

Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act

by
*Cyrus Sarosh Jan Manekshaw**

I. INTRODUCTION

The Internet has so completely permeated our lives in the past ten years that often we do not fully realize how truly revolutionary this technology is or how many legal issues and problems it can present. At its most basic level, the Internet is a system of worldwide computer networks that transfer data. To the ordinary user, the Internet is an all-purpose essential tool used to do everything from checking e-mail and reading the news to playing games and sharing music, pictures, and ideas. The power to share ideas and communicate with people all around the globe is the Internet's most powerful feature. The Internet enables the transfer of large amounts of information with great speed. This, in turn, allows users to transfer files including pictures, music, and movies in violation of copyright laws. Additionally, the numerous message boards and e-mail accounts allow publication of statements concerning virtually any and every topic.

One of our most cherished liberties in the United States is our freedom of expression, with only a very few, yet extremely necessary limitations imposed on us by the government. With this freedom, however, comes the potential for injustice. Because the Internet allows the exercise of our freedoms to exponentially increase, it facilitates an equally exponential increase in violations of our copyright and defamation laws. Copyright law aims to prevent people from copying others' original works, while defamation law focuses on protecting reputations of individuals. The Internet's capability to transfer large amounts of information with great speed enables users to steal ideas from the works of others by transferring files and using them to their own advantage.

Traditionally, copyright and defamation law have maintained strict liability for violators, including publishers of defamatory or infringing materials. Thus, if a magazine were to publish a copyrighted picture, without the proper authorization, it would be held liable for copyright infringement. Similarly, if a magazine published a defamatory statement, it could also be held liable. It does not take a huge leap of logic to determine that an Internet Service Provider ("ISP"), a company that provides users with access to the

* Mr. Manekshaw received a bachelor's degree from the University of Texas at Austin in December 2002, and he is a candidate for Juris Doctor, class of 2006, at Southern Methodist University Dedman School of Law. He would like to thank the members of the Computer Law Review and Technology Journal for their assistance with editing and his family for their constant support.

Internet, acts as a sort of “publisher” for its users, in much the same way and thus could be held liable for the copyright infringement and defamation of its subscribers.

Nevertheless, Congress has determined that holding ISPs liable for the copyright infringement and defamation of its subscribers is not in the public’s best interests, and thus has created statutes that protect ISPs from liability. In 1998, Congress enacted the Digital Millennium Copyright Act (“DMCA”).¹ The DMCA aimed to balance the rights of copyright holders against end users as well as copyright holders against ISPs.² The language of the DMCA provides both notice and take down provisions that encourage cooperation between copyright owners and ISPs in order to remove infringing material.³ An ISP will expose itself to liability only if it fails to comply with a proper take down notice.⁴ Additionally, Section 512 of the DMCA includes four safe harbor provisions that shield ISPs from liability for performing certain acts that an ISP must regularly perform, such as adopting, implementing and informing its subscribers of its policy against transmitting unauthorized content.⁵ This Congressional protection was meant to allow self-maintenance of the Internet in a less interfering manner.

In 1996, Congress enacted the Communications Decency Act (“CDA”) which gives protection to ISPs for publishing defamatory material. This Act promotes a free exchange of ideas, while also encouraging self-maintenance. Both the CDA and the DMCA responded to a blossoming technology that had the potential for both vast information transfer and unparalleled tortious action in the form of copyright infringement and defamation.

II. HISTORY OF COPYRIGHT

The Constitution of the United States gives Congress the power to “promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.”⁶ There is little incentive to expend one’s time, energy, and money creating an original work if another person is able to swoop in after the initial investment and copy, use, or claim the work as his own. Thus, by giving the original creator certain exclusive rights with respect to his work, the government encourages the development of new works of art and science because the creator knows his efforts will be rewarded and protected.

-
1. S. Rep. No. 105-190, at 2 (1998).
 2. S. Rep. No. 105-190, at 20.
 3. 17 U.S.C. § 512(c)(1)(C), (c)(3) (2002).
 4. *Id.*
 5. *Id.*
 6. U.S. CONST. art. I § 8, cl. 8.

The history of copyright legislation can be divided into three periods, beginning with the first federal Copyright Act in 1790.⁷ The Copyright Act of 1970 consisted of only seven sections and gave protection to authors or their assignees of maps, charts, or books for fourteen years with a renewal term of another fourteen years.⁸ The author had the exclusive right to “print, reprint, publish, or vend” the work upon fulfilling three basic requirements: (1) recording the title in the clerk’s office of the district court where he resided; (2) publishing a copy of the record in the newspaper for four weeks, and (3) giving a copy of the work to the Secretary of State within six months of publication.⁹ The remedy for infringement was forfeiture and destruction of all copies in the infringer’s possession as well as a fifty cents per page fine, with one half going to the author and the other half going to the government.¹⁰ The Act did not prohibit importing, selling, reprinting, or publishing foreign works.¹¹

Between 1790 and 1909, many amendments were added, extending the scope of the Act’s protection. The original term of protection was extended to 28 years in 1831.¹² The Act was broadened throughout the years to offer protection for prints¹³, musical compositions¹⁴, photographs¹⁵, paintings, drawings, chromolithographs, statues, and works of fine art.¹⁶ A notice requirement was added in 1802.¹⁷

The second period of copyright history began with the enactment of the Copyright Act of 1909. The 1909 Act itself included many changes. It applied to “all the writings” of an author.¹⁸ It also added to the exclusive rights of the creator, granting the creator the exclusive right to publicly perform the works and the right to create certain derivative works.¹⁹ The Act also listed

7. Act of May 31, 1790, ch. 15, § 1, 1 Stat. 124, 124 (repealed 1802).

8. *Id.*

9. *Id.*

10. § 2, 1 Stat. at 125.

11. § 5, 1 Stat. at 125.

12. Act of Feb. 3, 1831, ch. 16, § 1, 4 Stat. 436, 436 (amended 1870).

13. Act of Apr. 29, 1802, ch. 36, § 2, 2 Stat. 171, 171 (repealed 1831).

14. Act of Feb. 3, 1831, ch. 16, § 1, 4 Stat. 436, 436 (amended 1870).

15. Act of Mar. 3, 1865, ch. 126, § 1, 13 Stat. 540, 540 (current version at 17 U.S.C. § 102 (2000)).

16. Act of July 8, 1870, ch. 230, § 100, 16 Stat. 198, 214 (codified as amended at 17 U.S.C. § 101 (2000)).

17. Act of Apr. 29, 1802, ch. 36, § 1, 2 Stat. 171, 171 (repealed 1831).

18. Act of Mar. 4, 1909, ch. 320 § 4, 35 Stat. 1075, 1076.

19. § 1(d), 35 Stat. at 1075.

classes of works that could be copyrighted and provided certain differences in remedies based on these classes.²⁰

The third period of copyright law is based on the Copyright Act of 1976. It has significantly extended the scope of protection provided by the more conservative acts of the past.

III. CURRENT COPYRIGHT LAW

The current era of copyright law is based on the Copyright Act of 1976 and the resulting amendments. The current Act covers “original works of authorship fixed in any tangible medium of expression.”²¹ It divides copyrightable works into 8 categories: literary works; musical works; dramatic works; pantomimes and choreographic works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works; sound recordings; and architectural works.²² The Act gives the copyright holder the exclusive right to reproduce the work, to make derivative works, to distribute copies of the work to the public, to perform the work publicly, to display the work publicly, and to perform the work publicly by means of a digital audio transmission.²³ Additionally, the Act provides a mechanism for bringing a cause of action against one who infringes another’s copyright, and provides remedies for the copyright owner including damages and injunctive relief.²⁴

The Act also includes defenses and limits to infringement actions. An extremely important section of the Act limits the exclusive rights of a copyright owner by allowing the “fair use” of a copyrighted work.²⁵ The fair use doctrine states that using or copying a work is not copyright infringement if the use is for criticism, comment, news reporting, teaching, scholarship, or research.²⁶ The Act lists four factors that must be considered when determining if the use is “fair”: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and (4) the effect of the use upon the potential market for or value of the copyrighted work.²⁷

20. § 25(b), 35 Stat. at 1081.

21. 17 U.S.C. § 102(a) (1990).

22. § 102(a).

23. 17 U.S.C. § 106 (2002).

24. 17 U.S.C. §§ 501(b), 502(a), 504(a)-(c) (2002).

25. 17 U.S.C. § 107 (1992).

