FORTIFYING THE SAFE HARBORS: REEVALUATING THE DMCA IN A WEB 2.0 WORLD

By Brandon Brown

I. INTRODUCTION

As technology develops, so must the laws that govern it. Congress enacted the Digital Millennium Copyright Act (DMCA) in order to meet the growing need for copyright regulations on the Internet.[1] One of the most important elements of the DMCA was the codification of "safe harbors" for online service providers (OSPs).[2] As a form of quid pro quo between OSPs and copyright owners, the law provides limited immunity to OSPs if they meet certain minor burdens of copyright enforcement and cooperate with copyright owners looking to protect their works.

New developments in internet business models, however, may make the quid pro quo an unfair exchange for copyright holders. These new business models are embodied in websites utilizing what is known as the "Web 2.0" approach to web development. The websites created are almost completely based upon user-generated content, encouraging their own visitors to upload and control the content available on the website.[3] In return for the use of this service, visitors experience online advertisements tailored specifically to the type of content they view. The top websites implementing these systems (including YouTube, MySpace, Facebook)[4] were on track to amass over $1 billion in advertising revenue in 2007, which is expected to double by 2008. In some cases, these sites profit from high viewership significantly from pages that involve infringing content. For instance, some calculations predict that YouTube may be making as

---

1. *See* S. REP. No. 105-190, at 8 (1998) ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."); *see also* Peter S. Menell, Envisioning Copyright Law's Digital Future, 46 N.Y.L. Sch. L. Rev. 63, 134 (2002) (discussing the concerns behind the DMCA).

2. 17 U.S.C. § 512 (2000).

3. *See generally* Tim O'Reilly, *What is Web 2.0?*, O'REILLY (Sept. 30, 2005), http://www. oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html; *see infra* Section II.B for a discussion of Web 2.0.

4. These websites represent the most successful Web 2.0 applications on the Internet at the time of this Note. Facebook is available at http://www.facebook.com, MySpace at http://www.myspace.com, and YouTube at http://www.youtube.com.

much as $15 million directly from the presence of infringing material on their website, in addition to profits based on the traffic that the content lures into the website.[5] In exchange for this profit, these sites are only obligated to make the most minimal of efforts to prevent copyright infringement. Weighing those efforts against the financial gain of the service providers highlights a blatant inequity.

This Note posits that the Web 2.0 environment has altered the landscape of the Internet in a way that calls into question several DMCA requirements. In particular, the DMCA-embedded concepts of direct financial benefit, interference with standard technical measures, and the legislative red flag test for identifying infringing material are significantly challenged by the new ways that intellectual property is distributed on the Internet. The general policy inherent in the DMCA is that the burden for policing the Internet for copyright infringement is primarily on the copyright owner, and that online service providers must only cooperate when necessary to eliminate copyright infringement. This Note argues that this burden may be inequitable in light of the Web 2.0 movement and that a balancing test would be more appropriate for determining when OSPs should be expected to do more than simply cooperate with copyright owners.

Part II explains the legal background for secondary liability and lay the groundwork for an analysis of the Web 2.0 revolution. Next, Part II introduces the new litigation between Web 2.0 sites, such as YouTube and media conglomerate, Viacom. Part III summarizes the Millennium Copyright Act and the Online Copyright Infringement Liability Limitation Act. Part III also explores the case law and legislative history of the major safe harbor requirements and then applies the current standards to the current *YouTube* litigation.

Based on the application of the current DMCA safe harbor requirements to the *YouTube* litigation, Part IV offers a possible solution for a more flexible and equitable safe harbor test. Part IV establishes that DMCA is unnecessarily redundant when courts interpret the Act as a codification of certain parts of the common law language. The outcome of that redundancy is an inequitable application of safe harbors to some OSPs, which inevitably shields copyright infringement and could potentially discourage innovation. Since this appears counter to the Congressional intent and impetus behind the DMCA, it may be necessary to re-analyze the judicial approach to interpreting the language of the safe harbor provisions.

---

5. *See infra* Sections II.C and III.A.2.

II. BACKGROUND

A. Secondary Liability in the Digital Age

The Supreme Court was most notably presented with the issue of secondary liability in *Sony Corp. v. Universal City Studios, Inc.*[6] The defendant in *Sony* was the manufacturer of the Betamax VCR system, which at the time was a new technology that enabled the analog (but convincingly accurate) home copying of television broadcasts.[7] The plaintiffs, owners of copyrighted television content, brought suit out of concern that the new technology allowed for wide-spread infringement of their copyrighted material.[8] Unable to stop every individual home-user from recording their shows, the plaintiffs sought an injunction against the manufacturer and damages against the Betamax creator under a secondary liability theory.[9] After analyzing the value of the new technology and its significant legal uses, the Court held that when "copying equipment" is "capable of substantial noninfringing use," the manufacturer of that equipment cannot be held liable for contributory infringement.[10]

The analog copying of the Betamax was merely the beginning of a series of technological developments that would forever change the way information is reproduced. As the Internet became a more viable way of transmitting information, with the transition from dial-up networks to high-speed broadband lines in nearly every household, the possibility of wide-spread distribution of perfect digital copies of copyrighted material became a reality. In *MGM Studios, Inc. v. Grokster, Ltd.*,[11] the Court investigated an online file sharing service to determine if the defendants were shielded from liabilty under the *Sony* doctrine. Grokster is a peer-to-peer file sharing network used to transmit media files between users.[12] Although the early peer-to-peer file sharing networks developed a reputation for hosting the illegal dissemination of copyrighted material, Grokster and others defended its technology as one of the most economically efficient methods of transmitting large files, including non-infringing works.[13]

---

6. 464 U.S. 417 (1984).
7. *Id.* at 419.
8. *Id.* at 419-20.
9. *Id.*
10. *Id.* at 442.
11. 545 U.S. 913 (2005).
12. *See id.* at 919-20.
13. *See, e.g.*, Pablo Rodriguez et al., *On the Feasibility of Commercial, Legal P2P Content Distribution*, 36 ACM SIGCOMM 75 (2006), *available at* http://delivery.acm.org/10.1145/1120000/1111339/p75-rodriguez.pdf (describing P2P networks as a cost-effective solution for the distribution of large files).

Thus, in *Sony*'s terms, Grokster argued that its product had "substantial non-infringing uses."[14] The plaintiffs, however, produced significant evidence that the bulk of Grokster's corporate policy involved its system's use for distributing copyrighted material.[15] In fact, its marketing plan primarily sought to attract those who were interested in downloading copyrighted music for free.[16] Pulling from both patent law and principles of secondary liability, the *Grokster* Court held that the defendant's actions had actively induced copyright infringement and thus were not protected by the *Sony* substantial non-infringing use defense.[17] Importantly, it further elaborated that "mere knowledge of infringing *potential*" would still be insufficient to make a provider liable.[18]

Although both *Sony* and *Grokster* have some fundamental differences from Web 2.0 applications,[19] they comprise the current legal doctrine for secondary liability on the Internet and are still applicable in an analysis of Web 2.0 copyright liability. As demonstrated by *Grokster*, the Internet could host a vast nebula of potential copyright infringement, and copyright owners often viewed its continual growth as a continual threat to their content.[20] As such, the technologies that make up the backbone of the Internet—the service providers, web hosts, and search tools—would soon come under attack for similar secondary liability claims. In 1998, in partially codifying the defenses available from *Sony* and in helping protect the systems that make up the structure of the Internet from continual litigation, Congress enacted the Digital Millennium Copyright Act.[21]

---

14. *See Grokster*, 545 U.S. at 946.

