyright in "Picture." Originator posts an infringing

109. *See* § 512(b)(2)(A).
110. *See* § 512(b)(2)(B).
111. *See id.*
112. *See* § 512(b)(2)(C).
113. This is the number of people who access a website.
114. *See* § 512(b)(2)(D).
115. *See* Part VI, below for a further discussion and details.
116. *See* § 512(b)(2)(E). For the sake of simplicity in explaining the statutory provisions, any further references in this paper to *removal* of allegedly infringing material will also include *blocking access* to that material, unless otherwise specified.
117. *See* § 512(b)(2)(E)(ii).
118. *See* § 512(b)(2)(E)(i).

copy of Picture on Site A. Several of the users of SP's system have accessed Picture on Site A, so SP's system has automatically made a cache file of Site A. Assuming the first four safe harbor conditions have been met, SP is now under an obligation to remove the infringing material from its system upon receiving proper notice from Holder that Originator has posted an infringing copy of Picture on Site A. However, SP is only subject to this obligation if Holder confirms that the infringing copy of Picture has actually been removed (or has been ordered by a court to be removed) from Site A.

There have not yet been any cases involving this particular safe harbor. Presumably, however, it is not applicable when a service provider mirrors a particular site. When a site is mirrored, the service provider selectively, as opposed to automatically, decides to store a particular website on its server.[119] Since it does not occur automatically, mirroring would not appear to be the type of caching the statute is designed to protect.[120]

E. System Storage and Information Location Tools Safe Harbors

While they are intended to cover different activities, the system storage and the information location tools safe harbors essentially share the same requirements. The system storage safe harbor limits liability for copyright infringement for "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."[121] This includes "providing server space for a user's website, for a chat room, or other forum in which material may be posted at the direction of users."[122]

The information location tools safe harbor limits liability for copyright infringement for "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link."[123]

119. *See* Matisse.net, *at* http://www.matisse.net/flies/glossary.html#P (last visited Aug. 13, 2002).

120. *See* § 512(b)(1)(C).

121. § 512(c)(1).

122. SENATE REPORT, *supra* note 2, at 43.

123. § 512(d).

1. System Storage and Information Location Tools Safe Harbor Requirements

The first requirement is directed at the knowledge standard of the service provider regarding copyright infringement.[124] The statute lays out three possible levels of awareness of the infringing material or activity for which the service provider can claim the safe harbor.

One possibility is that the service provider lacks actual knowledge of the infringing material or activity.[125] A second possibility under which a service provider can claim the safe harbor is when it has no knowledge of any facts or circumstances from which infringing activity is apparent.[126] This is referred to as the "red flag" test.[127] The service provider is not under an obligation to monitor or actively seek out infringing material on its service, but if it becomes aware of "a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action."[128] Whether or not the facts constitute a "red flag" is an objective determination, even though a subjective analysis of the service provider's awareness can help determine whether the service provider was aware of the facts.[129] The third possibility is where the service provider obtains the aforementioned knowledge or awareness. In that instance, it may still claim the safe harbor as long as it "acts expeditiously to remove, or disable access to, the material."[130]

The second requirement is that, where the service provider has the right and ability to control the infringing activity, it cannot receive a financial benefit that is directly attributable to that activity.[131] The third requirement obligates a service provider to remove or block access to allegedly infringing material upon receipt of proper notice from the copyright holder or her agent.[132] The party who posted the material may, in some cases, contest removal of the material. While the details of the service provider's responsibilities in such a situation are beyond the scope of this paper, they can be found in section 512(g).

124. *See* § 512(c)(1)(A), (d)(1).
125. *See* § 512(c)(1)(A)(i), (d)(1)(A).
126. *See* § 512(c)(1)(A)(ii), (d)(1)(B).
127. *See* SENATE REPORT, *supra* note 2, at 44.
128. *Id.*
129. *See id.*
130. § 512(c)(1)(A)(iii), (d)(1)(C).
131. *See* § 512(c)(1)(B), (d)(2).
132. *See* § 512(c)(1)(C), (d)(3).