26. *Id.*

27. *Id.*

The DMCA provides safe harbor provisions to protect ISPs from liability for copyright infringement.²⁸ The first section applies when an ISP is merely a conduit for the transmission of the infringing material; that is, it only transmits, routes, or provides connections for the material.²⁹ The second provision protects an ISP when system caching or providing temporary storage of the material.³⁰ The third provision protects an ISP when it is storing infringing material on its system at the direction of its users.³¹ The fourth provision protects an ISP when it provides links to an online location that contains infringing material.³²

Courts have generally recognized three different types of copyright liability. The first and most obvious type is “direct liability.” To maintain a cause of action for direct liability, a plaintiff must “show ownership of the allegedly infringed material and . . . demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders under 17 U.S.C. § 106.”³³ A second type of liability is “contributory liability.” The general rule is that “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‘contributory’ infringer.”³⁴ Knowledge includes both actual and constructive knowledge, or as one court put it, “that the secondary infringer ‘know or have’ reason to know’ of direct infringement.”³⁵ Finally, the third type of liability states that “a defendant is vicariously liable for copyright infringement if he enjoys a direct financial benefit from another’s infringing activity and ‘has the right and ability to supervise’ the infringing activity.”³⁶

IV. HISTORY OF DEFAMATION

The Restatement Second of Torts lists four prima facie elements for the tort of defamation. These include a false statement concerning another, an unprivileged publication to a third-party, fault amounting at least to negligence on the part of the publisher, and actionability of the statement irrespective of special harm or the existence of special harm caused by the

28. 17 U.S.C. § 512(a)-(d) (1999).

29. § 512(a).

30. § 512(b).

31. § 512(c).

32. § 512(d).

33. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001).

34. *Gershwin Publ’g Corp. v. Columbia Artists Mgmt.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

35. *Napster*, 239 F.3d at 1020.

36. *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citing *Napster*, 239 F.3d at 1022).

publication.³⁷ Defenses to defamation generally take the form of defeating these elements; however, there are also conditional and absolute privileges, such as publishing something required by law or statements made by legislators and jurors in the pursuit of their governmental activities.³⁸ Early on, publishers such as newspapers were held strictly liable for publication of defamatory material even in the absence of knowledge of the defamatory character of the material.³⁹ Radio stations were held to be analogous to newspaper publishers and were similarly held strictly liable for publication of defamatory statements.⁴⁰ The Supreme Court, however, held in 1976 that an individual cannot recover against a publisher without a finding of fault on the part of the publisher.⁴¹ This demise of strict liability for publishers paved the way for the immunity given to ISPs by the CDA.⁴²

V. THE COMMUNICATIONS DECENCY ACT

The CDA was enacted in 1996.⁴³ The Act begins with the Congressional findings and a statement of the policy behind the Act.⁴⁴ The third section is the focal point of the Act, as it offers the immunities from liability.⁴⁵

- (c) Protection for “good samaritan” blocking and screening of offensive material
 - (1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
 - (2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of—
 - (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

37. RESTATEMENT (SECOND) OF TORTS § 558 (1977).

38. RESTATEMENT (SECOND) OF TORTS §§ 583, 612 (1977).

39. *Peck v. Tribune Co.*, 214 U.S. 185, 189-90 (1909).

40. *Sorensen v. Wood*, 243 N.W. 82, 86 (Neb. 1932).

41. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 352 (1974).

42. 47 U.S.C. § 230 (1998).

43. *Doe v. AOL, Inc.*, 783 So. 2d 1010, 1014 (Fla. 2001).

44. 47 U.S.C. § 230.

45. § 230(c).

-
- (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).⁴⁶

Virtually every ISP defendant that has used section 230 to immunize itself from liability from defamation claims has been successful.⁴⁷

Because the CDA is federal law and defamation claims are governed by state law, the topic of preemption must also be addressed. The CDA in section 230(e)(3) states that no state law cause of action may be brought that is inconsistent with section 230.⁴⁸ The Supreme Court of Florida expressly addressed the question of preemption and found that section 230 does, in fact, preempt state law causes of action.⁴⁹

A. Pre-CDA Case Law

The publisher/distributor distinction was used in determining liability of ISPs even before the CDA was enacted into law. In *Cubby, Inc. v. CompuServe*, the plaintiffs ran a computer database that published news and gossip.⁵⁰ The plaintiffs sued a rival online newsletter as well as its ISP, CompuServe, for defamatory statements published on the newsletter's website.⁵¹ CompuServe had no opportunity to review the contents of the newsletter.⁵² CompuServe argued that it was not liable for the defamatory statements because it was a distributor rather than a publisher and had no knowledge of the statements.⁵³ The Southern District of New York came to its decision in this new, uncertain area of the law by analogizing to older, similar, resolved situations. The court explained that "news vendors, book stores, and libraries. . . are not liable if they neither know nor have reason to know of the defamation."⁵⁴ The court cited basic First Amendment case law that described the potentially chilling effect of holding traditional print media booksellers liable for carrying obscene books without knowledge of their

46. § 230(c)(1)-(2).

47. See *Ben Ezra, Weinstein, and Co. v. AOL*, 206 F.3d 980, 986 (10th Cir. 2000); *Zeran v. AOL*, 129 F.3d 327, 335 (4th Cir. 1997); *Barrett v. Fonorow*, 799 N.E.2d 916, 924 (Ill. App. Ct. 2003); *Schneider v. Amazon.com*, 31 F.3d 37, 43 (Wash. Ct. App. 2001).

48. 47 U.S.C. § 230(e)(3).

49. *Doe v. AOL, Inc.*, 783 So. 2d 1010, 1013 (Fla. 2001).

50. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135, 138 (S.D.N.Y. 1991).

51. *Id.*

52. *Id.* at 137.

53. *Id.* at 138.

54. *Id.* at 139 (quoting *Lerman v. Chuckleberry Publ'g, Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981)).

obscenity.⁵⁵ Compuserve's control over editorial content was especially low in this case because the defamatory statements were published by a company whose only relation to Compuserve was through its contract to post the forum on the Internet.⁵⁶ The district court concluded that "[a] computerized database is the functional equivalent of a more traditional news vendor" and applying a higher standard of liability to an online distributor "would impose an undue burden on the free flow of information."⁵⁷ This conclusion is important because it demonstrates the commitment of the courts to keep the First Amendment alive and thriving in cyberspace. The courts have generally done a good job of handling cases of first impression that deal with the Internet by analogizing them to their traditional media counterparts. However, after only a short passage of time, the Internet has grown so enormously that it requires special treatment under the law.

B. Policy of CDA

Many courts have expounded on the purposes behind the Act, which are clearly indicated in the findings and policy stated directly in the Act itself. "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium."⁵⁸ Congress believed that imposing liability on ISPs would encourage more restrictions on free speech.⁵⁹ For example, the Fourth Circuit recognized that section 230 was created in order to encourage and sustain the immense growth of the Internet, rather than stifle it.⁶⁰ The court further emphasized that Congress enacted section 230 to restrict governmental interference by allowing the Internet community to police itself.⁶¹ The Congressional findings in section 230(a) state that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and a myriad of avenues for intellectual activity."⁶² The Fourth Circuit's analysis offers a frightening outlook on the chilling of free speech that may result if ISPs are not granted immunity from liability.⁶³ ISPs would not be able to monitor the extremely large amounts of information capable of being transferred over the Internet, and thus, in order to avoid liability, they would be forced to limit the amount and content of the

55. *Id.* at 139-140.

56. *Id.* at 140.

57. *Id.*

58. *Zeran v. AOL, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

59. *Id.*

60. *Id.*

61. *Id.*

62. 47 U.S.C. § 230(a)(3) (1998).

63. *Zeran*, 129 F.3d at 331.

messages.⁶⁴ An important thing to keep in mind while understanding ISP immunity from liability under CDA is that the original party who created the defamatory material does not also escape liability; the immunity only extends to the ISP.⁶⁵

There are both positive and negative consequences of extending immunity to the ISP but not to the individual party who created the defamatory material. On the one hand, plaintiffs will be disappointed that they will be forced to sue individuals who will often have substantially less money than the giant ISPs. Additionally, it is more difficult for plaintiffs to search out each individual defendant responsible for defamatory material as opposed to just suing the company most ostensibly responsible for the material on its site. Especially in this day of screen names, usernames, and anonymous e-mail addresses, it seems much easier to sue the large ISP rather than wasting time tracking down someone who could easily be on the other side of the world. The problem with this concept is that it allows the responsible parties to escape liability. Alternatively, imposing liability on these parties may not only chill free speech, it may also stifle technological progress on the Internet.

