

Winter 2005

## An Umbrella or a Canopy?: Why the 17 U.S.C. Section 512(a) Safe Harbor Should Be Read Broadly

Sven Skillrud

Follow this and additional works at: <https://scholarship.law.marquette.edu/iplr>



Part of the [Intellectual Property Law Commons](#)

---

### Repository Citation

Sven Skillrud, *An Umbrella or a Canopy?: Why the 17 U.S.C. Section 512(a) Safe Harbor Should Be Read Broadly*, 9 Marq. Intellectual Property L. Rev. 91 (2005).

Available at: <https://scholarship.law.marquette.edu/iplr/vol9/iss1/4>

This Comment is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Intellectual Property Law Review by an authorized editor of Marquette Law Scholarly Commons. For more information, please contact [elana.olson@marquette.edu](mailto:elana.olson@marquette.edu).

# **An Umbrella or a Canopy?: Why the 17 U.S.C. Section 512(a) Safe Harbor Should Be Read Broadly**

## **I. INTRODUCTION**

Copyright law arose when the framers of the Constitution gave Congress the power “[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors . . . the exclusive Right to their respective Writings . . . .”<sup>1</sup> Exercising this power in 1790, Congress created the first copyright law.<sup>2</sup> “Since then, the Supreme Court has defined the public purpose of copyright as one that intends to encourage and reward the creative expression of authors in exchange for a limited period of protection.”<sup>3</sup> Recently, within the past century, Congress has addressed these copyright law issues concluding in the enactment of the Copyright Act of 1976<sup>4</sup> and, ultimately, the passage of the Digital Millennium Copyright Act of 1998 (DMCA).<sup>5</sup>

With technology constantly changing, the interaction between copyright law and technology is always at odds, especially since the evolution of the Internet.<sup>6</sup> To keep up with the ever-changing Internet,

---

1. U.S. CONST. art. I, § 8, cl. 8.

2. See Brad Scheller, Note, *Hey, Keep Your Links to Yourself! Legal Challenges to Thumbnails and Inline Linking on the Web and the Potential Implications of a First Impression Decision in Kelly v. Arriba Soft Corp.*, 10 VILL. SPORTS & ENT. L.J. 415, 428-29 (2003).

3. *Id.* at 429.

4. Copyright Act of 1976, Pub L. No. 94-553, 90 Stat. 2550, (codified as amended at 17 U.S.C. §§ 101-1332 (2000)).

5. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

6. See generally Ryan Roemer, *The Digital Evolution: Freenet and the Future of Copyright on the Internet*, 2002 UCLA J.L. & TECH 5 at [http://www.lawtechjournal.com/articles/2002/05\\_021229\\_roemer.php](http://www.lawtechjournal.com/articles/2002/05_021229_roemer.php) (last visited Feb. 1, 2005). “The thesis of this paper is that the technology of P2P systems is stretching the applicability of modern copyright law to its limits. Content owners will possibly see the day that a technology like Freenet will render the current law ineffective against digital copyright infringement on the Internet.” *Id.* See also Ryan C. Edwards, *Who Said Nothing in This World Is Free? A & M Records, Inc. v. Napster, Inc.: Problems Presented, Solutions Explored, and Answers Posed*, 89 KY. L.J. 835, 874 (2001).

Moreover, there is a concern that Congress faces the same problems as the judiciary; despite the fact that it can act much more swiftly, technology is changing at an even quicker pace. One need look no further than the DMCA for an example. The DMCA was enacted for copyright management information protection, as well as

Congress enacted the DMCA;<sup>7</sup> one of the purposes of the DMCA was to provide “safe harbors” for Internet service providers, intended to protect those entities from allegations of copyright infringement.<sup>8</sup> However, it seems that the courts have had trouble interpreting who is covered under these safe harbors,<sup>9</sup> namely, as to what entities qualify under the first safe harbor “Transitory Digital Network Communications.”<sup>10</sup> There are only a few cases where entities have qualified under the “Transitory Digital Network Communications” safe harbor.<sup>11</sup>

This Comment will argue that more entities should qualify under the safe harbor 17 U.S.C. § 512(a), “Transitory Digital Network Communications.” Part II will provide a background of the Digital Millennium Copyright Act. Part III will explain safe harbor 17 U.S.C. § 512(a), “Transitory Digital Network Communications.” Part IV will discuss the legislative history behind the passage of 17 U.S.C. § 512(a). Part V will argue why 17 U.S.C. § 512(a) should be read broadly. Finally, Part VI will provide a brief conclusion.

---

protection for online service providers. In the author's opinion, the reason that Napster does not qualify under the DMCA is not truly because it fails to satisfy § 512(a). Rather, it is because the DMCA, enacted only two years ago by Congress, in all likelihood could not imagine a service like Napster. It would seem, then, that the legislature, like the courts, cannot move quickly enough to respond to technological change.

*Id.* 874.