2. The Vicarious Liability Conundrum

The Copyright Act does not impose liability on one party for another party's acts, i.e. there is no provision for secondary copyright infringement.[133] Thus, courts developed two doctrines of secondary infringement: vicarious and contributory infringement. An individual or other entity can be held liable for vicarious copyright infringement for (1) having the ability to control the activity of the direct infringer and (2) receiving a financial benefit from that activity.[134]

The system storage and information location tools safe harbors lay out the "circumstances under which a service provider would lose the protection of subsection (c) [or subsection (d)] by virtue of its benefit from and control over the infringing activity."[135] This exception makes it seem that neither of these safe harbors shelters vicarious copyright infringers.

a. The Control Prong

One commentator argues that "[a] narrow construction of the codified control prong can . . . salvage protection for qualifying service providers."[136] He argues that Title II of the DMCA can be reconciled with common law vicarious liability by reading actual control, as opposed to legal control, into the statute.[137]

Wright points out that there have been two approaches to the control prong of the vicarious liability test.[138] The narrow approach requires that the alleged vicarious infringer have actual control, and looks primarily at the "defendant's ongoing ability to prevent the actual infringement."[139] To be liable for vicarious copyright infringement, the defendant must be in a position so that she can actually take action to prevent infringement.[140]

133. *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A] (2000).

134. *See id.* at § 12.04[A][1].

135. SENATE REPORT, *supra* note 2, at 44.

136. 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 (2000).

137. *See id.*

138. *See id.* at 1012. Wright's article focuses solely on the language of the system storage safe harbor in § 512(c)(1)(B). Since the language of the information location tools safe harbor in § 512(d)(2) is identical, Wright's arguments can be expanded to apply to the latter section, too.

139. *Id.* at 1013 (citation omitted).

140. *See id.* at 1016.

The broader approach requires simply legal control, which will find "control in every legal relationship in which one party reserves, implicitly or explicitly, control over the infringer."[141] Thus, a party with potential rather than actual control over the direct infringer can be vicariously liable for copyright infringement, making the control prong appear as if it is a mere formality.[142]

Wright suggests that courts should read section 512(c)(1)(B) to require actual control.[143] He argues that the text of the statute, its structure, and the legislative history all support an actual control requirement.[144] If the statute is read to require only legal control, protection for vicariously liable service providers would be eliminated.[145] The only service provider who would be able to claim the safe harbor would be one who had either no ability to control the direct infringer, or one who realized no economic benefit from the infringer's acts.[146] However, a service provider lacking either control or a financial benefit would not need the safe harbor, as it could not be found vicariously liable for copyright infringement anyway.[147]

Furthermore, other requirements of subsections 512(c) and 512(i) are analogous to the findings of control that courts have made when holding a vicarious infringer liable under the legal control standard.[148] Section 512(c)(2) requires that the service provider have a designated agent available to receive notifications of alleged infringement. In *Gershwin Publishing Corp. v. Columbia Artists Management*,[149] the court found the defendant was vicariously liable because it exhibited the requisite control from its ability to police the infringing activity. Therefore, a service provider in compliance with section 512(c)(2) could be found to have lost the protection of the information location tools or system storage safe harbor if § 512(c)(1)(B) is read to require only legal control.[150]

Additionally, section 512(i) requires that the service provider implement a policy of terminating the accounts of repeat infringers. In *Fonovisa, Inc. v. Cherry Auction, Inc.*,[151] the court found that contractual

141. *Id.* at 1012.
142. *See id.* at 1016.
143. *See id.* at 1026.
144. *See id.*
145. *See id.* at 1028.
146. *See id.*
147. *See id.* at 1029.
148. *See id.* at 1029–31.
149. 443 F.2d 1159, 1163 (2d Cir. 1971).
150. *See* Wright, *supra* note 134, at 1007.
151. 76 F.3d 259, 262 (9th Cir. 1996).

control was sufficient for a finding of vicarious liability. Thus, a court applying the legal control standard would find that a service provider that complied with section 512(i) would not be able to claim the information locations tools or system storage safe harbor. Looking at these possible outcomes, it would not make sense that a requirement for a service provider to claim the proection of a safe harbor would simultaneously prevent the service provider from claiming the desired protection.

b. The Financial Benefit Prong

Courts should also be careful to not read the financial benefit element of section 512(c)(1)(B) too strictly. If courts find the service provider is financially benefiting from the infringement, the service provider can not claim the benefit of either the system storage or the information location tools safe harbors. In its discussion of section 512(c)(1)(B), the Senate Report indicated that Congress did not intend this section to be interpreted too narrowly. "In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one."[152] Thus, subsection 512(c)(1)(B) was not intended to banish from its protection a service provider conducting a legitimate business.