15. *See id.* at 924.

16. *See id.* at 924-27.

17. *See id.* at 934-36.

18. *Id.* at 937 (emphasis added).

19. Although Grokster was an Internet application, it included a client-side component that was downloaded and executed from the end-user's computer. This is in contrast with Web 2.0 applications, which function from central servers and are not downloaded to the end-user's computer. As explained *infra* Section II.C, that difference may raise slightly different questions of liability.

20. *See generally* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001); WILLIAM FISHER, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT (2004).

21. Statement by the President on Digital Millennium Copyright, 1998 WL 754861 (Oct. 29, 1998); 145 Cong. Rec. S15228-01 (1999).

B. What is Web 2.0?

Significant confusion and discussion exists over the term "Web 2.0" and its true meaning.[22] The name alone draws much consternation from veteran internet developers, who argue that such a term erroneously implies that there is a delineated and categorical difference between types of websites.[23] Some developers are also concerned about using a term which may falsely attribute progress or improvement to something that is simply different.[24] The originator of the term, Tim O'Reilly,[25] concedes that although the name might not be completely appropriate, it suffices as a decent "meme"[26] for defining this particular cultural practice.[27]

Based on the predominant abstract definition, a Web 2.0 framework exists on a website when the bulk of that website's content, growth, and development come from individual end-users.[28] User behavior is never anticipated nor predetermined, and the underlying technology of Web 2.0 applications grows with the growth of the user base.[29] The concept requires decentralization of activity and a focus on active user participation.[30] It harnesses the collective wisdom of a large user base and organizes it effectively.[31]

In practical application, Web 2.0 websites as they exist today rely on the content of their end-users but the programming of their own developers.[32] The materiality of the content can range from posted articles to digital family movies and from personal profiles to online photo albums.

---

22. *Compare* O'Reilly, *supra* note 3 *with* Tim Bray, *Web 2.0 or Not?*, Aug. 11, 2005, http://www.tbray.org/ongoing/When/200x/2005/08/09/Web-2.0 (arguing that such a classification is unneeded and irrelevant).

23. Bray, *supra* note 22.

24. *Id.*

25. Tim O'Reilly is the founder of O'Reilly Media, Inc., an American media company and publisher focusing on computer programming and technology books.

26. Posting of Tim O'Reilly to O'Reilly Radar, Not 2.0? (Oct. 5, 2005), http://radar.oreilly.com/archives/2005/ 08/not_20.html.

27. *Id.*

28. O'Reilly, *supra* note 3.

29. *Id.* at § 7.

30. *Id.* at §§ 1-2.

31. *Id.* at § 1.

32. This may be a tempting place to argue that open-source Web 2.0 environments allow their users to take full control of the system. However, such an advocate would be hard-pressed to find an online service that is actively open-source. There are significant security risks involved in allowing end-users to, in a manner similar to Wikipedia, alter the code of the website at will. As such, Web 2.0 applications do not develop in time with the users; rather, their programmers try to take the pulse of their users as often as possible and adjust the system to match.

While the content is provided by the end-users, the forum in which the content is posted is designed by the OSP.[33]

The distinction between the role of the end-user and the role of the OSP is important for a legal analysis of secondary liability in this area. It is true that a Web 2.0 environment is heavily shaped by the posting of its users. This, in turn, creates significant difficulties for OSPs who wish to police material posted to their website. However, the posted material is still shaped by the limits of the software and thus by the will of its programmers.[34] Since the software does not evolve organically, but rather is only changed by conscious choices made by its developers, the theory of a Web 2.0 environment being completely out of the hands of the online service providers is a legal and technological fiction.[35]

As use of the term Web 2.0 becomes increasingly prevalent, there is a large trend towards referring to many websites as user-generated content (UGC) sites.[36] For most copyright issues, the two concepts are synonymous; however, there are some philosophical and technical differences and, in general, UGC websites represent a subset of Web 2.0 environments.[37]

C. YouTube and Viacom

One of the premier examples of a Web 2.0 website on the Internet today is YouTube. YouTube is an online video-sharing website.[38] Founded in February 2005, YouTube has grown exponentially: it now amasses well over 100 million video views daily[39] and is the third-most viewed website

33. To be fair, there are certainly Web 2.0 applications that do allow this sort of growth. Open-source development, as found on sites like SourceForge, allow for implementation of the more theoretical elements of a Web 2.0 framework. The advancement of certain operating systems, like Linux, is dependent on the input of users and each release is heavily shaped by decentralized programmers who dedicate some of their time to improving the flaws in the system. However, these are the underlying frameworks of a Web 2.0 website; they do not represent the content posted on the website or play a visible role in its presentation.

34. Bray, *supra* note 22.

35. *See id.*

36. *See, e.g.*, Wikipedia, User Generated Content, http://en.wikipedia.org/wiki/User-generated_content (last modified Feb 1, 2007).

37. *See generally* O'Reilly, *supra* note 3, §§ 1-2.

38. YouTube—What is YouTube?, http://www.google.com/support/youtube/bin/answer.py?answer=55749&topic=10509 (last visited Dec. 1, 2007).

39. *YouTube Serves up 100 Million Videos a Day Online*, USATODAY.COM, http://www.usatoday.com/tech/news/2006-07-16-youtube-views_x.htm? (July 16, 2006.com.

on the Internet.[40] The website hosts, at best estimate, around 61 million videos.[41] It operates under a typical Web 2.0 format, utilizing user-based content as the bulk of its online material and employing user feedback and comments to rank videos and assign them priority in search methods.[42] In November 2006, it was purchased by Google Inc. for $1.65 billion.[43]

In March 2007, Viacom, an American media conglomerate, filed suit against YouTube for both direct and secondary copyright infringement allegedly occurring on the YouTube servers. Viacom alleges in its complaint that it has detected over 150,000 infringing "clips of copyrighted programming" on the YouTube servers that have amassed a total of 1.5 billion views.[44] This represents one of the first times that a Web 2.0 website has been legally challenged for this level of copyright infringement, and as such, is a perfect example to explore the application of the DMCA's provisions to a Web 2.0 website.