According to the Fourth Circuit in *Zeran v. AOL*, “Congress clearly enacted section 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.”⁶⁶ In *Zeran*, the court was responding to a New York case, *Stratton Oakmont v. Prodigy Services*.⁶⁷ In *Stratton*, a New York court held that because Prodigy was editing and blocking content, it was acting as a “publisher” rather than as a “distributor” and would be subject to strict liability, historically found in defamation law.⁶⁸ The *Stratton* holding, however, contravenes the legislative intent behind section 230. The legislature’s intent to encourage self-regulation by ISPs is evidenced by one of the stated policies of section 230: “to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material.”⁶⁹ Thus, “Congress clearly enacted section 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.”⁷⁰

64. *Id.*

65. *Noah v. AOL Time Warner Inc.*, 261 F. Supp. 2d 532, 538 (E.D. Va. 2003).

66. *Ben Ezra, Weinstein, and Co. v. AOL.*, 206 F.3d 980, 986 (10th Cir. 2000).

67. *Zeran*, 129 F.3d at 331 (responding to *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)).

68. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995).

69. 47 U.S.C. § 230(b)(4).

70. *Ben Ezra, Weinstein, and Co.*, 206 F.3d at 986.

C. The Publisher/Distributor Distinction

One of the first major problems in interpreting section 230 is understanding the publisher/distributor distinction. For traditional media, publishers are liable under a strict liability scheme, so that knowledge of the defamatory statement is not a prerequisite to holding the publisher liable.⁷¹ Distributors, on the other hand, cannot be held liable absent proof of knowledge of the defamatory material.⁷² In *Zeran v. AOL*, an individual brought a negligence action against AOL for the delay in removing defamatory statements concerning him.⁷³ An anonymous AOL user posted messages on a bulletin board advertising t-shirts with offensive statements concerning the Oklahoma City bombing and also gave the plaintiff's home telephone number.⁷⁴ The circuit court determined that section 230 was specifically meant to immunize ISPs acting not only as distributors but also as publishers with the power to edit the content of the material.⁷⁵

In another case, *Noah v. AOL*, a crafty plaintiff attempted to argue that AOL was the owner of a place of accommodation rather than a publisher.⁷⁶ The district court easily saw through this argument and explained that the plaintiff was attempting to place AOL in a publisher's role for the various anti-Islamic statements in an AOL chatroom.⁷⁷ The court concluded that this was precisely what section 230 was designed to prevent.⁷⁸

In *Barrett v. Fonorow*, a doctor brought a defamation claim against the president of a company that ran a website containing several posted articles claiming that the doctor was a liar.⁷⁹ The doctor attempted to interpret section 230(c)(1) as only limiting publisher liability, not distributor liability.⁸⁰ Thus the doctor argued that although the company's website, acting as a publisher was immune from liability, traditional notions of distributor liability (such as liability for a distributor who knew or had reason to know of the defamatory character of the material) should still apply.⁸¹ Following this train of logic, the doctor argued that the website owner was a distributor rather than a publisher because he had no editorial power over the content of

71. *Zeran*, 129 F.3d at 331.

72. *Id.*

73. *Id.* at 328.

74. *Id.* at 329.

75. *Id.* at 332-33.

76. *Noah v. AOL Time Warner Inc.*, 261 F. Supp. 2d 532, 538 (E.D. Va. 2003).

77. *Id.*

78. *Id.*

79. *Barrett v. Fonorow*, 799 N.E.2d 916, 919-20 (Ill. App. Ct. 2003).

80. *Id.* at 924.

81. *Id.*

the material.⁸² The Illinois court rejected this argument, stating that “Congress intended section 230 to prevent the element of ‘publication’ from being satisfied in a state tort cause of action” when a computer service provides information from another.⁸³ The court explained that “Congress partially precluded liability for defamation under both the strict liability standard applicable to ‘publishers’ and the fault-based standard applicable to ‘distributors.’”⁸⁴ The court’s interpretation of the CDA as removing the publisher/distributor distinction is vital to the Internet’s survival and growth for a limited period of time. Nevertheless, once the Internet has solidified itself as a widespread, traditional form of media, the distinction should be reintroduced. As companies consolidate and merge with one another, ISPs are becoming part of huge media conglomerations that act as publishers of material with editorial rights and responsibilities. We are no longer living in a time when AOL is simply a way to connect to the Internet. It now has the ability to channel unfathomable amounts of information to millions of people and should be held correspondingly responsible for the use or abuse of that immense power.

D. Interactive Computer Service and Information Content Provider

Another key step in understanding the CDA is trying to understand to whom it grants immunity. A heavily litigated topic is the difference between an “interactive computer service” and an “information content provider.”⁸⁵ The definitions section of the statute states:

(2) Interactive computer service

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term “information content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.⁸⁶

82. *Id.*

83. *Id.*

84. *Id.*

85. *See, e.g.,* Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003); Ben Ezra, Weinstein, and Co. v. AOL, 206 F.3d 980, 983 (10th Cir. 2000); Barrett v. Fonorow, 799 N.E.2d 916, 920 (Ill. App. Ct. 2003).

86. 47 U.S.C. § 230(f)(2)-(3).

In order for an ISP to qualify for immunity from liability under section 230(c)(1), it must first be determined to be an interactive computer service.⁸⁷ In *Ben Ezra, Weinstein, and Company v. AOL*, the plaintiff was a computer software company that sought to hold AOL liable for defamation as a result of AOL providing an incorrect stock quote for the computer software company.⁸⁸ The plaintiff agreed that AOL was an interactive computer service as defined by section 230(f)(2), but argued that AOL was also an information content provider under section 230(f)(3) because the company worked closely with the third-party companies that provided it with the stock information.⁸⁹ The Tenth Circuit ruled that AOL did not work so closely as to render it an information content provider.⁹⁰ The court found that AOL's practice of informing the third-party stock information providers of errors in the information did not "constitute the development or creation of the stock quote information."⁹¹ The plaintiff then argued that AOL's practice of deleting incorrect information met the definition of information content provider.⁹² The court also rejected this argument by stating that deleting information was obviously not the same as creating or developing it.⁹³ While this is true, deleting certain information can give the remaining information a different meaning. Courts should focus more on the ability to control the content of the material as a whole rather than focusing exclusively on the ability to create or develop it. This change would provide clarity to the definition of an information content provider under section 230, and the statutes' goals would be more consistent with the provisions of the DMCA concerning ability to control infringing materials.

Courts have held that the term "Interactive Computer Service" be interpreted broadly to extend protection from liability to many companies.⁹⁴ For example, in *Batzel v. Smith*, the court stated that "'development of information' mean[t] something more substantial than merely editing portions of an e-mail and selecting material for publication."⁹⁵ In *Barrett v. Fonorow*, the plaintiff attempted to defeat the defendant's use of section 230 by arguing that the defendant website was not an interactive computer service because

87. § 230(c)(1).

88. *Ben Ezra, Weinstein, and Co.*, 206 F.3d at 983.

89. *Id.* at 985.

90. *Id.*

91. *Id.*

92. *Id.* at 985-86.

93. *Id.* at 986.

94. See, e.g., *Batzel v. Smith*, 333 F.3d 1018, 1031 (9th Cir. 2003); *Barrett v. Fonorow*, 799 N.E.2d 916, 922 (Ill. App. Ct. 2003); *Schneider v. Amazon.com*, 31 P.3d 37, 40 (Wash. Ct. App. 2001).

95. *Batzel*, 333 F.3d at 1031.

“it is not in the business of providing access to the Internet.”⁹⁶ The *Barrett* court found this argument to be plainly contrary to the language of section 230.⁹⁷ The way in which the term “interactive computer service” is defined clearly shows that it is not limited to services that provide access to the Internet.⁹⁸ “The definition includes, but is not limited to, Internet providers.”⁹⁹ Thus, a defendant is not barred from invoking the immunity provided under section 230 because he does not actually provide Internet access.