7. See Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

8. See generally 17 U.S.C. §§ 512(a)-(d).

9. See, e.g., *ALS Scan, Inc. v. Remarq Cmty., Inc.*, 239 F.3d 619 (4th Cir. 2001) (applying safe harbor 512(c) to an Internet service provider, Remarq Communities); *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077 (C.D. Cal. 2004) (applying safe harbor 512(a) to an age verification system and payment processing companies); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002) (applying safe harbors 512(c) and 512(d) to an age verification service, Cybernet Ventures); *Costar Group, Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688 (D. Md. 2001) (applying safe harbor 512(c) to a web site host, Loopnet); *Ellison v. Robertson*, 189 F. Supp. 2d 1051 (C.D. Cal. 2002), *rev'd on other grounds*, 357 F.3d 1072 (9th Cir. 2004) (Applying safe harbor 512(a) to America Online as an Internet service provider); *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 634 (N.D. Ill. 2002) (applying safe harbors 512(a), 512(b), and 512(d) to peer-to-peer file sharing program, Aimster); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (applying safe harbor 512(c) to eBay); *A & M Records, Inc. v. Napster, Inc.*, 54 U.S.P.Q.2d (BNA) 1746 (N.D. Cal. 2000) (applying safe harbor 512(a) to Napster).

10. See 17 U.S.C. § 512(a).

11. See *Ellison*, 189 F. Supp. 2d at 1051; *Perfect 10*, 340 F. Supp. 2d 1077 at 1091.

## II. DIGITAL MILLENNIUM COPYRIGHT ACT

Congress's purpose behind the passage of the DMCA was to implement a pair of international treaties, the Copyright Treaty and the Performances and Phonograms Treaty, which were signed by more than 125 other countries, including the United States, before the World Intellectual Property Organization (WIPO) in Geneva during 1996.<sup>12</sup> These treaties came about as countries recognized the possibility to update copyright laws with regard to the digital revolution; specifically, the growth of globalization, the Internet, and electronic commerce.<sup>13</sup> Initially, the DMCA simply implemented the two WIPO treaties as freestanding law, but as the legislative debate and recognition for a balance between "promoting the continued growth and development of electronic commerce; and protecting intellectual property rights"<sup>14</sup> grew, the DMCA was expanded.

Signed into law on October 28, 1998, the DMCA addresses, among other things, the effect of the Internet on such copyrighted works as photographs, sound recordings, and motion pictures, along with the other possible endless amounts of copyrighted works that may be transmitted over the Internet.<sup>15</sup> The DMCA is divided into five titles.<sup>16</sup> Whereas each Title addresses different copyright issues, for purposes of

---

12. See H.R. REP. NO. 105-551, pt. 2, at 21 (1998). Specifically, "[i]n July 1997, the Clinton Administration submitted the treaties to the Senate for ratification and submitted proposed implementing legislation to both the House and the Senate." *Id.*

13. See *id.*

14. *Id.* at 23.

These goals are mutually supportive. A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment. And a plentiful supply of intellectual property—whether in the form of software, music, movies, literature, or other works—drives the demand for a more flexible and efficient electronic marketplace.

*Id.*

15. U.S. Copyright Off., The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary (Dec. 1998), *available at* <http://www.copyright.gov/legislation/dmca.pdf>.

16. See *id.* The five titles include: Title I which implements two recent 1996 World Intellectual Property Organization (WIPO) treaties; Title II which creates copyright infringement liability limitations for online service providers; Title III which allows for a copyright infringement exemption when copying a computer program for the purpose of maintenance or repair; Title IV which contains six miscellaneous provisions that relate to everything from the function of the Copyright Office to the "webcasting" of sound recordings over the Internet; and Title V which safeguards against liability for design of vessel hulls. See *id.*

this Comment the focus will be on Title II: Online Copyright Infringement Liability Limitation Act.<sup>17</sup>

Title II adds section 512 to the Copyright Act to ensure that the growth of the Internet is not hindered by copyright infringement liability.<sup>18</sup> Section 512, among other things,<sup>19</sup> creates four safe harbors for online service providers to escape certain monetary damages and types of injunctive relief.<sup>20</sup> These four safe harbor categories include: (1) "Transitory Digital Network Communications";<sup>21</sup> (2) "System Caching";<sup>22</sup> (3) "Information Residing On Systems Or Networks At Direction Of Users";<sup>23</sup> and (4) "Information Location Tools."<sup>24</sup> Each of these four safe harbors is independent of the others and because a service provider qualifies for one safe harbor does not mean that the service provider qualifies for the other three.<sup>25</sup> Furthermore, a service provider that fails to qualify for any of the four safe harbors is not automatically liable for copyright infringement since the burden is still on the copyright owner to prove infringement, and the service provider may still utilize any of the general copyright defenses, such as fair use.<sup>26</sup>

### III. ARTICLE 17 U.S.C. § 512(A), "TRANSITORY DIGITAL NETWORK COMMUNICATIONS"

Article 17 U.S.C. § 512(a) (512(a)) provides a safe harbor for an online service provider who simply acts as a pass through or middleman by transmitting digital information from one point to another at a user's request.<sup>27</sup> Generally, whereas the definition of an online service

---

17. See 17 U.S.C. § 512.

18. H.R. Rep. No. 105-551, pt. 2, at 50.

19. For purposes of this Comment only the four safe harbor categories of 17 U.S.C. § 512 will be discussed.

20. See 17 U.S.C. § 512(j); Copyright Office Summary, *supra* note 15, at 8.

21. 17 U.S.C. § 512(a).