III. DMCA PROVISIONS

The Digital Millennium Copyright Act (DMCA), signed into law on October 28, 1998, was written to address the growing threat of digital copyright infringement. It criminalizes the production and dissemination of technology designed to circumvent digital protection schemes,[45] but contains provisions for shielding service providers from liability for copyright infringement.[46] According to President Bill Clinton, who signed the bill into law, the DMCA "grant[s] writers, artists, and other creators of copyrighted material global protection from piracy in the digital age."[47]

---

40. Youtube.com—Traffic Details from Alexa, http://www.alexa.com/data/details/traffic_details?url=http://www.youtube.com (last visited June 1, 2007).

41. YouTube—Search, http://www.youtube.com/results?search_query=*&search=Search (last visited Dec. 1, 2007). Although this number is not published anywhere, a search for the universal wildcard character ["*"] should reveal all the items contained in YouTube's database; at this time, the number of files retrieved was "about 61,100,000."

42. YouTube—How Do Videos Get Featured?, http://www.google.com/support/youtube/bin/answer.py?answer=55751&ctx=sibling (last visited Dec. 1, 2007).

43. Ben Charny, *Google to Acquire YouTube for $1.65 Billion in Stock*, MARKETWATCH, http://www.marketwatch.com/News/Story/Story.aspx?guid=%7B05306ED9-F56E-467C-BBA3-AFD9EB7335F8%7D&siteid=yhoo&dist=yhoo (last visited Dec. 1, 2007).

44. Complaint at 3, Viacom Int'l v. YouTube, Inc., No. 1:07CV02103, 2007 WL 775695 (S.D.N.Y. Feb. 30, 2007).

45. 17 U.S.C. § 1201 (2000).

46. 17 U.S.C. § 512 (2000).

47. Statement by the President on Digital Millennium Copyright, 1998 WL 754861 (Oct. 29, 1998).

The provisions meant to protect service providers from liability are known as the Online Copyright Infringement Liability Limitation Act (OCILLA) and are codified in Title II of the DMCA.[48] The provisions offer "safe harbor" protections, or immunity from copyright liability, to qualifying internet entities known as "OSPs".[49] An OSP must meet two general conditions in order to receive the protections of the OCILLA: first, it must publicly "adopt and reasonably implement a policy" of addressing and terminating accounts of users who are found to be "repeat infringers;"[50] and, second, the OSP must accommodate and not interfere with "standard technical measures."[51]

The statute defines standard technical measures as technological means of detecting online copyright infringement which have been developed via inter-industry discussions and are both available to any person on reasonable terms and do not impose substantial costs on service providers.[52] The legislative history notes that "the Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age."[53] The idea is that by building in measures that develop with industry standards, the statute will have the flexibility to grow with the technology, rather than codifying any particular system of detecting infringement.[54]

The OCILLA extends protections to several different types of OSPs. Only one protection is relevant for this Note: § 512(c), which limits the liability of OSPs for hosting infringing material on their servers. In order to acquire this immunity, § 512(c) requires: that an OSP 1) must not receive a financial benefit directly attributable to the infringing activity;[55] 2) must not be aware of the presence of the infringing material[56] or know any

48. 17 U.S.C. § 512 (2000).

49. Online service providers ("OSPs") are "entit[ies] offering the transmission, routing, or providing of connections for digital online communications . . . [and] of material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C. § 512(k)(1)(A) (2000). Safe harbor protections extend to OSPs involved in "transitory communications," "system caching," "storage of information on systems or networks at the direction of users," and "information location tools." 17 U.S.C. § 512(a)-(d) (2000).

50. 17 U.S.C. § 512(i)(1)(A) (2000).

51. 17 U.S.C. § 512(i)(1)(B) (2000).

52. 17 U.S.C. § 512(i)(2) (2000).

53. H.R. REP. NO. 105-551, at 61 (1998). The irony of this statement is that technology is a double-edged sword: it is both the cause and solution to the copyright infringement problems that the DMCA was written to address.

54. *See* H.R. REP. NO. 105-551, at 61 (1998).

55. 17 U.S.C. § 512(c)(1)(B) (2000).

56. 17 U.S.C. § 512(c)(1)(A)(i) (2000).

facts or circumstances that would make infringing material apparent;[57] and 3) upon receiving statutorily-proper notice from copyright owners or their agents, must act expeditiously to remove any claimed infringing material.[58] These requirements are in addition to the underlying prerequisites of complying with standard technical measures and removing repeat infringers.[59]

One of the key features found in the DMCA and its history is the concept of an economic balancing test for the burden of policing for copyrighted material on the Internet.[60] Traditionally, this burden has rested solely on the copyright owner.[61] However, with the development of vicarious liability in *Sony* and *Grokster*, OSPs now have a duty to avoid inducing or directly contributing to online copyright infringement.[62] The DMCA goes further, offering a quid pro quo for OSPs: OSPs may receive immunity from secondary liability if they cooperate with a copyright owner who has a good-faith belief that direct infringement is occurring within the confines of that OSP's services.[63] In essence, OSPs seeking safe harbor immunity must take on part of the copyright enforcement burden. The extent to which they are expected to take on that burden, however, is often weighed in the courtroom and plays a major role in the analysis of the requirements of whether they are entitled to immunity under § 512(c) delineated above.

The scope, depth, and application of those requirements will be explored individually below. Following that, each Section will be individually applied to both real and hypothetical situations in a Web 2.0 context in order to evaluate their flexibility and unveil any inconsistencies that may make their application unappealing or injudicious.

A. Direct Financial Benefit

1. Legislative History

Section 512(c)(1)(B) of the Digital Millennium Copyright Act requires that an OSP not receive any "financial benefit directly attributable to the infringing activity" in order to enjoy safe harbor immunity from secondary

57. 17 U.S.C. § 512(c)(1)(A)(ii) (2000).
58. 17 U.S.C. § 512(c)(1)(C) (2000).
59. *See* 17 U.S.C. § 512(i)(1)(A)-(B) (2000).
60. *See* H.R. REP. NO. 105-796, at 83-84 (1998), *available at* http://www.hrrc.org/File/H.R._2281_conf._report.pdf.
61. *See* S. Rep. No. 105-190, at 8 (1998).
62. *See infra* Section II.A.
63. *See generally* 17 U.S.C. § 512 (2000).

liability for copyright infringement.[64] However, since most OSPs function for profit, that statement requires more clarity to identify which types of financial benefit Congress sought to target.

The legislative history is dichotomous. It states that, on one hand, a service that receives a "one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities" is not receiving a direct financial benefit, but, on the other hand, a provider whose "value . . . lies in providing access to infringing material" is considered to be receiving a direct benefit.[65] The absence of any substantive metric (e.g., "whose *primary* value lies in provided access to infringing material," which would significantly clarify the standard) creates a confusing analysis of modern internet service providers.[66]

The language of the statute itself appears to be derived from the general elements of vicarious liability for copyright infringement. Its appearance in the DMCA is consistent with this concept: if there is a direct financial benefit from the infringement, then the OSP is secondarily liable; if not, it has a significant defense to the claim, and so should be protected against undue litigation by a DMCA safe harbor.[67] However, because the DMCA is intended to make "important improvements" to current intellectual property laws[68] and to provide "global protection from piracy in the digital age,"[69] it seems reasonable to expect a more modernized and specific statutory scheme than the common law rule for vicarious liability for addressing when and where direct financial benefit exists in online transactions.