Similarly, in *Batzel v. Smith*, the Ninth Circuit reversed the district court’s conclusion that section 230 only applies to services that provide Internet access as a whole.¹⁰⁰ In the *Batzel* case, an attorney sued the operator of a website that posted information concerning stolen art.¹⁰¹ The website operator had received an e-mail tip concerning some stolen paintings the attorney may have had.¹⁰² The circuit court focused on the use of the words “‘any’ information services” in section 230(f)(2).¹⁰³ The court also explained that the use of the word “including” before “provid[ing] access to the Internet” meant that ISPs are only a subset of the group that is immune from liability under section 230.¹⁰⁴

In *Schneider v. Amazon.com*, a Washington court found that Amazon was an interactive computer service under section 230(f)(2) because its website allowed visitors “to comment about authors and their work, thus providing an information service that necessarily enables access by multiple users to a server.”¹⁰⁵ In *Gentry v. Ebay*, a California court stated in a footnote that, according to the definition, Ebay was an “interactive computer service” because the site allowed “users to conduct sales transactions, as well as provide information (feedback) about other users of the service.”¹⁰⁶ As in *Schneider*, the *Gentry* court held that this service enabled access by multiple users to a server.¹⁰⁷

96. *Barrett*, 799 N.E.2d at 922.

97. *Id.*

98. *See* 47 U.S.C. § 230(f)(2); *Barrett*, 799 N.E.2d at 922.

99. *Barrett*, 799 N.E.2d at 922.

100. *Batzel*, 333 F.3d at 1030.

101. *Id.* at 1021-22.

102. *Id.* at 1021.

103. *Id.*

104. *Id.*

105. *Schneider v. Amazon.com*, 31 P.3d 37, 40 (Wash. Ct. App. 2001).

106. *Gentry v. Ebay*, 121 Cal. Rptr. 2d 703, 715 (Cal. Ct. App. 2002).

107. *Id.*

E. No Immunity

In *MCW v. Badbusinessbureau.com*, a job and career counseling company sued a website operator for business disparagement after the defendant's website posted consumer complaints and other statements concerning the plaintiff.¹⁰⁸ The Northern District of Texas held that the CDA did not provide immunity for an interactive computer service that also functioned as the provider of the material that was at issue in the case.¹⁰⁹ The court explained that section 230 would not shield a defendant from liability if it participated in the creation of the material and had thus acted as an information content provider for the specific material.¹¹⁰ The court in *MCW* held that one of the individual defendants could not avail himself of section 230 immunity from liability because he did not fit the definition of an interactive computer service.¹¹¹ This particular defendant failed to offer proof of whether he was a provider or user of an interactive computer service and argued that he neither owned nor operated the websites at issue.¹¹² Furthermore, the fact that defendants created disparaging titles and headings for the otherwise disparaging content of others' posts made them creators and developers of the material, thus barring them from using section 230 to escape liability.¹¹³ This decision is more in line with traditional publisher/distributor notions of liability, and it makes sense to hold a defendant liable for its defamatory actions.

VI. THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. Policy of DMCA

The Digital Millennium Copyright Act was created in 1998 with two crucial and sometimes conflicting goals: "promoting the continued growth and development of electronic commerce and protecting intellectual property rights."¹¹⁴ The DMCA provides "immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider."¹¹⁵

The DMCA does not just give blanket immunity to any Internet Service Provider.¹¹⁶ The immunity only extends to "'innocent' service providers

108. *MCW, Inc. v. Badbusinessbureau.com*, No. Civ.A.3:02-CV-2727-G, 2004 WL 833595, at *1-2 (N.D. Tex. Apr. 19, 2004).

109. *Id.* at *7.

110. *Id.* at *8.

111. *Id.* at *9.

112. *Id.*

113. *Id.* at *10.

114. H.R. Rep. No. 105-551, pt. 1, at 23 (1998).

115. *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004).

116. *Id.*

who can prove they do not have actual or constructive knowledge of the infringement.”¹¹⁷ An ISP loses its “safe harbor protection” when it has knowledge of the infringement.¹¹⁸ Additionally, an interesting aspect of the safe harbor provisions is the idea that they “do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability.”¹¹⁹ Instead, the safe harbor provisions act only to limit the relief available against service providers.¹²⁰

Another interesting thing to keep in mind about the DMCA’s safe harbor provisions is that the statute is not exclusive and does not replace all previous copyright common law.¹²¹ In interpreting the Congressional intent behind the DMCA, courts have expressed the idea that the DMCA is a “floor of protection for ISPs” rather than a ceiling.¹²² At the time of the DMCA’s enactment, Congress realized that the Internet was still developing and growing, and the law was doing so with it.¹²³ Rather than enacting a static statute, Congress believed allowing the courts to continue to interpret the DMCA in light of the previous cases to determine ISP copyright liability would result in a better system.¹²⁴

B. Pre-DMCA Case Law

In *Playboy v. Frena*, the defendant ran a computer bulletin board service that distributed pictures copyrighted by Playboy.¹²⁵ The district court found the defendant liable for copyright infringement based on the fact that Playboy owned the copyright to the images being distributed.¹²⁶ While there was no dispute that Playboy owned the copyright, in order to determine if the defendant copied the images, the court considered several factors, including: (1) whether the defendant had access to the images; (2) whether the copyrighted images were substantially similar to the images on defendant’s bulletin board; and (3) whether “one of the rights statutorily guaranteed to copyright owners [was] implicated by [defendant’s] actions.”¹²⁷ The first two components were not disputed, and the court held that by posting the images on the

117. *Id.*

118. *Id.*

119. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002).

120. *Id.*

121. *Costar Group, Inc. v. Loopnet, Inc.*, 373 F.3d 544, 552 (4th Cir. 2004).

122. *Id.* at 553.

123. *See id.*

124. *Id.*

125. *Playboy v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993).

126. *Id.* at 1556, 1559.

127. *Id.* at 1556.

bulletin board, the defendant publicly distributed and displayed the images in violation of Playboy's copyright protection rights.¹²⁸ After discounting defendant's fair use defense, the court found the defendant liable, despite his claimed lack of knowledge of the infringement, because "[i]ntent or knowledge is not an element of infringement."¹²⁹ The defendant also argued that his infringement was *de minimis*, and should not be held liable; however, the district court disagreed, holding that the widespread potential of the Internet made the infringement dangerous to Playboy.¹³⁰

The *Playboy* court's recognition that a few infringing pictures on one site should not be ignored was extremely important. The precedent that would have been set, had the court agreed that the injury was insubstantial, would have been a dangerous one. The advantages and rights given to a copyright holder depend on the ability to control the material, and restrict its use and distribution by others without authorization or licensing. The speed and expanse of the Internet allows material posted in one place to be accessed in millions of other places virtually immediately. The longer the material remains accessible, the more likely it is to be saved, stored, and redistributed on more and more computers. The incentive for spending time and energy creating or distributing material is drastically decreased when there is no recourse for the illegal dissemination of the material worldwide.

In *Religious Technology Center v. Netcom On-Line Communication Services*, the copyright holders of works of the Church of Scientology sued a former minister and his ISP for posting part of those works on an online bulletin board.¹³¹ A California district court found that the copyrighted material was copied onto the ISP's system, but also recognized that these copies were not made as a result of any affirmative action on the part of the ISP, and that the system "automatically and uniformly create[d] temporary copies of all data sent through it."¹³² The court analogized this situation by explaining that it would not hold the owner of a copying machine directly liable for infringing use by public users.¹³³ The district court expressed the belief that contributory infringement would be a more appropriate remedy than direct infringement because it could focus on the relationship between the ISP and the user/infringer.¹³⁴ If the ISP had been found liable, it would be logical to extend that liability to many other servers around the world that had nothing

128. *Id.* at 1556-57.

129. *Id.* at 1559.

130. *Id.* at 1558-59.

131. *Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995).

132. *Id.* at 1369.

133. *Id.*

134. *Id.*

to do with the infringing material, other than unknowingly transmitting it.¹³⁵ The district court distinguished *Playboy v. Frena* by holding that the defendant in this case was not distributing or displaying the material, but rather was storing and retransmitting it.¹³⁶ This holding makes sense, because the Internet is a vast web of interconnected computers, each of which requires the others to transmit information. Servers routinely transmit data without any active participation other than being part of a network. To hold every server and service provider liable would be ludicrous and would surely have halted the creation and development of the Internet.

C. Threshold Requirement - Definition of ISP

Before an ISP can avail itself of the DMCA's safe harbor provisions, it must first prove that it is in fact a service provider as defined in 17 U.S.C. § 512(k)(1). Two different definitions exist, depending on whether an ISP is attempting to use the conduit safe harbor provision (§ 512(a)) or one of the other three (§ 512(b), (c), or (d)).¹³⁷

(k) Definitions.—

- (1) Service provider.—(A) As used in subsection (a), the term “service provider” means 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.
- (B) As used in this section, other than subsection (a), the term “service provider” means a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A).¹³⁸

Courts have determined that section 512(k)(1)(B) is a broad definition that allows many different types of services to be included within the safe harbor definition of service provider.¹³⁹ In *Corbis v. Amazon*, a Washington district court determined that Amazon met the definition in section 512(k)(1)(B) because it “operate[d] web sites, provide[d] retail and third-party selling services to Internet users, and maintain[ed] computers to govern access to its web sites.”¹⁴⁰ In *Perfect 10 v. Cybernet*, the plaintiffs argued that

135. *Id.*

136. *Id.* at 1370.