For example, charging all users a one-time set-up fee or a flat periodic payment for the provider's services would not mean that the service provider was deriving a financial benefit from any infringing activity that might occur on its system. Neither would charging user fees based on the length of the message they posted or by the amount of time they were connected to the service.[153] In contrast, fees charged where the value of the service depends on providing access to infringing material would eliminate the service provider's safe harbor protection.[154]

Therefore, courts should read sections 512(c)(1)(B) and 512(d)(2) as requiring the service provider to have actual control over the direct infringer before the service provider loses the protection of either safe harbor. Indeed, the Ninth Circuit stated that "[w]e need not accept a blanket conclusion that § 512 of the Digital Millennium Copyright Act will never protect secondary infringers."[155] Additionally, courts should recognize assessed user charges do not necessarily

152. SENATE REPORT, *supra* note 2, at 44.
153. *See id.*
154. *See id.*
155. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

mean the service provider is receiving a financial benefit from any infringement that might occur on its system.

VI. Effective Notice Under Section 512(c)(3)

As noted above, a service provider that receives proper notice of alleged copyright infringement becomes subject to another requirement if it wishes to claim the protection of the system caching, system storage, or information location tools safe harbors. Specifically, it must remove or disable access to the allegedly infringing material, and provide proper notice of the alleged infringement.[156] In order to constitute proper notification, the notice must be written and "include[ ] substantially the following"[157] elements.

A. Elements of Proper Notice

1. Verification Requirements

Three of the six elements of proper notice relate to verification of the person filing the notice (the "complainant"). The verification elements include a requirement that the notice be signed, physically or electronically, by a person authorized to act on behalf of the owner of the allegedly infringed right.[158] The complainant must also include a written statement that he has a "good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law."[159] The final verification element requires the complainant to include an affidavit stating that the information in the notice is accurate, and a statement under penalty of perjury that the complainant is authorized to act on behalf of the owner of the allegedly infringed copyright.[160] Note that the complaint itself need not be made under oath.

156. *See* 17 U.S.C. § 512(b)(2)(E), (c)(1)(C), (d)(3). "Subsection (b)[(2)(E)] establishes a notification and take down procedure for cached material modeled on the procedure under subsection (c)" with certain exceptions, as discussed above in Part V.C. *See also* SENATE REPORT, *supra* note 2, at 43. "Subsection (d) incorporates the notification and take down structure of subsection (c) and applies it to the provision of references and links to infringing sites." SENATE REPORT, *supra* note 2, at 47.

157. § 512(c)(3)(A).

158. *See* § 512(c)(3)(A)(i).

159. § 512(c)(3)(A)(v).

160. *See* § 512(c)(3)(A)(vi).

2. Identification Requirements

The other three elements of proper notification (the "identification requirements"), require the complainant to give the service provider enough information to be able to identify: (1) the allegedly infringed work,[161] (2) the allegedly infringing work,[162] and (3) the complainant.[163] If several works from a single website are allegedly infringed, one notification for all of them is sufficient if it contains a representative list of those works.[164]

When the complainant identifies the allegedly infringing work, i.e. the work she would like removed, she must supply the service provider with sufficient information to locate the allegedly infringing material.[165] In the case of the information location tools safe harbor, this element requires the notice to identify the "reference or link[ ] to material or activity claimed to be infringing . . . and information reasonably sufficient to permit the service provider to locate that reference or link."[166]

Finally, the complainant must include in the notice reasonably sufficient information to allow the service provider to contact him, such as an address, telephone number, or e-mail address.[167]

3. Substantial Compliance

The statute provides that if the notice fails to substantially comply with the listed elements, it shall not be considered in determining whether the service provider had actual knowledge of infringing activity or was aware of facts from which infringing activity was apparent.[168] As discussed previously, actual knowledge of infringement or awareness of facts from which infringing activity is apparent precludes a service provider from claiming the protection of either the system storage or the information location tools safe harbors.[169]

However, the introductory language of section 512(c)(3)(A)—that the notification need only comply "substantially" with the listed elements—and the provisions of section 512(c)(3)(B)(ii) indicate that there need not be *strict* compliance with all six elements. Indeed,

161. *See* § 512(c)(3)(A)(ii).
162. *See* § 512(c)(3)(A)(iii).
163. *See* § 512(c)(3)(A)(iv).
164. *See* § 512(c)(3)(A)(ii).
165. *See* § 512(c)(3)(A)(iii).
166. § 512(d)(3).
167. *See* § 512(c)(3)(A)(iv).
168. *See* § 512(c)(3)(B)(i).
169. *See* § 512(c)(1)(A), (d)(1)

the latter provides that if the notice complies substantially with the identification requirements, it will be sufficient to put the service provider on notice of the alleged infringement.