2. Case Law

The Ninth Circuit in *Perfect 10, Inc. v. CCBill, LLC* sought to clarify this situation by revisiting the common law roots of the term "direct financial benefit."[70] CCBill (with commercial partner, CWIE) is an online web hosting and credit card processing company that caters primarily to the web-based adult entertainment community.[71] Perfect 10 is a publisher of online adult content whose copyrighted works were found to be on multi-

64. 17 U.S.C. § 512(c)(1)(B) (2000).
65. H.R. REP. NO. 105-551, at 54 (1998).
66. *Id.*
67. *See, e.g.*, Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102 (9th Cir. 2007).
68. 145 CONG. REC. S15228-01 (1999).
69. Statement by the President on Digital Millennium Copyright, 1998 WL 754861 (Oct. 29, 1998).
70. Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).
71. *See id.* at 1108.

ple sites hosted by CCBill/CWIE.[72] CCBill sought safe harbor under the § 512 provisions as a web host and was challenged by Perfect 10, who argued that CCBill was receiving a financial benefit from the infringing material and should thus be held secondarily liable for it.[73] Although the Ninth Circuit remanded on the facts, the court also held that "'direct financial benefit' [under § 512(c)] should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability."[74] In order to analyze how that common law standard has developed, and its limits when applied to internet technology, an examination of prior case history of the common law standard of vicarious copyright liability is necessary.

The Ninth Circuit in *A&M Records, Inc. v. Napster, Inc.*[75] examined the liability of a service provider whose primary (one might even say sole) purpose was in facilitating the distribution of copyrighted material. Napster was an online peer-to-peer file sharing distribution system that utilized a centralized database system to track songs available for download. The system facilitated the large-scale distribution of media files (primarily music) across a network of, at one point, 26.4 million users.[76]

Restating the common law rule of traditional vicarious infringement, the *Napster* court held that a direct financial benefit exists when the availability of infringing material "acts as a 'draw' for customers."[77] The court found that Napster's revenue was "directly dependent" upon the size of its userbase, and that as that base increased, so did the "quality and quantity of available [copyrighted material]."[78] That is, Napster's revenue was tied directly to the number of times advertisements were viewed on the system, and that number was directly proportional to the number of users on the system. Since the only reason these users accessed Napster's system was to exchange and download media files, the court concluded that the copyrighted material available on Napster's system acted as "draw" for customers and thus found that Napster was receiving a direct financial benefit from the presence of infringing material.

---

72. *See id.* at 1117.

73. *See id.* at 1116.

74. *See id.* at 1117.

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

76. Press Release, Jupiter Media Metrix, Global Napster Usage Plummets, But New File-Sharing Alternatives Gaining Ground, July 20, 2001, http://www.comscore.com/press/release.asp?id=249.

77. *See Napster*, 239 F.3d at 1023.

78. *Id.*

A few years later, the Ninth Circuit arguably attempted to close some of the wider doors that *Napster* had opened in *Ellison v. Robertson*.[79] In *Ellison*, the court addressed the larger question of whether an internet provider which simultaneously cached and stored messages from various online discussion groups could be liable for infringing material found in those stored messages.[80] USENET, which stems from "user network," was a large-scale news-group network, upon which any user may post material, comments, news, or engage in discussions.[81] The network relied on cooperating service providers to receive, transmit, and store messages in order to achieve its wide-spread distribution and syndication.[82] As part of their service to customers, the service provider, America Online (AOL), operated servers to and upon which USENET messages were forwarded and stored.[83]

The case stemmed from one particular message transmitted to USENET servers, in which a digital version of the plaintiff's copyrighted fictional work was included and distributed.[84] As a USENET service provider, AOL's servers received, retained, and provided copies of this message to its users.[85] The *Ellison* court examined whether AOL's profit from the presence of the infringing material was sufficient to establish a direct financial benefit.[86]

The district court in *Ellison* attempted to distinguish the facts involving AOL from *Napster* by declaring that a financial benefit must represent a "substantial" proportion of the provider's income.[87] The Ninth Circuit, however, expressed concern, noting that any subset of income will be unsubstantial when compared to the whole to a large service provider.[88] The Ninth Circuit instead distinguished between whether activity constituted a "draw" or whether it was simply an added benefit to customers.[89] The Ninth Circuit went no further in explaining the difference between the two alternatives than to find that since AOL neither "attracted [n]or retained

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

80. *See id.* at 1074-75.

81. *See generally* Wikipedia, Usenet, http://en.wikipedia.org/wiki/Usenet (last modified Nov. 21, 2007).

82. *See generally id.*

83. *See Ellison*, 357 F.3d at 1075.

84. *See id.* at 1074-75.

85. *See id.*; *see also* Wikipedia, Usenet, *supra* note 81.

86. *See Ellison*, 357 F.3d at 1078-79.

87. *Id.*

88. *See id.*

89. *See id.*

. . . [n]or lost . . . subscriptions" because of the infringing material, there was no direct financial benefit to AOL.[90]

It is unclear whether, in dismissing the district court's "substantial" analysis in favor of its own "draw" standard articulated in *Napster*, the Ninth Circuit attempted in *Ellison* to clarify the financial benefit requirement. The concept of the "draw" standard seems to hinge not on the economic balancing instilled in the DMCA,[91] but rather on the terms found in secondary copyright infringement liability.[92] The "draw" standard measures customer attraction and attempts to indirectly determine if the OSP has induced this behavior.[93] In contrast, a "substantial" analysis explores whether the OSP has the economic ability to take on some of the burden of copyright policing.[94] Part IV of this Note will argue that the "substantial" test is a more adequate analyzer of whether or not the OSP can assume some of the burden of policing for copyrighted material and is thus more true to the purpose of the DMCA.

The application of this standard has not yet been clarified in *CCBill*, which is on remand for this issue, but future decision making with a similar fact pattern will most likely require such clarification. In *CCBill* or a similar situation (i.e., addressing online web hosting providers and online financial transaction providers), courts will be called upon to examine a service provider whose activity lies somewhere between Napster and AOL. CCBill acts as a middleman in the transactions involving infringing material and is also involved in providing server space for those who may wish to infringe. Whereas Napster is more obviously peddling in copyrighted material, and whereas AOL's storage and access represents a very minor amount of copyrighted material, CCBill serves as a web hosting service for potentially infringing material and also handles credit card processing for those websites. This appears to be well beyond the financial effects in the AOL scenario because of the possibility that a significant amount of CCBill's income may be derived from websites hosting infringing material. However, it does not appear to reach the Napster level of income being derived nearly purely from infringing material.

---

90. *See id.*

91. *See supra* Part II.

92. *See supra* Section II.A.

93. *See supra* text accompanying note 11. As will be argued in Section III.A.2 and Part IV, *infra*, there is no purpose to an overlapping financial benefit test in the DMCA safe harbor provisions. Such a redundancy accomplishes nothing and prevents the DMCA from satisfying its Congressional purpose. *See supra* notes 47 & 60; *see generally* Part II.