137. 17 U.S.C. § 512(k)(1).

138. § 512(k)(1).

139. *Corbis Corp. v. Amazon.com*, 351 F. Supp. 2d 1090, 1100 (W.D. Wash. 2004).

140. *Id.*

the definition of service provider was not meant to include services that take an interest in the content of the material.¹⁴¹ The California district court disagreed with this statement, reasoning that the inclusion of section 512(d), the safe harbor provision for ISPs that provide links, demonstrates that the definition of service provider includes services that manage the content of material.¹⁴² In interpreting section 512(k)(1)(A), the Ninth Circuit held that AOL fit the definition as a matter of law because it did not keep the information on its network for more time than was reasonably necessary.¹⁴³ There was no dispute between the parties as to whether Ebay was a service provider in *Hendrickson v. Ebay*.¹⁴⁴ The Central District of California glossed over the issue, holding that Ebay was clearly within the broad definition.¹⁴⁵ The Seventh Circuit ruled in *In re Aimster Copyright Litigation* that although Congress was not thinking about Napster-like file-sharing services when it enacted section 512, Aimster and other similar services easily fit into the broad definition.¹⁴⁶

D. Threshold Requirement – Reasonable Termination Policy

Once a service provider has met the definition of section 512(k)(1), it must still meet the conditions for eligibility of section 512(i). This threshold and the accompanying analysis is a more difficult hurdle to cross than the initial definition:

- (1) Accommodation of technology.—The limitations on liability established by this section shall apply to a service provider only if the service provider—
 - (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers . . .¹⁴⁷

The legislative history of section 512(i) suggests that Congress did not intend to suggest that “a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is

141. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1175 (C.D. Cal. 2002).

142. *Id.*

143. *Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004).

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

145. *Id.*

146. *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003).

147. 17 U.S.C. § 512(i).

not infringing.”¹⁴⁸ Congress did, however, intend to require negative consequences for repeat infringers.¹⁴⁹ It seems that Congress was very concerned about not requiring too much from ISPs in the initial stages of development of the Internet. Now that the Internet has grown beyond these initial stages it might seem like a good idea to require some monitoring or investigation by ISPs into possible infringements.

Some would argue that requiring ISPs to monitor or investigate possible infringements may bring with it the ever present possibility of a chilling effect on free speech. If an ISP set up a system that searched for possibly infringing material, it would eventually determine that certain categories of material were more likely to contain infringing material and, based on the potential expense of liability, would decide not to carry those specific categories. For example, if an ISP were required to monitor MP3 sound files that it posted for copyright infringement, it would eventually determine that certain types of music, such as rap, are more likely to contain samples, or snippets of one recording used in another new recording. An ISP would realize that every sample used is not necessarily cleared by the original artist and could consequently refuse to post rap songs on its sites.

The section 512(i) requirements are generally divided into three separate parts: adopting a policy, reasonably implementing the policy, and informing subscribers of that policy.¹⁵⁰ In *Ellison v. Robertson*, the Ninth Circuit decided that there was a triable issue of material fact with respect to whether AOL had reasonably implemented a policy because it changed the e-mail address that infringement notices were to be sent to without forwarding old e-mail messages to the new account and without alerting users that the old address was inactive.¹⁵¹

The issue of a reasonably implemented policy was disputed in *Perfect 10 v. CCBill*.¹⁵² Perfect 10, an adult magazine publisher, sued IBill, a company that processes payments for online merchants, for copyright infringement when IBill’s clients had posted copyrighted material owned by Perfect 10 on their own sites.¹⁵³ IBill described its policy: after receiving a notice of copyright infringement, it suspended services to the client, and if it determined that it had received previous complaints, it terminated services.¹⁵⁴ Perfect 10 argued that the policy was not reasonably implemented because it did not suspend all repeat infringers.¹⁵⁵ A California district court held that

148. H.R. Rep. No. 105-551, pt. 2, at 61 (1998).

149. *Id.*

150. *Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004).

151. *Id.*

152. *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004).

153. *Id.* at 1085.

154. *Id.* at 1088.

155. *Id.*

section 512(i) was enacted to force ISPs to terminate infringing users rather than just delete infringing content.¹⁵⁶ After examining the actual wording of IBill's policy and finding that it met the requirement of "adopting a policy," the court examined whether IBill had actually reasonably implemented this policy.¹⁵⁷ The district court held that single instances of IBill failing to terminate services could not be used to disprove compliance with the threshold requirements of section 512(i) because the statute required "reasonable" implementation rather than "perfect" implementation.¹⁵⁸ Also, because the reasonable implementation of a policy can turn on the sufficiency of the notice given to a defendant by plaintiff, courts must determine whether such notice was properly given under section 512(b), (c), or (d).¹⁵⁹ Another defendant in the *Perfect 10 v. CCBill* case was Internet Key, an age verification system for websites.¹⁶⁰ Perfect 10 argued that Internet Key's policy did not meet the requirement of adopting a policy which provides for termination of services of repeat infringers because the policy that they did adopt allowed repeat infringers to maintain services as long as they did not receive complaints about three different websites owned by the same webmaster.¹⁶¹ However, the California district court disagreed with plaintiff's reading of Internet Key's policy and held that the policy's statement that a website would be terminated after only one notice of infringement met the requirement of adopting a policy that terminated services of repeat infringers.¹⁶² Again, the reasonable implementation analysis concerning Internet Key was tied into the notice provisions of section 512. Perfect 10 also sued CWIE, an Internet access provider, and CCBill, a company that provided payment services to websites.¹⁶³ The *CCBill* court held that defendants' omission of the names of a few webmasters on a spreadsheet listing notifications of infringement did not mean that they did not reasonably implement a policy.¹⁶⁴

In *Perfect 10 v. Cybernet*, a California district court held that section 512(i) created "substantive responsibilities for service providers."¹⁶⁵ The district court was careful not to create too great a level of responsibility by holding: (1) the knowledge standard under section 512(i) was not as high as

156. *Perfect 10 v. CCBill*, 340 F. Supp. 2d at 1088.

157. *Id.* at 1089.

158. *Id.*

159. *Id.* (holding that the "information reasonably sufficient to permit the service provider to locate the material" term was not met in this case).

160. *Id.* at 1085.

161. *Id.* at 1093.

162. *Id.* at 1094.

163. *Id.* at 1085.

164. *Id.* at 1100.

165. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1176 (C.D. Cal. 2002).

that of section 512(c); (2) service providers are not required to terminate service for first time infringers; (3) service providers are not required to “address difficult infringement issues;” and (4) service providers are not required to monitor their services for violation of copyright law.¹⁶⁶ The *Cybernet* court interpreted section 512(i) as allowing for service provider policing policies that were less formal and strict than the notice provisions found in section 512(b), (c), and (d), but which still had some force as a result of the “reasonable” requirement.¹⁶⁷ Although the defendant argued that it removed infringing links from its search engine, it did not take on the responsibility of terminating service completely, and thus the court held that it did not meet the threshold requirements of section 512(i).¹⁶⁸

In *In re Aimster Copyright Litigation*, instead of searching for a policy, the Seventh Circuit summarily found that rather than preventing repeat infringement, Aimster encouraged it by teaching infringers how to encrypt infringing material so that Aimster would not be able to prevent it.¹⁶⁹ In *Corbis v. Amazon*, the plaintiff attempted to defeat Amazon’s safe harbor defense by arguing that Amazon had not adopted a reasonable policy and informed its users of the policy.¹⁷⁰ Corbis argued that the policy was too vague because it did not explain the process of terminating repeat infringers and thus did not fully inform the users about the policy.¹⁷¹ The Washington district court compared section 512(i) and its lack of definitions with the formality of the notice provisions and held that Congress intended to maintain only loose obligations for service providers.¹⁷² By allowing fluidity and flexibility in the process, Congress allows the courts and ISPs themselves to determine new issues and solve new problems as the technology develops.¹⁷³ The *Corbis* court held that Amazon’s policy met the threshold requirements because it informed users that infringing materials would result in penalties including termination of service.¹⁷⁴ The district court concluded that just because Amazon’s policy did not specifically include the term “repeat infringer” did not mean that it did not comply with section 512(i)’s

166. *Id.*

167. *Id.* at 1178.