22. 17 U.S.C. § 512(b).

23. 17 U.S.C. § 512(c).

24. 17 U.S.C. § 512(d).

25. See 17 U.S.C. § 512(n).

Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

*Id.*

26. See 17 U.S.C. § 512(l).

27. See 17 U.S.C. § 512(a).

provider differs depending on the safe harbor, online service providers must meet two overarching conditions to qualify for any one of the four safe harbors: (1) they must adopt and implement a policy that terminates repeat infringers' accounts; and (2) the policy does not interfere with "standard technical measures."<sup>28</sup> Specifically, to qualify as an online service provider for 512(a) the provider must be "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."<sup>29</sup>

Once an entity meets the two overarching conditions, as stated in 17 U.S.C. § 512(i), and qualifies as an online service provider as defined under 17 U.S.C. § 512(k)(1)(A), then the service provider must comply with five conditions to be immune from certain monetary damages and injunctive relief for "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."<sup>30</sup> First, a person other than the online service provider must initiate the transmission of the material.<sup>31</sup> Second, the material should be transmitted, routed, connected, or stored "through an automatic technical process without selection of the material by the service provider."<sup>32</sup> Third, the online service provider may not determine who receives the material, as it is an automatic response at the request of a third person.<sup>33</sup> Fourth, a copy of the material on the system or network is not available "in a manner ordinarily accessible to anyone other than anticipated recipients," and the copy does not remain

---

28. See 17 U.S.C. § 512(i)(2).

As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms;

(C) and do not impose substantial costs on service providers or substantial burdens on their systems or networks.

*Id.*

29. 17 U.S.C. § 512(k)(1)(A).

30. 17 U.S.C. § 512(a).

31. See 17 U.S.C. § 512(a)(1).

32. 17 U.S.C. § 512(a)(2).

33. See 17 U.S.C. § 512(a)(3).

on the online service provider's system or network "for a longer period than is reasonably necessary for the transmission, routing, or provision of connections."<sup>34</sup> Finally, the content of the transmitted material may not be modified.<sup>35</sup>

#### IV. LEGISLATIVE HISTORY BEHIND THE PASSAGE OF 17 U.S.C. § 512(A)

Being a relatively new statute, there is only a small amount of case law interpreting the DMCA, especially regarding the interpretation of 512(a). Therefore, "[t]o the extent that the statutory language may be unclear, the legislative history of the DMCA can be useful in fleshing out its meaning given the paucity of precedent interpreting the statute."<sup>36</sup> As stated above, the DMCA was originally enacted to comply with two WIPO treaties and expanded to include copyright implications regarding the Internet.<sup>37</sup> Hence, the addition of section 512, the Online Copyright Infringement Liability Limitation Act,<sup>38</sup> to the Copyright Act.

With the passage of section 512, Congress hoped 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."<sup>39</sup> Also, Congress wanted to provide "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."<sup>40</sup> Consequently, the four safe harbors within section 512 were enacted, and Congress created a tradeoff within section 512, as online service providers would escape copyright infringement liability from copyright owners for helping the copyright owners in assisting, dealing, and identifying copyright infringers.<sup>41</sup>

Congress created 512(a) to protect online service providers who act as a mere "conduit" for the communications of others" by "transmitting, routing, or providing connections for material, and [include] some forms of intermediate and transient storage of material in the course of

---

34. 17 U.S.C. § 512(a)(4).

35. See 17 U.S.C. § 512(a)(5).

36. *Costar Group, Inc.*, 164 F. Supp. 2d at 700.

37. See H.R. REP. NO. 105-551, pt. 2, at 20-21.

38. 17 U.S.C. § 512.

39. See H.R. REP. NO. 105-551, pt. 2, at 49.

40. *Id.* at 50.

41. See *In re Verizon Internet Serv., Inc.*, 240 F. Supp. 2d 24 (D.D.C. 2003).

performing these functions.”<sup>42</sup> Congress stated that in this context the terms “intermediate and transient” referred to copied or stored material “in the course of a transmission, not a copy made or stored at the points where the transmission is initiated or received.”<sup>43</sup> Likewise, “[t]he use of the term ‘transmitting’ throughout new section 512 was not intended to be limited to transmissions of ‘a performance or display’ of ‘images or sounds’ within the meaning of Section 101 of the Copyright Act.”<sup>44</sup>

Specifically, Congress addressed each of the five conditions except for 512(a)(1), which seemed to be self-explanatory, as the online service provider may not initiate the transmission of the material. In 512(a)(2), Congress intended the terms “selection of the material” to mean “the editorial function of determining what material to send, or the specific sources of material to place on-line (e.g., a radio station)” and “an automatic technical process” to be that of a response to a command or request by someone or thing such as a user, Internet location tool, or another network.<sup>45</sup> Similarly, in 512(a)(3), Congress stated that the term “automatic response to the request of another” encompasses an online service provider’s actions of responding “to requests by a user or other networks, such as requests to forward e-mail traffic or to route messages to a mailing list agent (such as a “Listserv”) or other discussion group.”<sup>46</sup> Section 512(a)(4) codifies the result of *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*<sup>47</sup> and allows online service providers to escape liability for copies made of material while the material is in transit to its destination.<sup>48</sup> Examples include “copies made on a router or mail server, storage of a web page in the course of transmission to a specific user, store and forward functions, and other transient copies that occur en route.”<sup>49</sup> Also, Congress intended the term “ordinarily accessible” to mean material that is not accessible by third parties; however, material that is accessible by an illegal intruder, service provider personnel in the course of maintenance, or law

---

42. See H.R. REP. NO. 105-551, pt. 2, at 51.

43. *Id.*

44. *Id.* at 51.