94. *See infra* Part IV.

One can see how the analysis of the direct financial benefit in *CCBill* could turn either way. On one hand, CCBill likely hosts many non-infringing sites.[95] Indeed, it is plausible that CCBill hosts more non-infringing sites than infringing sites.[96] The substantial "draw" that CCBill offers its customers is that it provides web-hosting services; that draw does not vary according to whether or not its customers wish to have infringing material hosted.[97] Further, CCBill does not appear to be providing a haven for copyright infringement, as there are no facts in the record indicating that, like Napster, CCBill attracted customers solely because it facilitated online transactions of infringing material.[98] Thus, under the *Ellison* standard of a "draw," it would be impossible for a web host to ever be found to have a direct financial benefit from infringing material because there are so many non-infringing uses for their servers. The ability to host infringing material is simply, perhaps, an "added benefit."[99]

However, on the other hand, it is possible that the sites that CCBill does host are often involved in some form of copyright infringement, and therefore CCBill could be liable for vicarious copyright infringement. The Ninth Circuit, however, struck the "substantial[ity]" analysis in *Ellison*. Although that may have been appropriate when dealing with a large-scale internet provider like AOL (where a substantial analysis may prove unwieldy for a court), it may improperly immunize certain web-hosting providers for whom a significant amount of profit is derived from hosting infringing material. The analysis becomes even more complex when an OSP begins to profit in-line with infringing material.

3. Direct Financial Benefit in a Web 2.0 Environment

The standards set by *Ellison* and *CCBill* may prove unwieldy when applied to a Web 2.0 website. Using the *YouTube* litigation introduced *su-*

95. *See CCBill*, 488 F.3d at 1108.

96. *See id.*

97. CCBill's business model is not built around the content of the websites that it hosts, but is based on attracting customers who wish to have a reliable web hosting service combined with an integral credit-card billing service. Since CCBill doesn't regularly advertise its client base or the contents of their websites, a new client would be unaware that the company has clients that post infringing materials. As such, an argument that CCBill is "drawing" customers because of their commercial activity in infringing content will fail. *See* CaveCreek Web Hosting, http://www.cavecreek.com/ (last visited 12/1/07) (stating that CCBill's web hosting partner's website has no way to determine who its clients are or what types of sites it hosts).

98. *See CCBill*, 488 F.3d at 1102 (noting that nothing in record suggested customers were attracted solely, or at all, to host infringing content); *see also supra* note 97.

99. *See supra* Section II.A (discussing the *Betamax* case).

pra, this section will apply the "direct financial benefit" standard of the DMCA to a Web 2.0, user-generated content website.

YouTube derives a substantial part of its income through advertisements it displays on webpages with its videos.[100] Because it is likely that the infringing content on YouTube draws a significant amount of users to the site, YouTube almost certainly generates a substantial amount of income from infringing material.[101]

In its complaint, Viacom contends that it has identified 150,000 clips on YouTube that violate its copyrights.[102] The total number of views for those videos cumulatively equals 1.5 billion.[103] For this analysis, this Note will put aside YouTube's future plans for display advertisements in-line with videos[104] and prior to videos playing[105] (which would greatly increase the user's exposure to advertisements, and thus likely increase advertising revenue) and focus solely on the banner advertisements displayed in various locations on YouTube's movie pages.

For example, advertisements in Google's scheme are typically paid out based on a "price per click" system (PPC), where advertisers pay based on how many users actually click on the advertisements on the hosting webpage.[106] The average PPC varies based on the site, and is usually based on the type of viewers who visit that site. In other words, because customers who are actively looking to buy something are considered more valuable, search engines tailored to shopping websites may receive a higher PPC

---

100. DON TAPSCOTT ET. AL., WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING 270-71 (2007).

101. The analysis that follows is based on information alleged in the Viacom complaint and reasonable estimates based on readily available information about the YouTube service. This analysis is only an attempt to draw conclusions based on the available information and should not be taken as a complete analysis of the economic situation.

102. Complaint at 3, Viacom Int'l v. YouTube, Inc., No. 1:07CV02103, 2007 WL 775695 (S.D.N.Y. Feb. 30, 2007).

103. *Id.* These numbers may be contestable, considering the total number of videos and the views they receive on YouTube. *See YouTube Serves up 100 Million Videos [Views] a Day Online*, USATODAY.COM, http://www.usatoday.com/tech/news/2006-07-16-youtube-views_x.htm? (July 16, 2007).

104. Posting of Liz Gannes to Newteevee.com, Youtube's New In-Line Ads, http://newteevee.com/2007/05/ 11/youtubes-new-inline-ads-screenshots/ (May 11, 2007).

105. Directtraffic.org, Google Announces YouTube Video Advertising in 2008, http://www.directtraffic.org/OnlineNews/Google_announces_YouTube_video_advertising_for_2008_18125991.html (April 23, 2007).

106. *See* Google.com, Adwords Program Explanation, https://adwords.google.com/select/Signup1/index.html (last visited Feb. 10, 2008).

than a site where users are more actively involved in a non-commercial pursuit.[107]

The PPC for all sites has been on the rise significantly over the last few years.[108] Although it is difficult to track down the exact value for a specific website or a specific page in that website, for this analysis it will suffice to take the low-end and estimate that an advertisement on YouTube's webpage (if it follows the Google method) will have a PPC of approximately $1.00.[109]

The next metric required is a determination of how many visitors to a site will actually click on an advertising link. This is known as the "click-through rate" ("CTR").[110] This information, as well, is difficult to define and is also completely dependent on the advertisement being shown.[111] Given the presence of *some* available data on standard website advertising trends, the low estimate of a 1% CTR will be used to present a conservative analysis for YouTube.[112]

Performing a profit calculation on these two estimations and Viacom's numbers, with 1%[113] of 1.5 billion users[114] clicking on an advertisement paying $1.00 per click[115], one finds that 15 million users will click through and bring YouTube $15 million in advertising revenues based purely on infringing content.

---

107. *See, e.g.*, Posting of Nathan Weinberg to Inside Google, Price Per Click Up 25% Last Year, http://google.blognewschannel. com/archives/2006/03/22/price-per-click-up-25-last-year/ (March 22, 2006) (showing that the average cost-per-click for shopping search engines is higher than for a general webpage); *see also* DOUBLECLICK, SEARCH TREND REPORT Q4 2006 (2007), http://www.doubleclick.com/insight/pdfs/dc_search_q42006.pdf; DOUBLECLICK PERFORMICS, Q1 2007 SEARCH TREND REPORT (2007), http://www.doubleclick.com/insight/pdfs/DoubleclickPerformics50_Q1_2007.pdf [hereinafter DoubleClick Search Trend Reports].