168. *Id.*

169. *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003).

170. *Corbis Corp. v. Amazon.com*, 351 F. Supp. 2d 1090, 1100 (W.D. Wash. 2004).

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.*

requirements.¹⁷⁵ The fact that Amazon explained that repeated violations could result in a permanent ban from Amazon's services was sufficient.¹⁷⁶

Although flexibility is important in Internet law, many of the courts' loose interpretations of the reasonable termination policy requirements have allowed ISPs to pay lip service to being tough on copyright infringement. Obviously, the ISP with the most lax termination policy will attract a great deal of customers interested in violating copyright infringement laws. By keeping the termination policy requirements loose, the courts allow ISPs to exploit this flexibility. ISPs may implement termination policies to placate copyright holders, but, in an effort to retain customers, may fail to strictly enforce those policies. Not only is this unfair to copyright holders, it also creates uncertainty in the law that is unfair to customers. The uncertainty of the termination policies puts customers in the position of not being able to predict what they can and cannot get away with without being terminated from their ISP.

E. Notice and Takedown Provisions

A crucial component of the safe harbor provisions of the DMCA is the "notice and takedown process." Rather than absolutely protecting ISPs from all copyright liability, Congress created a duty for ISPs to remove infringing material upon receiving notice. Upon receiving notice, an ISP that removes the material will be immune from liability. A failure to remove the material, however, will result in liability for the ISP. This procedure eliminates an implicit duty for ISPs to constantly monitor their customers, and it shifts the burden to the copyright holders to initiate the process. The notice and takedown process applies to three of the four safe harbor provisions. The specific process for notification of infringing material by a copyright holder is found in section 512(c)(3).¹⁷⁷

(3) Elements of notification.—

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

175. *Id.*

176. *Id.*

177. 17 U.S.C. § 512(c)(3) (2005).

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.¹⁷⁸

Three of the safe harbor provisions—system caching, direction of user, and linking—directly reference the notice and takedown provisions of section 512(c)(3). All three notice and takedown provisions contain language that protects an ISP who “responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.”¹⁷⁹ Obviously, section 512(a) does not have a notice and takedown provision because it involves ISPs that merely act as conduits, and thus, the ISP would have no control or ability to remove or disable access to the infringing material.¹⁸⁰

1. Notice

Litigation regarding the notice provision occurs frequently because “the service provider’s duty to act is triggered only upon receipt of proper notice.”¹⁸¹ In *Hendrickson v. Ebay*, the plaintiff sent a letter informing Ebay of the fact that there were copyright infringing DVD copies of a specific movie offered for sale on their site.¹⁸² The letter did not tell Ebay which of the copies infringed plaintiff’s copyright, nor did it explain the copyright interests or rights of the plaintiff.¹⁸³ The plaintiff argued that because Ebay had actual or constructive knowledge of the infringing material, he need not strictly comply with the requirements of section 512(c)(3).¹⁸⁴ The Central District of California disagreed with this argument, citing section 512(c)(3)(B)(i), which states that notifications that do not comply substantially with section 512(c)(3) will not be used as evidence of actual or constructive knowledge of infringement.¹⁸⁵ The district court also found that the

178. *Id.*

179. 17 U.S.C. §§ 512(c)(1)(C), (d)(3); *see also*, 17 U.S.C. § 512(b)(2)(E).

180. *In re Charter Communications, Inc.*, Subpoena Enforcement Matter, 393 F.3d 771, 776 (8th Cir. 2005).

181. *Hendrickson v. Ebay, Inc.*, 165 F. Supp. 2d 1082, 1089 (C.D. Cal. 2001).

182. *Id.* at 1084.

183. *Id.*

184. *Id.* at 1089.

185. *Id.*

letter sent by plaintiffs did not substantially comply with section 512(c)(3) because it lacked the “key elements” of a notice statement.¹⁸⁶ In response to plaintiff’s argument that he should not be required to identify the specific infringing copies of the movies, the court held that in a case such as this where not all copies listed on Ebay were infringing, Ebay needed additional information to determine which copies should be removed.¹⁸⁷ The *Hendrickson* court also held that more was required than merely offering Ebay the user IDs of individuals who were selling infringing copies of the movie. Instead, the specific item numbers of the listings were required.¹⁸⁸ Without proper notice, Ebay had no duty to act under the third prong of the safe harbor test.¹⁸⁹

The requirement for specificity rightly places the burden on the copyright holder. If a copyright holder could merely inform an ISP that it published infringing material on its site, ISPs would spend inordinate amounts of time and money patrolling and searching for the infringing material. The result would be a chilling effect with ISPs predetermining what kind of material was safe and unlikely to contain infringing material. The ISPs would then only allow that kind of material on its sites.

In *Perfect 10 v. Cybernet*, a California district court disapproved of the ISPs using alternative notice requirements, which conflicted with section 512(c)(3).¹⁹⁰ An example of a difference disapproved of by the court was Cybernet’s refusal to accept a representative list of multiple copyrighted works on a single website despite its explicit allowance by section 512(c)(3)(A).¹⁹¹ The district court asserted that this seemingly insignificant difference has the effect of placing the majority of the burden on the copyright holder rather than splitting it evenly between the copyright holder and the ISP.¹⁹² The use of a representative list was a wise inclusion in section 512(c)(3). This small provision helps maintain the ever important balance between the rights and responsibilities of ISPs and copyright holders. Although the burden falls on the copyright holder to inform ISPs of infringing material, the copyright holder need not separately identify every copyrighted work if multiple infringements exist on a single site. The use of the representative list eases the copyright holder’s burden with no substantial harm to ISPs.

186. *Id.*

187. *Id.* at 1090.

188. *Id.* at 1091-92.

189. *Id.* at 1092.

190. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1179-80 (C.D. Cal. 2002).

191. *Id.* at 1180.

192. *Id.*

In *Perfect 10 v. CCBill*, the Central District of California indicated that some interplay exists between the notification requirements and the desire to stop repeat infringers.¹⁹³ The district court held that an ISP's termination policy is not reasonable under section 512(i) if the ISP fails to exclude a customer's account despite receiving multiple notifications that comply substantially with the requirements of section 512(c)(3).¹⁹⁴ One defendant argued that post-litigation notifications of infringement do not act as DMCA compliant notifications.¹⁹⁵ Although the court found that the specific notification letter lacked compliance with section 512(c)(3), it found compliance lacking because the letter failed to identify the copyright owners, not because the notice was sent after litigation began.¹⁹⁶ With respect to another defendant, the *CCBill* court held that a notification which identified the website, without the URLs of the infringing images, did not substantially comply with section 512(c)(3).¹⁹⁷ The reason for requiring the inclusion of the URL was to assist the ISP in locating and removing the infringing material, and the district court made it clear that the copyright holder must assume the responsibility.¹⁹⁸ Plaintiffs also sent notifications regarding password hacking websites; however, because they failed to submit "any evidence that the use of the passwords on these websites actually resulted in the infringement of Perfect 10's copyrights," the court concluded that this notification lacked substantial compliance with the DMCA.¹⁹⁹

The requirement of specific URLs seems necessary to identify material, and thus, it ought to be required that a copyright holder specifically identify the infringing material. Many large sites have complex levels and areas. Those that are not well organized can be extremely difficult to navigate. The inclusion of the specific URL for infringing content eliminates any problems that an ISP may encounter in attempting to remove the material. The court's decision not to find post-litigation notices per se noncompliant with the DMCA is not surprising. By allowing post-litigation notices to comply with the DMCA, the courts leave an opportunity for cases to settle without resolution from the courts.

The Fourth Circuit in *ALS Scan v. Remarq Communities* interpreted the elements of notification from section 512(c)(3) loosely as well.²⁰⁰ This flexible interpretation aids copyright owners by preventing ISPs from shielding themselves from liability when they receive notifications that do not meticu-

193. *Perfect 10 v. CCBill*, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004).

194. *Id.*

195. *Id.* at 1096.

196. *Id.*

197. *Id.* at 1100.

198. *Id.*

199. *Id.* at 1101.