B. "Substantial Compliance" Applied: *ALS Scan v. RemarQ Communities, Inc.*[170]

The Fourth Circuit dealt with such a "substantial compliance" issue in *ALS Scan, Inc.* The plaintiff, ALS Scan, displayed its copyrighted adult photos on the Internet to paying customers and sold them on CD ROMs and videotapes.[171] The defendant, RemarQ, was an "online Internet service provider" providing access to over 30,000 newsgroups for its subscribers.[172] Two of the newsgroups on RemarQ's service incorporated ALS Scan's name in their titles and contained hundreds of images that infringed ALS Scan's copyrights.[173] The postings were placed there by subscribers.

When plaintiff discovered its copyrights were being infringed, it sent the defendant a cease and desist letter, requesting that the defendant stop carrying the two newsgroups.[174] The letter identified the newsgroups, a web address where plaintiff's models could be found, and a web address where its copyright information could be found.[175] RemarQ responded that it would not cease carrying the newsgroups, but would remove individual infringing items if ALS Scan specifically identified them.[176] Rather than identify the allegedly infringing items, ALS Scan responded by stating that there were 10,000 of its copyrighted images on RemarQ's system, and that the two newsgroups appeared to have been created solely for the purpose of posting and distributing ALS Scan's copyrighted images.[177] After failed negotiations between the parties, ALS Scan filed suit for copyright infringement, claiming that RemarQ had both actual and constructive knowledge of the infringing material. The latter claim was based on the notice ALS Scan gave to RemarQ.[178]

170. 239 F.3d. 619 (4th Cir. 2001).

171. *See id.* at 620.

172. *Id.* In this case, as in *Napster Summary Adjudication,* the plaintiff did not challenge the defendant's status as a service provider. *See id.* at 623.

173. *See id.* at 620. The newsgroups were entitled "alt.als" and "alt.binaries.pictures.erotica.als."

174. *See id.*

175. *See id.* at 620–21.

176. *See id.* at 621.

177. *See id.*

178. *See id.*

RemarQ filed a motion to dismiss and in the alternative, for summary judgment, claiming that it was protected by the DMCA's system storage safe harbor.[179] It claimed that it did not have knowledge of the infringement because ALS Scan failed to comply with the notice requirements of section 512(c)(3)(A).[180] The district court ruled for the defendant, finding that RemarQ was not liable for contributory infringement because ALS Scan's notice did not comply with the required notice provision.[181]

The Fourth Circuit disagreed, holding that ALS Scan substantially complied with the notice requirement, thus obligating RemarQ to remove the infringing material.[182] Since RemarQ failed to do so, it did not meet the third element of the system storage safe harbor, and, therefore, could not claim its protection.[183]

The court reasoned that, for the purposes of the statute, it was sufficient for ALS Scan to provide RemarQ with information (1) identifying two newsgroups that it alleged were created for the sole purpose of publishing ALS Scan's copyrighted works; (2) claiming that the two newsgroups consisted almost exclusively of ALS Scan's copyrighted material; and (3) referring RemarQ to two web addresses where it could find pictures of ALS Scan's models and copyright information.[184] The court also found persuasive ALS Scan's claim that all of its material contained ALS Scan's name and/or copyright symbol.[185]

According to the court, this information substantially complied with the requirement that ALS Scan provide "a representative list of infringing material as well as information reasonably sufficient to en-

179. *See id.* at 621, 623.

180. *See id.* at 622.

181. *See id.* at 621–22. It is not clear whether the court granted the motion to dismiss or the motion for summary judgment. The district court stated that it was treating the defendant's motion to dismiss as one for summary judgment. *See id.* However, the Fourth Circuit noted that the district court's procedure was inconsistent with a grant of summary judgment. *See id.* at 623. The court ultimately decided that this point was unimportant because it concluded that RemarQ was not entitled to the protection of the system storage safe harbor. *See id.* at 624.

182. *See id.* at 624.

183. *See id.* The court ruled in defendant's favor with regard to direct copyright infringement because the DMCA codified the rule from *Religious Technology Center. v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995) that "liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another." (quoting H.R. REP. No. 105–551(I), at 11 (1998)).

184. 239 F.3d. 619, 625 (4th Cir. 2001).