108. DoubleClick Search Trend Reports, *supra* note 107.

109. Weinberg, *supra* note 107; *see also supra* note 101.

110. *See* Lee Sherman et al., *Banner Advertising: Measuring Effectiveness and Optimizing Placement*, 15 J. OF INTERACTIVE MARKETING 61 (2005) (defining a click-through rate as a measure of audience response to banner advertising).

111. *See, e.g.*, *id.*

112. *See, e.g.*, Press Release, ADTECH Analysis Reveals Online Advertising Click-through Rates are Falling (May 10, 2007), http://www.adtech.info/en/pr-07-10.html (click through rates vary based on search terms, type of advertisement, and user locations, but video ads receive a 5% click through rate typically). Extrapolating from this data, a 1% CTR estimate seems reasonable. It is still relatively conservative for a site of YouTube's success and user base, but more accurate numbers are simply not available.

113. *See id.*

114. *See* Complaint, *supra* note 102, at 3.

115. *See* Weinberg, *supra* note 109 and accompanying text.

This data can be aggregated across the bulk of Web 2.0-style sites. According to a recent study, user-generated content sites will amass over $1 billion in advertisement revenue in 2007 and are on track to nearly double that sum in 2008.[116]

This very real profit was not envisioned by the DMCA. Although YouTube must promptly respond to notices generated pursuant to § 512(c)(3)(a),[117] in the interval they will have generated substantial income from infringing material. Viacom's estimates imply that the majority of views on YouTube's website infringe on *its* copyrights, a fact that is questionable.[118] Assuming, instead, that infringing material represents a low 5-10% of content on YouTube,[119] current case law implies that YouTube would not be receiving a "direct financial benefit" from that content.[120] However, when deciding who bears the burden for copyright enforcement on the Internet, general profitability should enter into the equation even if the large majority of the content on a Web 2.0 user-generated website is non-infringing.

B. Knowledge of Infringement

1. Legislative History and Case Law (Notice and Red Flags)

One of the key policy roles of the safe harbor provisions is to shift the burden of policing and identifying infringing material from OSPs to the most knowledgeable source: the copyright owner. The legislative history supports this concept, explaining that a service provider "need not monitor its service or affirmatively seeks facts indicating infringing activity."[121] This concept is supported by numerous provisions of § 512, particularly in that it requires action when the OSP has actual knowledge or when the OSP has received near-perfect notice from the copyright owner.[122]

There are two ways that an OSP might receive notice of infringement. The first is through proper notice of infringement from copyright owners. In order to protect against unduly burdening providers, an OSP is not obli-

---

116. eMarketer Reports, http://www.emarketer.com/Reports/All/ Emarketer_2000421.aspx?src=report_head_info_reports (last visited Dec. 5, 2007).

117. *See infra* Section III.B.1 on knowledge and take-down notices.

118. *See YouTube Serves up 100 Million Videos a Day Online*, USATODAY.COM, http:// www.usatoday.com/tech/news/2006-07-16-youtube-views_x.htm? (July 16, 2006).

119. *See Sony*, *supra* note 6, at 443 (estimating that copyright owners in suit owned between 5-10% of all broadcasted television content).

120. It is worth noting that if Viacom's numbers are accurate, or the 5-10% estimate is low, a court could find that YouTube *is* receiving a direct financial benefit. In such a case, YouTube would lose their safe harbor.

121. H.R. REP. NO. 105-551, at 53 (1998).

122. *See* 17 U.S.C. §§ 512(c)(1)(A)(i) & 512(c)(1)(C) (2000).

gated to actively monitor its service for infringement. Instead, it is only required to act upon receiving knowledge or notice of infringement on its system.

When notice comes from a copyright owner, it must satisfy six requirements of § 512(C)(3)(a).[123] Although the statute reads that compliance with these elements must only be "substantial," the court in *CCBill*[124] recognized that the language of the statute in fact requires "substantial compliance with *all* of 512(c)(3)'s clauses."

The lenient aspect of the "substantial" requirement is in the technical details of the notice. First noted by the court in *RIAA v. Verizon Internet Services, Inc.*,[125] the legislative history identifies that errors such as "misspelling a name" or "supplying an outdated area code" will not render ineffective an otherwise complete notification.[126]

The strict notice requirement serves an important purpose. The effort required for a provider to actively monitor and attempt to identify possible infringing material would be both substantial and expensive.[127] The policy, then, represents an allocation of the initial burden for identifying and policing infringing material to the most knowledgeable source: the copyright owner.[128] Notices that do not satisfy the strict requirements do not place the service provider on notice of the potential infringement.

Further attempting to reduce the burden on OSPs, the *CCBill* court held that properly-constructed notice must exist within the bounds of a single correspondence.[129] The court noted that permitting a copyright owner to "cobble together adequate notice from separately defective notices" would represent an undue burden on the provider, who would then have to track all incoming correspondence and attempt to identify when that correspondence finally reached the levels required by § 512(c)(3).[130] Further, even though CCBill did receive some form of notice regarding potential copyright infringement, according to the court, that defective notice could not be read to give CCBill the knowledge required by § 512(C)(1)(a).[131]

---

123. *See* 17 U.S.C. § 512(c)(3)(A) (2000).

124. Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1108 (9th Cir. 2007).

125. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1239 (D.C. Cir. 2003).

126. H.R. REP. NO. 105-551 (II), at 50 (1998).

127. *See, e.g.*, *CCBill*, 488 F.3d at 1113 (finding such a burden to be substantial).

128. *See id.*; *supra* Part III.

129. *See CCBill*, 488 F.3d at 1113.

130. *Id.*

131. *Id.*

When a provider receives proper notice, it is deemed as "on notice" for a limited length of time regarding the specific infringing material identified in the notice.[132] In other words, a copyright holder may not attempt to "blanket" notice a provider for all current and future infringing materials. In *Hendrickson v. Amazon.com*, the Central District of California explored this issue on first impression and found that the "actual language of the DMCA is present tense."[133] In an attempt to shift the burden away from internet providers, the court noted that the amount of labor required to keep track of such blanket notices and filter out that material would be too onerous.[134] Instead, the court reasoned, notice only effectively concerns infringing activity that is occurring at the time the provider receives the communication.[135]

The second way an OSP can obtain knowledge of infringing activity is embodied in § 512(c)(1)(A)(ii), which is referred to in its legislative history as the "red flag" test.[136] The statute requires that an OSP not be "aware of facts or circumstances from which infringing activity is *apparent*."[137] The legislative history explains that the test to determine whether infringing activity is "apparent" contains both a subjective and an objective element. While the subjective element examines the OSP's knowledge during the time it was hosting or otherwise providing service to the infringing material, the objective element requires that the court examine the relevant facts to determine if a "reasonable person operating under the same or similar circumstances" would find that infringing activity was apparent.[138]

This absence of immunity when a provider possesses actual knowledge of infringement parallels the inducement concept in traditional copyright infringement law. Where traditional copyright law finds that evidence of "active steps . . . taken to encourage direct infringement"[139] is often sufficient to establish secondary liability, such steps are also sufficient to impute knowledge or awareness of a red flag, which thereby strips a service provider's immunity.[140]

---

132. Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003).
133. *Id.*
134. *See id.* at 917.
135. *See id.* at 916-17.
136. H.R. REP. NO. 105-551, at 25 (1998).
137. 17 U.S.C. § 512(c)(1)(A)(ii) (2000) (emphasis added).
138. *See* H.R. REP. NO. 105-551 (II) at 53 (1998).
139. Oak Indus., Inc. v. Zenith Elec. Corp., 697 F. Supp. 988, 992 (N.D. Ill. 1988).
140. *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 936 (2005).