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

lously meet all requirements of section 512(c)(3). The plaintiffs in this case sent a letter to the ISP informing it that certain newsgroups contained copyright infringing images.²⁰¹ The letter included a website where the plaintiffs' models could be identified and another website with the plaintiffs' copyright information.²⁰² The ISP responded by refusing to shut down the newsgroups without more information about specific infringing images.²⁰³ The plaintiffs responded that the "newsgroups have apparently been created by individuals for the express sole purpose of illegally posting, transferring and disseminating photographs that have been copyrighted."²⁰⁴ The plaintiff claimed that the newsgroups "serve no other purpose."²⁰⁵ The ISP's motion to dismiss was granted by the district court, holding that the notice failed to comply with section 512(c)(3).²⁰⁶ Plaintiff argued to the Fourth Circuit that it was not the intent of Congress to allow ISPs to shield themselves from liability when "a cease and desist notice failed to technically comply with the DMCA."²⁰⁷ The ISP claimed to be shielded from liability because "it did not have 'knowledge of the infringing activity as a matter of law.'"²⁰⁸ The circuit court's decision mentioned the Congressional goal of maintaining the "balance between the responsibilities of the service provider and the copyright owner."²⁰⁹ The court then focused its attention on the use of the modifiers "substantially" and "reasonably" in section 512(c)(3) and concluded that the requirements were not meant to "burden copyright holders with the responsibility of identifying every infringing work—or even most of them."²¹⁰ This decision wrongly shifts much of the burden from the copyright holder to the ISPs. The copyright holder has a self-interest in policing infringement, and therefore he should be required to notify the ISP of the specific material that infringes his specific rights. To place the majority of the burden on the ISP would disrupt the careful balance that Congress created.

In contrast to the loose interpretation in *ALS*, the Central District of California in *Hendrickson v. Amazon.com* strictly interpreted the notification requirements of section 512(c)(3), which allowed Amazon to escape liability.²¹¹ In *Hendrickson*, the plaintiff sent a letter notifying Amazon that all

201. *Id.* at 620.

202. *Id.* at 620-21.

203. *Id.* at 621.

204. *Id.*

205. *Id.*

206. *Id.*

207. *Id.* at 622.

208. *Id.*

209. *Id.* at 625.

210. *Id.*

211. *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003).

DVD copies of a specific movie infringed his copyright.²¹² At the time the letter was sent, the plaintiff had not released or authorized the release of the movie in DVD format.²¹³ Approximately nine months later, the plaintiff found a DVD copy of his movie on sale on Amazon, purchased it, and filed suit.²¹⁴ Similar to the *ALS* decision, the *Hendrickson* court discussed the balance created by Congress that “both the copyright owner and the ISP should cooperate with each other to detect and deal with copyright infringement.”²¹⁵ The California district court stated that a copyright holder should not be able to “write one blanket notice to all service providers alerting them of infringing material, thus, relieving him of any further responsibility, and thereby, placing the onus forever on the ISP.”²¹⁶ The district court, however, also recognized that Congress did not intend for copyright owners to solely and perpetually police the Internet for infringement.²¹⁷ Furthermore, just as the court in *ALS* mentioned balance and then proceeded to take a seemingly polar position, the court in *Hendrickson* took similar action. The *Hendrickson* court determined that the present tense of the DMCA meant that a notification must be referring to infringing activity occurring at the time the ISP receives notice.²¹⁸ This holding does not require ISPs to continually and perpetually monitor the Internet nor does it require ISPs to respond to merely potential infringement.²¹⁹ The district court reasoned that the purpose of the notice and takedown provisions was to promote the removal of infringing material from the Internet; however, this goal cannot be accomplished if the material is not posted on the Internet at the time of the notice.²²⁰ The court stated that nine months was too large a span of time for the notice to remain effective.²²¹ The court’s analysis of the present tense language seems slightly forced. Nine months is not a very long time considering the ability of ISPs to use automated computers to monitor the posting of infringing material. After informing an ISP of a bona fide potential infringement, its responsibilities and duties should be heightened. It is inequitable to say that an ISP can escape liability simply because a copyright holder informed the ISP too early of a possible infringement. Rather, in the spirit of cooperation created by the DMCA, a possible solution would be requiring repeat notice from the copy-

212. *Id.* at 915.

213. *Id.* at 914.

214. *Id.* at 915.

215. *Id.* at 916-17.

216. *Id.* at 917.

217. *Id.*

218. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

right holder to the ISP that need not substantially comply with the technical requirements of the initial notice.

An interesting view concerning the notice and takedown provisions of the DMCA is found in *Fatwallet v. Best Buy*, a case in which the plaintiff sought declaratory relief regarding the alleged unconstitutionality of the DMCA.²²² In *Fatwallet*, the district court made a point of declaring that no additional liability other than that normally found in copyright law attaches to an ISP that does not respond to a proper notice by removing the infringing material.²²³ Thus, an ISP is “in no worse a position regarding potential copyright liability for the postings of its subscribers whether it responded to the notice or not.”²²⁴ The fact that an ISP cannot be harmed by the DMCA’s notice provisions led the court to hold that the plaintiff did not have standing because it could not “claim it suffered any injury or harm.”²²⁵

A discussion of the balance between copyright holders and ISPs would be incomplete without reference to section 512(f). As mentioned before, the notice and takedown scheme is meant to encourage ISPs to remove infringing material upon proper notice from the copyright holder by shielding ISPs from liability in exchange for compliance. The potential for abuse of this system is plain to see. An individual or corporation could easily send a false notice in order to compel an ISP to remove material from the Internet for the purposes of censorship or even to reduce competition. Larger ISPs with teams of lawyers would probably not be bullied into cooperating, but smaller ISPs and website operators unaware of the law may consider the possibility of being held liable too costly to risk not acquiescing.

Apart from the obvious inequities of such a situation, there could also be the potential for the dreaded chilling effect on free speech. ISPs would begin closely monitoring the material they allow to be posted on the Internet and would stay away from borderline material that could expose them to liability. Fortunately, section 512(f) protects against the possibility of abuse by making liable “[a]ny person who knowingly materially misrepresents. . . that material or activity is infringing.”²²⁶ The party responsible for the misrepresentations is liable for the damages and attorneys’ fees that an ISP suffers in acting to remove allegedly infringing material.²²⁷ In interpreting section 512(f), the court in *Online Policy Group v. Diebold*, rejected both plaintiffs’ and defendants’ interpretation of “knowingly materially misrepre-

222. *Fatwallet, Inc. v. Best Buy*, 2004 WL 793548, at *1 (N.D. Ill. 2004).

223. *Id.* at *2.

224. *Id.*

225. *Id.*

226. 17 U.S.C. § 512(f).

227. § 512(f).

sents.”²²⁸ Plaintiffs argued that the standard meant that section 512(f) was violated if notice of infringement was sent without a “likelihood of success” on the merits of the claim.²²⁹ On the other hand, defendants argued that section 512(f) was not violated unless the notice sent was “frivolous.”²³⁰ Recognizing problems with both standards offered by the parties, the California district court chose to stick with the plain language of the statute.²³¹ It used the Black’s Law Dictionary definition of knowingly: “a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations.”²³² “Material” meant that “the misrepresentation affected the ISP’s response to a DMCA letter.”²³³ The court held the copyright holder liable under section 512(f) for sending notice to ISPs and requesting removal of e-mail archives, much of which clearly was subject to a fair use defense.²³⁴ The court chastised the copyright holder for using the notice provisions “as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.”²³⁵

2. Actual or Constructive Knowledge

The safe harbor provision for information residing on systems or networks at the direction of users, section 512(c), seems to be the most highly litigated limitation on liability. In *Hendrickson v. Ebay*, a California district court held that section 512(c) required an ISP to satisfy three prongs before it could be shielded from immunity.²³⁶ Requiring the takedown of infringing material upon proper notice from a copyright holder is only the third prong.²³⁷ The first prong, found in section 512(c)(1)(A), requires an ISP to “demonstrate that it does not have actual knowledge that an activity using the material stored on its website is infringing or an awareness of ‘facts or circumstances from which infringing activity is apparent.’”²³⁸ However, if an ISP did have such knowledge, it must show that it acted expeditiously to

228. *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004).

229. *Id.*

230. *Id.*

231. *Id.*

232. *Id.* (quoting BLACK’S LAW DICTIONARY (8th ed. 2004)).

233. *Id.* (quoting BLACK’S LAW DICTIONARY (8th ed. 2004)).

234. *Id.*

235. *Id.* at 1204-05.