45. *Id.*

46. *Id.*

47. 907 F. Supp. 1361 (N.D. Cal. 1995). In this case, the court found that an online service provider was not liable for direct infringement for intermediate copies temporarily stored on its servers during transmission between a bulletin board service and a subscriber to that bulletin board. *Id.* at 1381.

48. See H.R. REP. NO. 105-551, pt. 1, at 24 (1998).

49. See *id.* pt. 2, at 51.



enforcement officials do not qualify as “ordinarily accessible.”<sup>50</sup> “However, the term does not include copies made by a service provider for the purpose of making the material available to other users. Such copying is addressed in subsection (b).”<sup>51</sup> Finally, in 512(a)(5), Congress states that the modification need apply only to the content of the material and not the format; thus, an email that is received, that was originally bolded and not currently displayed as being bolded, does not count as being modified.<sup>52</sup>

Congress also contemplated the narrower definition of “online service provider” found in 512(k)(1), which is a prerequisite to comply with 512(a).<sup>53</sup> Congress based its definition of “service provider” on the definition of “telecommunications” that is found in the Communications Act of 1934<sup>54</sup> because “the functions covered by new subsection (a) are essentially conduit-only functions” and added the terms “digital” and “online” to make the provision apply only to digital communications that are transferred over interactive computer networks such as the Internet.<sup>55</sup> Furthermore, to comply with the section 512(k)(1) definition each specified function must fall under the definition. “For example, hosting a web site does not fall within the new . . . definition, whereas the mere provision of connectivity to a web site does fall within that definition.”<sup>56</sup> Consequently, just because certain online service provider’s functions qualify does not mean that all of the provider’s functions qualify.<sup>57</sup>

#### V. WHY 17 U.S.C. § 512(A) SHOULD BE READ BROADLY

Since the enactment of the DMCA in 1998, there are only a few cases where an online service provider has qualified for the 512(a) safe harbor.<sup>58</sup> There have been numerous other cases where the four safe harbors have been applied and discussed,<sup>59</sup> but the courts restrict 512(a) to only those online service providers who provide Internet access, such as America Online; age verification systems, such as Internet Key; and

---

50. *Id.*

51. *Id.*

52. *See id.*

53. *See* 17 U.S.C. § 512(a).

54. *See* 47 U.S.C. §§ 153–614 (2000).

55. *See* H.R. REP. NO. 105-551, pt. 2, at 63.

56. *Id.* at 63-64.

57. *See id.* at 64.

58. *See, e.g., Ellison*, 189 F. Supp. 2d at 1051; *Perfect 10*, 340 F. Supp. 2d 1077 at 1091.

59. *See* cases cited *supra* note 8.

payment processing companies, such as Ibill and CCBill.<sup>60</sup> This Comment believes that 512(a) applies to more entities.<sup>61</sup>

By narrowly interpreting 512(a), the courts are eliminating the person whom Congress hoped to exempt, the online service provider. As stated above, section 512 offers a tradeoff for online service providers to escape copyright infringement liability in exchange for helping copyright owners in identifying and terminating copyright infringers.<sup>62</sup> Online service providers who are not responsible for initially supplying users with the copyrighted material, but instead only provide an automated link in the chain of access, should not be punished. Absent this immunity, it could be argued that the online service providers access to this copyrighted material would not occur, and therefore, Congress enacted section 512 for exactly this reason, to protect online service providers from contributory and vicarious liability.<sup>63</sup> To narrowly interpret 512(a) undermines Congress's intent to encourage development of the Internet by not removing the threat of litigation over automated activities.

Assuming compliance with the two conditions stated in 17 U.S.C. § 512(i) and the definition of online service provider in 17 U.S.C. § 512(k)(1)(A), 512(a) should apply to any online service provider that controls both ends of the system, or, more specifically, any online service provider that requires its users to have the same software in order to do such things as communicate or transfer files. Nothing in the legislative history specifies that the court narrowly interpret 512(a), as

---

60. See *Ellison*, 189 F. Supp. 2d at 1051; *Perfect 10*, 340 F. Supp. 2d 1077 at 1091.

61. See generally Justin Williamson, Note, *Online Service Provider Copyright Liability: Is the Digital Millennium Copyright Act the Answer?*, 88 KY. L.J. 987 (2000). This note states that 512(a) "may also be broadly read so as to encompass businesses providing employee e-mail accounts as well as media companies hosting strictly informational Web sites." *Id.* at 998.