In application, the identification and isolation of red flags may not be as simple as it seems. In *CCBill*, the Ninth Circuit explored several potential "red flags."[141] CCBill hosted several "password-hacking websites" that provided passwords furnishing access to presumably protected data.[142] The plaintiffs argued that this amounted to enabling users to infringe upon copyrights, and that CCBill's apparent knowledge of the content of these websites was sufficient to establish their actual knowledge of infringement.[143] Dismissing this argument, the court found that password-hacking sites are not per se copyright infringement.[144] It reasoned that passwords may have been provided as a short-term promotion or to collect anonymous information from viewers.[145]

In truth, the Ninth Circuit's reasoning indicates a concern about placing nearly any burden on the service providers. Although the legislative history makes clear that providers are not expected to police their own networks and content, *CCBill* arguably lays out an even broader expectation.[146] Yet if courts require service providers to actively police their hosted content by holding them liable for potentially infringing sites (e.g., the above password-hacking site), it is likely that they would shut down websites where content was questionable rather than risk liability. This creates a disconcerting slippery slope that turns service providers into censoring organizations. Out of fear for liability, OSPs would likely shut down any site which appeared to be, if only on its face, involved in copyright infringement. The password-hacking websites in *CCBill* would be shut down immediately, even if they were not actually involved in copyright infringement and merely claimed to be doing something illicit in order to attract a larger audience. The result of this would be a much less expressive Internet, and in turn, an Internet upon which the freedoms of expression protected under the First Amendment are lost as websites are shut down by OSPs out of fear of losing their immunity.

2. Red Flags in Web 2.0

In a Web 2.0 scheme, particularly a site on the magnitude of YouTube, identifying and examining red flags is even more complicated. Given the automated process in which videos are uploaded, it is hard to assume that any human employee at YouTube would see "red flags" if they were in-

141. *See* Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1113-14 (9th Cir. 2007).
142. *Id.*
143. *See id.* at 1114.
144. *See id.*
145. *See id.*
146. *See* 145 CONG. REC. S15228-01 (1999) (red flag test); *see also CCBill*, 488 F.3d at 1113-14 (finding suggested red flags to be unconvincing).

cluded in the titles of videos or in the videos themselves. The obvious circumvention is a "hack:" a program that disallows the naming or tagging of any items that have been identified as including copyrighted terms.[147] Thus, when somebody searches for "South Park" (an example from the Viacom complaint), the search will return no results. However, there are two somewhat obvious problems with this solution. First, a video with the title of "South Park" may not necessarily contain infringing content; various copyright exceptions and protections indeed encourage parodies and fair use, which often use titles of copyright material, thus unfairly limiting free expression.[148] Second, this technique has already been tried on other internet applications, but clever infringers circumvented the strategy by coining terms that allow users but not filters to identify infringing content.[149] For example, an infringer would convert the label "South Park" into "S0uth Park" or something similar, creating an endless variety of pseudonyms for potentially infringing material.

Given the complexity of this process and the reasoning behind the red flag test, it appears as though there is no necessary purpose for the test. Generally, the reason the burden of noticing copyright infringement is shifted to the copyright owner is because the copyright owner is in the best position to identify when his material is being infringed upon.[150] In truth, there are few scenarios that would raise clear and certain red flags of copyright infringement to the OSP directly. In fact, short of a service running completely for the purpose of enabling copyright infringement,[151] courts have yet to isolate specific red flags of infringement. There almost

147. *See* CDT Issue Brief: Blocking and Filtering Content on the Internet after the CDA: Empowering Users and Families Without Chilling the Free Flow of Information Online, http://www.cdt.org/speech/971015rating_issues.html (last visited Dec 1, 2007); *see generally* Wikipedia, Content Filtering, http://en.wikipedia.org/wiki/Content_filtering (last modified Dec 2, 2007).

148. *See* Press Release, Electronic Freedom Foundation, Fair Use Advocates Issue Principles for Protecting Online Videos (Oct. 31, 2007) *available at* http://www.eff.org/press/archives/2007/10/31. Additionally, YouTube remains a source of critical and parody works, many of which may fall into fair use categories. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994) (applying fair use defense to copyright infringement); *see also* Mattel, Inc. v. MCA Records, 296 F.3d 894 (9th Cir. 2002) (applying nominative and parody defense to trademark infringement).

149. The terms 'Warez,' 'Gamez,' and 'Appz' have gained popularity as alternative terms to find infringing Software, Games, and Applications available for free download online. *See, e.g.*, Wikipedia, Warez, http://en.wikipedia.org/wiki/Warez (last modified Feb. 7, 2008).

150. *See CCBill*, 488 F.3d at 1114 ("We impose no . . . investigative duties on service providers.").

151. *See, e.g.*, MGM Studios v. Grokster, Ltd., 545 U.S. 913 (2005).

always seems to be rational reasons why alleged red flags may not actually point to infringing material.

Given the profitability of hosting infringing material, however, and the somewhat general awareness (although perhaps not legally sufficient notice) of ongoing activity occurring on its servers, it is hard to imagine any Web 2.0 provider that is not sensitive if not completely aware of the infringing uses available on its system. The question of whether it is equitable to allow, expect, and even encourage OSPs to put their heads in the sand and feign ignorance will be explored in Part IV, infra.

Despite its complexities, new technology may offer a solution. Google announced in October 2007 that it would begin testing a video identification service designed to filter out infringing content.[152] The concept is a basic comparison of content: copyright owners would provide clips of their content to Google for storage in a database, and Google would compare each uploaded movie against those in the database.[153] Uploaded files that too closely resembled a file in the database would be removed.

In addition to the potential technical complexities that might arise from this (or any) technological solution, there are significant legal issues that must be addressed. One of the primary issues would be fair use: digital critiques of movies and shows, parodies, and various other potential legitimate uses of copyrighted works could be unduly censored.

Certainly, Google's algorithm represents a good-faith effort to detect infringing material and that enterprises to automatically detect infringing material are technically feasible. Given the future technological capabilities of an automated method of this kind, which will make policing infringing content easier, the legislative concern for burdening online service providers may be outdated. If this type of screening method (similar to the requested filtering methods contemplated in *Grokster* and hinted at in Google's verification system)[154] can be implemented at a low cost, then it may be reasonable to expect OSPs to play at least a minor role in the policing of content on their websites. This concept will be explored more in Part IV, infra, and considered as a potential new remedy for easing what may be an unfairly located burden.