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

237. *Id.*

238. *Id.*

remove the material.²³⁹ As discussed earlier, the court pointed out that a notice sent to an ISP by a copyright holder that fails to substantially comply with the requirements of section 512(c)(3) will not be used to resolve whether an ISP had actual or constructive knowledge under the first prong of the test.²⁴⁰ In the *Hendrickson* case, the district court dispensed with the issue rather quickly by stating “eBay’s evidence shows that prior to this lawsuit, it did not have actual or constructive knowledge.”²⁴¹

Corbis v. Amazon.com spends more time on this first prong because the copyright holder chose to initially file suit rather than to use the notice provisions of section 512(c)(3).²⁴² The copyright holder argued that Amazon had knowledge, despite their failure to give notice, because Amazon had received notice from other copyright holders about their own infringing photos and because Amazon knew that the copyright holder licensed their photos.²⁴³ The Washington district court held that this “general awareness that a particular type of item may be easily infringed” was not proof of knowledge.²⁴⁴ Amazon’s specific knowledge of actual infringing items would work in the copyright holder’s favor.²⁴⁵ The court then turned its attention to apparent knowledge and explained that “the question is not ‘what a reasonable person would have deduced given all the circumstances,’” but rather “‘whether the service provider deliberately proceeded in the face of blatant factors of which it was aware.’”²⁴⁶ The *Corbis* court held that according to Congress, apparent knowledge could be demonstrated by showing that a site had “red flags” of infringement.²⁴⁷ Examples of these red flags are the presence of words like “pirate” or “bootleg” or other “slang terms in their URL and header information to make their illegal purpose obvious.”²⁴⁸ Finally, the district court rejected the copyright holder’s argument that Amazon had apparent knowledge because of the other infringement notices it received from other copyright holders.²⁴⁹

The safe harbor provision for referring or linking users, section 512(d), contains the same three prong analysis as section 512(c). In *Perfect 10 v.*

239. *Id.*

240. *Id.* at 1092-93.

241. *Id.* at 1093.

242. *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1107 (W.D. Wash. 2004).

243. *Id.*

244. *Id.* at 1107-08.

245. *Id.* at 1108.

246. *Id.*

247. *Id.*

248. *Id.*

249. *Id.*

CCBill, the California district court held that the fact that websites had disclaimers that “the copyrighted images are in the public domain or that the webmaster is posting the images for newsworthy purposes” was not enough to constitute a red flag of potential copyright infringement to the ISP.²⁵⁰ The court, however, gave no credence to the plaintiff’s argument that the ISP had knowledge under section 512(c) because the site at issue was a celebrity website with pictures of celebrities and that most celebrity websites contained infringing stolen material.²⁵¹

3. Financial Benefit and Ability to Control

The second prong of the section 512(c) safe harbor provision requires an ISP to show that it “does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.”²⁵² Thus, before a court will examine whether an ISP receives a financial benefit (which oftentimes they do), it will first look to whether the ISP can control the infringing activity. In interpreting the ability to control language, the district court in *Hendrickson v. Ebay* held that it “cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system.”²⁵³ The court’s reasoning for this was that to hold otherwise would make the DMCA internally inconsistent.²⁵⁴ The court explained that section 512(i) requires an ISP to adopt a reasonable termination policy for infringers and that the courts cannot remove the liability shield via section 512(c)(1)(B) from an ISP that is merely complying with another section of the DMCA.²⁵⁵ Additionally, eBay’s practice of monitoring for infringing material was voluntary, and the court believed that they should not be penalized for engaging in such practices.²⁵⁶ Furthermore, because eBay never had “possession of, or opportunity to inspect” the items sold through it, the company did not have the ability to control the infringing activity.²⁵⁷

Similarly, in *Hendrickson v. Amazon.com*, the district court found that Amazon never had possession of the infringing movie since it was a third party sale and thus Amazon never had the opportunity to inspect it nor the ability to control it.²⁵⁸ Even the fact that Amazon provided automatic e-mail responses when sales were transacted and helped with the processing of

250. *Perfect 10 v. CCBill*, 340 F. Supp. 2d 1077, 1098 (C.D. Cal. 2004).

251. *Id.* at 1103-04.

252. 17 U.S.C. § 512(c)(1)(B).

253. *Hendrickson v. Ebay, Inc.*, 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001).

254. *Id.*

255. *Id.* at 1093-94.

256. *Id.* at 1094.

257. *Id.*

258. *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003).

credit card payments did not convince the court that Amazon had the ability or right to control the infringing activity.²⁵⁹ The plaintiff in *Corbis v. Amazon.com* attempted to distinguish the *Hendrickson* case by claiming that Amazon met with and encouraged vendors to list their material on its site.²⁶⁰ The *Corbis* court dismissed this argument because there was no indication that Amazon knew that the vendors' materials were copyright infringing and because Amazon never had the materials in its possession.²⁶¹

The district court in *Perfect 10 v. Cybernet* held that the ISP did receive a financial benefit as well as had the ability to control the infringing material, thus preventing the ISP from availing itself of the safe harbor shield.²⁶² The defendant had a "direct flow of income" based on the increase of users from sites carrying infringing material.²⁶³ The court described it very simply as "[t]he more new visitors an infringing site attracts, the more money Cybernet makes."²⁶⁴ In addition, the ISP had an ability to control the infringing activity because it "prescreens sites, gives them extensive advice, [and] prohibits the proliferation of identical sites."²⁶⁵ The district court in *Perfect 10 v. CCBill* held that although the *Cybernet* court found that the ISP had the ability to control the infringing activity in that case based on its screening and advice giving activities, prescreening sites for child pornography and other obscenity alone would not be sufficient to deem an ISP as having the ability to control the infringing activity.²⁶⁶

VII. WITH KNOWLEDGE AND POWER COMES LIABILITY

The amount of knowledge and power that an ISP has is inextricably tied to the potential liability it is exposed to. This is apparent in traditional media with publishers responsible for editing content being held liable more often for defamation compared with distributors who merely supply it. This idea is also apparent in copyright law with the ability to control element of the second prong of section 512(c). The parallel between increased liability and increased knowledge and control is justified because as ISPs become more than mere conduits for connecting to the Internet, they should be held correspondingly more responsible for the increasingly diverse roles they play in mass communication. The more editorial control an ISP has over a posting, the more liable it will be for defamatory comments within that posting. Con-

259. *Id.*

260. *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004).

261. *Id.*

262. *Perfect 10, Inc. v. Cybernet, Inc.*, 213 F. Supp. 2d 1146, 1181 (C.D. Cal. 2002).

263. *Id.*

264. *Id.*

265. *Id.* at 1182.

266. *Perfect 10, Inc. v. CCBill, L.L.C.*, 340 F. Supp. 2d 1077, 1105 (C.D. Cal. 2004).

versely, if an ISP's server is being used as a merely passive way station between other computers, it should not be held liable at all. The reasoning behind this is that an ISP with power has the choice to decide whether to publish something potentially defamatory or not and therefore should have to face the consequences of that choice. A passive server has no choice or power to determine the content that passes through it, and bears no corresponding guilt for the defamatory material. Similarly, in copyright law, if an ISP knows of infringing material, it has the duty to remove it. Without knowledge, an ISP is not required to go out looking for infringing material; however, once it receives notice and the awareness of the existence of the infringing material, it gains a corresponding responsibility to remove the material. In this way, it is not intentionally facilitating a violation of the copyright holder's constitutionally protected rights.

VIII. FIRST AMENDMENT AND THE INTERNET

The Internet has already revolutionized the way in which we communicate. It is a powerful tool that must be carefully maintained if we are to continue using it far into the future. The First Amendment exemplifies our most important values regarding communication. It is inevitable that the First Amendment and the Internet will sometimes clash and yet, we must be mindful of maintaining both and somehow synthesizing the two. The potential chilling effect discussed above may seem like a slippery slope argument that presents no actual danger. Nevertheless, the realities of the marketplace and human nature compel us to always look for the easiest, least costly solutions to our problems. When it comes to liability, a preemptive decision not to include certain material is far easier and less costly than months or years of expensive litigation. As time goes on, ISPs begin to see patterns and trends in material that carries with it potential liability, and they avoid those materials and others seemingly related. The courts have paid careful attention in the past to this potential chilling effect and have maintained traditional liability rules in order to decrease it. It is wise that current and future courts do the same with respect to the Internet.

IX. CONCLUSION

Overall, courts have done promisingly well in interpreting the CDA and the DMCA. They have been careful to maintain the balance of burdens and rights of copyrights holders, ISPs, and their customers. The courts have recognized the potential for the Internet and have gone to great lengths to promote its growth. The time has now come to begin reexamining the devices used to encourage the Internet's growth and to continue curbing the potential abuses the speed and expanse of the Internet may perpetuate.