62. See *Verizon*, 240 F. Supp. 2d at 37.

63. Contra Adam R. Fox, *The Digital Millennium Copyright Act: Disabusing the Notion of a Constitutional Moment*, 27 RUTGERS COMPUTER & TECH. L.J. 267, 273-74 (2001).

The scope of the copyright infringement apparently facilitated by Napster is staggering. In a much-publicized lawsuit brought against the company by various large copyright owners, the district court found that the roughly 75 million Napster users were swapping as many as 10,000 music files *per second*. A year of such use, discounting the continued increase of the number of Napster users, would result in over 300 billion discrete acts of copyright infringement. Proceeding against each individual who directly infringes a copyright owner's exclusive right is clearly burdensome. How, for example, could A & M Records seek and enforce judgments against billions of infringing acts involving millions of individual defendants?

*Id.*

the “[n]ew Section 512(a) applies to communications functions associated with sending digital communications of others across digital networks, such as the Internet and other on-line networks.”<sup>64</sup> To illustrate this expansive reading of 512(a), this Comment will demonstrate how the 512(a) safe harbor applies to two commonly used programs: Instant Messenger and peer-to-peer file sharing programs.

### *A. Instant Messenger Programs*

Instant Messenger (“IM”) programs should qualify for the 512(a) safe harbor. IM programs are commonplace amongst computer users and act as a go-between that allows users to communicate and transfer files between their computers. Numerous different IM programs exist including America Online IM, Yahoo IM, MSN IM, and ICQ IM.<sup>65</sup> This Comment will explain how an IM program works (using America Online Instant Messenger as an example) and argue why IM programs should fall under the 512(a) safe harbor.

America Online IM (“AIM”) allows a user to communicate and transfer files with any other user who has the AIM program.<sup>66</sup> To begin, users must download the AIM client from the Internet located at *aim.com* and install the AIM software on their computer.<sup>67</sup> Once the user opens the AIM client, the client connects to an AIM server “us[ing] a proprietary protocol that is not understood by other instant messaging services.”<sup>68</sup> When the AIM client connects to the AIM server, the client provides the server with that user’s IP address, port number, and a list of the user’s contacts or “buddies.”<sup>69</sup> The server then stores that information and checks to see if any of the user’s buddies are “online,” and, if so, the AIM server sends their connection information to that

---

64. H.R. REP. NO. 105-551, pt. 2, at 50.

65. More information may be found at the Web sites each company has created for offering their IM programs. American Online’s may be found at <http://www.aim.com> (last visited Feb. 2, 2005); Yahoo’s at <http://www.messenger.yahoo.com> (last visited Feb. 2, 2005); MSN’s at <http://messenger.msn.com> (last visited Feb. 2, 2005); and ICQ’s at <http://www.icq.com> (last visited Feb. 2, 2005).

66. See *Aimster*, 252 F. Supp. 2d at 640.

67. For an explanation on the basic method of function of an IM program see Jeff Tyson, *How Instant Messaging Works, How Stuff Works*, at <http://computer.howstuffworks.com/instant-messaging.htm> (last visited Feb. 2, 2005). Tyson’s article specifically discusses the ICQ IM, but the basic process is the same for all IM programs.

68. See *id.* Consequently, AIM may not be used in conjunction with other IMs such as Yahoo or MSN.

69. See *id.*

user.<sup>70</sup> Once it is determined what buddies are online, the user may chat or transfer files with any of the buddies by simply clicking on the specific buddy's name and typing the preferred information or uploading the preferred file and clicking the "send" button.<sup>71</sup> Since the AIM client has the IP address and port number for a buddy's computer, the message or file is sent directly to the AIM client on that buddy's computer without going through the AIM server.<sup>72</sup> Hence, a connection is created directly between the two users, which the user specified material is transferred through. Finally, once a user is finished using the AIM client and logs off, the AIM client sends a message to the AIM server to terminate the session, in which case the server lets all of the user's buddies know that the user has logged off and deletes the temporary file that contained user's IP address and port number information.<sup>73</sup>

Assuming the IM program complies with both 17 U.S.C. § 512(i) conditions, IM programs, such as AIM, are eligible for 512(a) safe harbor immunity from copyright infringement claims, as the IM programs are communication "functions associated with sending digital communications of others across digital networks."<sup>74</sup> IM programs qualify as online service providers under 17 U.S.C. § 512(k)(1)(a) because IM programs transmit or send "digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."<sup>75</sup>

Similarly, IM programs satisfy the requisite conditions under 512(a). First, IM programs transmit or send "material through a system or network controlled or operated by [the IM program]."<sup>76</sup> The material being sent is either the conversation between users (otherwise known as "chatting") or the specified files. The material is transferred through a network controlled and operated by the IM program because the IM program creates the network or connection by providing both users with the software that identifies the requisite IP address and port number to establish or create the network or connection. Furthermore, the IM program controls and operates the network because both users must have that IM's software to establish the network or connection that is

---

70. *See id.*

71. *See id.*

72. *See* Tyson, *supra* note 67.

73. *See id.*

74. H.R. REP. NO. 105-551, pt. 2, at 50.

75. 17 U.S.C. § 512(k)(1)(A).