185. *See id.*

able RemarQ to locate the infringing material."[186] The court misconstrued the statute, however. The complainant is supposed to give a representative a list of the allegedly *infringed* items, i.e. the copyrighted ones, not of the allegedly *infringing* ones.[187] The notification did include ALS Scan's website, but it did not include a representative list of the infringed works. To substantially comply with the notice requirements, the plaintiff should have included printed copies of the copyrighted images, or provided a CD ROM containing the images.

As for the allegedly infringing material, the complainant is required to supply the service provider with substantially enough information to locate *and* identify the material.[188] The Senate Report indicates that an example of sufficient information would be "a copy or description of the allegedly infringing material *and* the URL address of the webpage which is alleged to contain the infringing material."[189] Here, ALS Scan only provided RemarQ with the location of the allegedly infringing material. It failed to include either a copy or a description of the targeted material.

"The goal of this provision is to provide the service provider with adequate information to find and address the allegedly infringing material *expeditiously*."[190] In a case such as this, where the complainant and the service provider clearly disputed whether all of the images were infringing, simply telling the service provider where the allegedly infringing material might be found does not serve this goal. The service provider would have to spend a great deal of time sifting through thousands of images, likely not knowing what specifically to look for.

Moreover, the court acknowledged that the parties disputed not only this issue, but also whether the sole purpose of the newsgroups was to distribute, and thus infringe, ALS Scan's copyrighted works.[191] Despite these contested issues of fact, the court concluded that the notice was sufficient.[192] However, this decision allows copyright owners to deny service providers the protection of three of the DMCA's safe harbors by filing bald, sweeping allegations of copyright infringement on the service providers' systems. Thus, this decision seems to fly in the face of the purpose of the DMCA: to "preserve[ ] strong incentives for service providers and copyright owners to cooperate to detect

186. *Id.*
187. *See* 17 U.S.C. § 512(c)(3)(A)(ii).
188. *See* § 512(c)(3)(A)(iii).
189. SENATE REPORT, *supra* note 2, at 46 (emphasis added).
190. *Id.* (emphasis added).
191. *See ALS Scan*, 239 F.3d at 626.
192. *See id.* at 625.

and deal with copyright infringements that take place in the digital networked environment . . . [and] provide[ ] greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[193]

Conclusion

Congress's intent in passing the DMCA was to encourage service providers to invest in expanding the Internet by giving them more certainty as to the extent of their liability for copyright infringement. In giving service providers a series of safe harbors, Congress wanted to "ensure[ ] that the efficiency of the Internet [would] continue to improve and that the variety and quality of services on the internet [would] expand."[194]

However, an overly strict reading of the provisions of section 512 will deny service providers the protection Congress desired them to have. If service providers are denied that protection, they will cease to invest in Internet expansion, and individuals, such as Shawn Fanning, will no longer have an incentive to create new technologies, like Napster.

Congress drafted the DMCA after considering the comments of "the major copyright owners and the major OSP's and ISP's . . . [as well as] representatives of individual copyright owners and small ISP's."[195] After hearing from both sides, Congress struck a balance between protecting the rights of copyright holders and protecting the rights of service providers to freely expand their technologies without fear of liability for copyright infringement. It would not be appropriate for the courts to tilt that balance in favor of the copyright owners. The courts should give the statute the effect that Congress intended.

Ultimately, the courts should adopt the following analysis for section 512 claims: First, a court should first make sure the entity claiming immunity fits the definition of "service provider" for the particular safe harbor that provider hopes to apply. To use the conduit safe harbor, it must meet the narrow definition. For all the other safe harbors, meeting either definition will suffice. Second, the court should look to see if the service provider meets the basic statutory requirements. The court should consider, however, that most website operators do not use access control measures, such as passwords, for internet users to

193. *Id.* at 625 (quoting H.R. Conf. Rep. No. 105–796, at 72 (1998).
194. SENATE REPORT, *supra* note 2, at 8.
195. SENATE REPORT, *supra* note 2, at 9–10.

view their sites. Thus, such entities may not be able to block repeat infringers from their services. Third, if the service provider is relying on the system cache, system storage, or information location tools safe harbor, the service provider must register an agent with the Copyright Office, whose job it is to receive notice of the alleged infringement. Fourth, the court should analyze whether the particular activities the service provider seeks to insulate from liability meets all of the elements of the claimed safe harbor. Additionally, if the copyright owner notified the service provider of the alleged infringement, the court should make sure the notice was proper, and that the service provider responded accordingly. This analysis should be done while keeping in mind the purpose of Title II of the DMCA: to provide service providers with an incentive to continue to improve, develop, and expand the Internet.