76. 17 U.S.C. § 512(a).

required to transfer the material through, and only that specific IM program has the ability to terminate the network or connection between the users.<sup>77</sup> Second, the user, not the IM program, “initiate[s] the transmission of the material”<sup>78</sup> by specifying the buddy or other user to establish a connection. Third, the material is automatically transmitted or sent by a command or request from the user with the user determining what to write for the conversation or what file to transfer.<sup>79</sup> Fourth, the user, not the IM program, selects the recipients of the material.<sup>80</sup> Fifth, the IM program does not maintain a copy of the user’s conversation or transferred file and automatically deletes the temporary file containing the user’s IP address and port number information stored on the IM’s server.<sup>81</sup> Finally, the IM program does not modify the content of either the conversation or the transferred file.<sup>82</sup>

Furthermore, allowing IM programs to qualify under 512(a) is aligned with Congress’s intent in passing the 512(a) safe harbor. IM programs could be considered a mere “conduit” for the communications of others,<sup>83</sup> as IM programs allows users to transfer material through a network created by the IM to other users on the network. Likewise, keeping IM programs immune from liability under the 512(a) umbrella follows Congress’s general ideal in passing the section 512 safe harbors, which is not to punish online service providers, but to encourage online service providers to assist copyright owners in dealing with copyright infringement that is done by the online service provider’s users.<sup>84</sup>

### *B. Peer-To-Peer File Sharing Programs*

Section 512(a) insulates peer-to-peer file sharing programs from copyright liability.<sup>85</sup> Analogous to IM programs, peer-to-peer programs

---

77. Assuming the user maintains an Internet connection.

78. 17 U.S.C. § 512(a)(1).

79. See 17 U.S.C. § 512(a)(2).

80. See 17 U.S.C. § 512(a)(3).

81. See 17 U.S.C. § 512(a)(4).

82. See 17 U.S.C. § 512(a)(5).

83. H.R. REP. NO. 105-551, pt. 2, at 51.

84. See *id.*

85. But see Eleanor M. Lackman, *Slowing Down the Speed of Sound: A Transatlantic Race to Head Off Digital Copyright Infringement*, 13 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1161, 1175 (2003). In referring to peer-to-peer file sharing programs:

They could then try to define themselves as ISPs under section 512 and “do their best” to help the record industry stop infringement, even though the services’ “best” may amount to doing nothing. Although this argument could be successful on technical grounds, peer-to-peer services are unlikely to pass the first hurdle that

are premised on the idea that software can act as a middleman between two users who want to share a file. These programs do not provide the users with the material, but simply allow a user access to another user's material over the Internet. To better explain, this Comment will describe in more detail how a peer-to-peer program works (using the old Napster as an example), establish that a peer-to-peer program's technology is basically the same as an IM program under a 512(a) analysis, apply the 512(a) safe harbor to a peer-to-peer program, and rebut the courts' arguments against providing 512(a) immunity to peer-to-peer file sharing programs.

Napster was a peer-to-peer file-sharing program which a user could download from the Internet to access or exchange specific files (such as MP3 music files) with other users.<sup>86</sup> Once the specific software was downloaded, users could access Napster's system from his or her computer by logging in, which automatically connected the user to Napster's servers.<sup>87</sup> Napster's software then read the selected files that the user made available and added those files to a directory and index on Napster's servers that was shared with other users.<sup>88</sup> Users located specific files by typing in the requisite name of the file (such as the name of a song) and clicking on the "search" button.<sup>89</sup> A screen then popped up on the user's computer displaying all the files that matched the search, and the user could select the specific file by clicking on the name of the file.<sup>90</sup> Once the requesting user clicked on the file, Napster's servers routed the request to the other user's browser where the specific file was located to determine if the file could be supplied.<sup>91</sup> If so, Napster's server communicated the other user's IP address and routing information to the requesting user's browser where a connection was made allowing the requesting user to download the file onto his or her computer directly from the other user's computer without any modification of the file.<sup>92</sup> The actual exchange of the file was not

---

Napster failed: the requirement for the service to "transmit, route, or provide connections for allegedly infringing material through its system."

*Id.*

86. *See A&M Records, Inc.*, 54 U.S.P.Q. (BNA) at 1747.

87. *See id.*

88. *See id.*

89. *See id.*

90. *See id.*

91. *See A&M Records, Inc.*, 54 U.S.P.Q. (BNA) at 1747.

92. *See id.*

transmitted through Napster's servers, but through the network or connection created and controlled by Napster's software.<sup>93</sup>

Under a 512(a) analysis, the technology used in a peer-to-peer program and an IM program is essentially the same. Both programs require users to download the requisite software and only establish a connection or network between users who both have that software. Also, both programs control and operate the connection or network because the programs create the network that is used to transfer the material through by providing both users with the necessary IP address and routing information, and only those programs can terminate the network or connection assuming the users are connected to the Internet. Furthermore, the users of both programs, not the programs themselves, initiate and select the recipients of the material. Where the programs differ is how a user specifies to establish a connection with another user. A peer-to-peer program creates a directory from which users choose a specific file to download, whereas a user of an IM program uses its buddy list to establish a connection. But, this process of establishing a connection or network is immaterial under a 512(a) analysis because once the user specifies the file or buddy the creation of the network or connection is the same, as the requisite information to establish the connection is communicated to the specified user's computer. Consequently, if IM programs are covered under 512(a), then peer-to-peer programs will be covered as well.

As stated above, to qualify for 512(a), Napster must first comply with both of the 17 U.S.C. § 512(i) conditions and qualify as an online service provider as defined under 17 U.S.C. § 512(k)(1)(A).<sup>94</sup> Assuming Napster complied with the 17 U.S.C. § 512(i) conditions, Napster qualifies as an online service provider as stated under 17 U.S.C. § 512(k)(1)(A) because Napster was a program or entity that provided "connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or receive."<sup>95</sup>

Like AIM, Napster satisfies the five requisite conditions to comply with 512(a). Napster provided "connections for, material through a system or network controlled or operated by [Napster]"<sup>96</sup> as it provided users, who both have the Napster software, the connection or network

---

93. *See id.*

94. *See* 17 U.S.C. § 512.

95. 17 U.S.C. § 512(k)(1)(A).

96. 17 U.S.C. § 512(a).

to transfer the files through. The files are transferred through Napster's network, and Napster controlled and operated the network because, analogous to AIM, Napster created the network or connection between two users by providing both users with the requisite IP address and routing information to establish or create the network or connection. Furthermore, Napster controlled and operated the network since it controlled both of the transfer points because both the requesting and other user must have the Napster software to transfer the files, and only Napster had the ability to terminate the network or connection between the users.

Again, like AIM, the requesting user, not Napster, initiated the transmission of the specified files, and Napster's program provided a connection to the files "through an automatic technical process without selection of the material."<sup>97</sup> Napster did not determine who received the file "except as an automatic response"<sup>98</sup> to the requesting user, and it did not maintain a copy of the file on its network. Finally, nothing indicated that Napster modified the content of the files that are transmitted through its system.

Whereas this comment argues that both IM and peer-to-peer file sharing programs should be covered under the 512(a) safe harbor, the courts have disagreed. In both *A & M Records, Inc. v. Napster, Inc.*<sup>99</sup> and *In re Aimster Copyright Litigation*,<sup>100</sup> the courts have denied 512(a) safe harbor immunity to peer-to-peer file sharing programs, with only *Aimster* even addressing IM programs. The court in *Aimster* distinguished the file sharing abilities of AIM, which was not even a party to the suit, from Aimster, a peer-to-peer file sharing program, on the basis of "the means by which they allow file transfers between users."<sup>101</sup> The court stated that "Aimster's system makes the process of locating and copying an infringing file extremely easy while the transfer file capabilities of AOL's system are clearly of secondary importance. Even more important . . . is the fact that Aimster clearly encourages, entices, and contributes to the infringement of its users."<sup>102</sup> Hence, it seems that the court in *Aimster* acquiesced to the fact that the file sharing capabilities of AIM should be covered under 512(a), which

---

97. 17 U.S.C. § 512(a)(2).

98. 17 U.S.C. § 512(a)(3).

99. 54 U.S.P.Q. (BNA) at 1747.

100. 252 F. Supp. 2d 634.

101. *Id.* at 656.

102. *Id.*



means that Aimster should have been covered as well because under a 512(a) analysis the process and technology used in both programs is essentially the same. However, the court makes the distinction on the supposed fact that it is easier to locate a file on Aimster and that Aimster encourages or entices users to engage in copyright infringement, which are two facts that are not even addressed by the language in 512(a) or the legislative history.

But, the court in *Perfect 10, Inc. v. CCBill, LLC*<sup>103</sup> distinguishes the holding in *Aimster*. In *Perfect 10*, Perfect 10, the publisher of an adult magazine and owner of the Web site *perfect10.com*, sued an age verification system, Internet Key, and payment processing companies, IBill and CCBill, for copyright infringement.<sup>104</sup> In granting summary judgment, the court held that 512(a) applies to Internet Key, IBill, and CCBill because the entities “provide a connection to the material on its clients’ websites through a system which it operates in order to provide its clients with . . . services.”<sup>105</sup> In distinguishing *Aimster*, the court stated, “Perfect 10’s reliance on *In re Aimster Litigation* is misplaced because that case dealt with the transmission of material, not the provision of a connection to the material.”<sup>106</sup>

Ultimately, however, courts deny the 512(a) safe harbor to peer-to-peer programs based on the narrow interpretation that peer-to-peer programs do “not operate as a passive conduit within the meaning of subsection 512(a)”<sup>107</sup> because “the transmission [of the file] goes *from* one part of the system *to* another, or *between* parts of the system, but not ‘through’ the system,”<sup>108</sup> as the courts believe the transmission goes through the Internet. Since the technology of both peer-to-peer and IM programs is the same under a 512(a) analysis, this argument could be applied to IM programs as well, even though the court in *Aimster* does not acknowledge this fact.

The material in both peer-to-peer and IM programs is transferred “through a system or network controlled or operated by [the peer-to-peer or IM program].”<sup>109</sup> As stated above, both programs control and operate the connection or network because both programs create the

---

103. 340 F. Supp. 2d 1077.

104. *Id.* at 1082.

105. *Id.* at 1091.

106. *Id.*

107. *A&M Records, Inc.*, 54 U.S.P.Q. (BNA) at 1749.

108. *Id.* at 1751.

109. 17 U.S.C. § 512(a).

network that is used to transfer the material through by providing both users with the necessary IP address and routing information, and only those programs can terminate the network or connection assuming the users are connected to the Internet. The material is then transferred through this connection or network that is established by the programs. If the material is not transferred through this network or connection, then how come a person cannot transfer the material without this connection or network and just through the Internet.

Furthermore, as long as the material transferred between two users on a network created by an online service provider is not modified and complies with the 512(a) conditions, it should be irrelevant whether the material transferred goes “through” the Internet or “through” the network created by a peer-to-peer or IM program because the file is not altered, as it is the identical file either way. Just because a copyrighted music file is transferred through the Internet, and not through the online service provider’s personal private network does not make the transferring of the music file any more or less infringing, as nothing about the copyrighted material is changed or modified. Therefore, unless the copyrighted material is changed or modified, it makes no difference whether the copyrighted material is transferred through the Internet or through the online service provider’s network because the material is the same either way.

A third argument against narrowly interpreting the word “through” can be made when looking at the specific language of 512(a). Looking at the specific language of 512(a), it states that an online service provider is not liable for “providing connections for, material through a system or network controlled or operated by or for the service provider.”<sup>110</sup> This language indicates that the material may be transferred through two types of networks: 1) “a system or network controlled or operated by [the service provider]”;<sup>111</sup> or 2) “a system or network . . . for the service provider.”<sup>112</sup> Therefore, since the Internet is “a system or network . . . for the service provider,”<sup>113</sup> as long as the material is transferred through either a peer-to-peer or IM program’s network or the Internet is immaterial.

A fourth argument against construing the word through can be made when interpreting the legislative history of 512(a). The legislative

---

110. 17 U.S.C. § 512(a).

111. *Id.*

112. *Id.*

113. *Id.*

history indicates that Congress did not intend for the courts to make such a big distinction about whether the material passes through the Internet or an online service provider's own network. Congress enacted 512(a) to apply "to communications functions associated with sending digital communications of others across digital networks, such as the Internet and other on-line networks."<sup>114</sup> This statement suggests that Congress believed the Internet is a digital network. Hence, by the courts making the distinction of whether the material passes through the Internet or an online service provider's network, the courts are making a distinction that Congress did not intend.

Finally, by narrowly interpreting 512(a), courts are hindering the potential growth of the Internet. Taking a more restrictive approach with 512(a) could result "in overdeterrence—excessive monitoring and overzealous censorship by [online service providers],"<sup>115</sup> which forces the online service provider to put more resources towards monitoring and less resources toward innovation and creation. Similarly, smaller online service providers "lack deep pockets [and] will not be able to fight time-consuming and costly courtroom battles, and ultimately they will be forced to wind up their operations."<sup>116</sup> Allowing IM and peer-to-peer programs to qualify for 512(a) creates a quick and inexpensive way for these programs to police copyright infringement, and also serves a societal interest "by making copyrights more valuable and productive."<sup>117</sup>

## VI. CONCLUSION

Perhaps troubled by the DMCA's trespass into the realm of the judicially-made doctrines of contributory and vicarious copyright liability, courts seem to have initiated a "trend toward dismantling the legislative safe harbors."<sup>118</sup> Section 512(a) is an underutilized safe harbor that applies to more than just Internet service providers. Taking

114. H.R. REP. NO. 105-551, pt. 2, at 50.

115. Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 910 (2002) Whereas this article does an economic analysis of holding Internet Service Providers strictly liable, generally these same principles could be applied to entities that also qualify as an online service provider under 17 U.S.C. § 512(k)(1)(A).

116. V.K. Unni, *Internet Service Provider's Liability for Copyright Infringement—How to Clear the Misty Indian Perspective*, 8 RICH. J.L. & TECH. 13 ¶ 10 (Fall 2001), at <http://www.richmond.edu/jolt/v8i2/article1.html>.

117. Alfred Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1887 (2000).

118. Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 55 (2003).

a broader view, as long as an IM or peer-to-peer file sharing program qualifies as an online service provider under 17 U.S.C. § 512(k)(1)(A) and complies with both 17 U.S.C. § 512(i) conditions, the program should qualify for the 512(a) safe harbor because users are required to use the same IM or peer-to-peer software. These programs provide connections for users to transfer material through a digital network, which may be either the program's network or the Internet since the material transferred is the same either way, that is initiated by the user and carried out through an automatic technical process that does not select the recipients of the material, store any copies of the material, or modify the content of the material. By refusing to acknowledge this, courts are defying Congress's intent behind the passage of the 512(a) safe harbor and creating liability for entities that should be immune to copyright infringement.

SVEN ERIC SKILLRUD\*

---

\* Bachelor of Business Administration with Honors 2002, University of Wisconsin-Madison; Juris Doctor candidate 2005, Marquette University Law School. The author would like to thank Professor Eric Goldman of Marquette Law School for his encouragement and support.