---

152. *YouTube Rolls Out Filtering Tools*, BBC NEWS http://news.bbc.co.uk/2/hi/technology/7046916.stm (Oct. 16, 2007).

153. *Id.*

154. *See, e.g.*, *Grokster*, 545 U.S. at 916 (regarding Grokster's potential ability to develop filtering tools); *supra* Section III.B.2 (regarding YouTube's new video filtering technology).

C. Interference with Standard Technical Measures

1. Legislative History and Case Law

Section 512(i)(B) was enacted in order to allow copyright owners to exercise their due burden of monitoring the use of their copyrighted material. It requires that service providers accommodate and not interfere with "standard technical measures" used by copyright owners for identifying and protected copyrighted works.[155] In many situations, the copyright owner uses the same method available to the standard user in order to identify infringing material. For instance, the Recording Industry Association of America (RIAA) has automated its analysis of online peer-to-peer file sharing networks by implementing technology that runs on top of the software available to the average end-user.[156] The RIAA utilizes a software suite, made available by information security company MediaSentry,[157] which systematically searches file sharing networks for infringing content. In reality, the system does not appear to do much more than use publicly available end-user software to search the network.[158] In general, this is synonymous with a copyright owner using a search engine to find his material on sites not licensed to use it. When techniques like these represent the "standard technical measures" being employed by copyright owners, there is no burden on OSPs to avoid interfering with the measures since the technical measures utilize the publicly available functions of the OSP's service.

However, the statute's requirement for not interfering with standard technical measures does not always yield a simple or readily apparent analysis. For instance, in *CCBill*,[159] the court had to determine whether access to a website, which was impeded by password-protected websites,

---

155. *See* 17 U.S.C. § 512(i)(1)(B) (2000).

156. Transcript of Cross-Examination of Gary Millin, BMG Canada et al. v. John Doe, 2005 FCA 193, Court File No. T-292-04, question and answers 75, 96, 178-179, 200-03, *available at* http://www.ilrweb.com/viewILRPDF.asp?filename=bmg_doecanada_millindeposition (explaining that MediaSentry's technology for searching for infringing material ran on top of standard peer-to-peer file sharing applications).

157. MediaSentry appears to have changed their company name to SafeNet but retain the product name MediaSentry to describe their services. Since the information cited regarding the company's techniques refer to MediaSentry, that name will be used throughout in order to preserve accuracy.

158. *See, e.g.*, SafeNet Website / Media Sentry, http://www.safenet-inc.com/products/sentinel/mediasentry_intellectual_property_protection.asp (last visited Nov. 15, 2007); Transcript of Cross-Examination of Gary Millin, BMG Canada et al. v. John Doe, Court File No. T-292-04, question and answers 75, 96, 178-179, 200-03, *available at* http://www.ilrweb.com/viewILRPDF.asp?filename=bmg_doecanada_millindeposition.

159. *See supra* Section III.A.2.

was a "standard technical measure" with which CCBill was required not to interfere. In order to protect access to its hosted content, and thus gain income by selling subscriptions, CCBill facilitates a process of password-protecting websites and then uses its financial transaction system to grant access to those who pay. These sites are, in what is otherwise a commercially reasonably way, blocking access to their internal content.[160] In *CCBill*, the plaintiff Perfect 10, Inc., argued that this type of system interfered with its standard technical measures for identifying infringing material because it could not determine whether CCBill affiliated websites contained infringing material.[161]

The *CCBill* court remanded to determine whether "access to a website" constitutes a standard technical measure.[162] Although it is likely that the lower court will hesitate to conclude that any service provider password protecting some of its hosted material automatically waives its safe harbor immunity, each side of the argument has interesting merits that will be discussed in the following Section.

2. Accessing Protected User-Content in a Web 2.0 Environment

The question of whether or not access to online content is a "standard technical measure" also arose in the recent complaint filed against Google and YouTube by media conglomerate Viacom.[163] In its complaint, Viacom claimed that YouTube interferes with standard technical measures in two ways. First, YouTube allows users to restrict access to content that they post.[164] In other words, a user may upload a video and then only allow his or her "friends" to access it.[165] According to YouTube, this restriction is intended to be a privacy measure that enables users to retain control over who views their videos.[166] For instance, it allows users to both post family

160. These sites function on a pay-to-view system. They are not interfering with technical measures so much as they are protecting access to something that requires paid admission to enter. Movie theaters do not block standard technical measures simply because they require a ticket to enter.

161. *See* Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1115 (9th Cir. 2007).

162. *Id.*

163. Complaint at 1-9, Viacom Int'l v. YouTube, Inc., No. 1:07CV02103, 2007 WL 775695 (S.D.N.Y. Feb. 30, 2007).

164. *Id.* at 16.

165. I place friends in quotes to emphasis the important distinction between "real" friends and friends in a virtual community: the widespread, anonymous nature of internal circles of "friends" on YouTube contrasts greatly with the smaller scale infringement that would be possible in an actual, personal circle of friends.

166. YouTube: How Do I Make My Video Private?, http://www.google.com/support/youtube/bin/answer.py?answer=59208&topic=10519 (last visited Dec. 1, 2007);

videos and protect the privacy of those depicted in personal videos. It is one of many steps taken by Web 2.0 websites to protect the privacy of their users while simultaneously encouraging content posting and site growth.[167] However, as alleged in Viacom's complaint, these privacy settings may also have the side effect of creating hidden caches of infringing material.[168] Since the material is effectively hidden from all but the allowed users' searches, copyright owners and their agents who are searching the site for infringing content will unable to access potentially infringing material.

In addition to permitting users to restrict access, YouTube also offers a search function allowing visitors to search through the descriptions of posted videos in order to locate and watch specific types or genres of content.[169] Likewise, copyright owners also use the search feature to identify intellectual property present on YouTube. However, the search function on YouTube has been crippled in a way that Viacom contends interferes with the standard technical measures available to copyright owners: it returns only the first 1,000 video clips matching any search query, making it much less effective for Viacom's policing efforts.[170] Furthermore, Viacom alleges in its complaint that this was only a recent change to the search functionality, thus implying that the limitation may be more of a selective than a technical restriction.[171] Viacom claims that the addition of this limitation prevents it from identifying all infringing material on any given website because it will never be able to explore beyond 1,000 files containing certain key terms.[172]

Given the widespread use of passwords and other privacy features for protecting both user-generated and publisher-generated content, a holding

---

YouTube: Who Can See My Private Video?, http://www.google.com/support/youtube/bin/answer.py?answer=57739&topic=10519 (last visited Dec. 1, 2007).

167. *See, e.g.*, Christi Cassel, Note, *Keep out of MySpace! Protecting Students from Unconstitutional Suspensions and Expulsions*, 49 WM & MARY L. REV. 643 (2007); Jennifer Epstein, *Who's Reading Your Facebook*?, DAILY PRINCETONIAN, http://www.dailyprincetonian. com/archives/2006/02/10/news/14416.shtml (Feb. 2, 2006).

168. Complaint at 16-17, Viacom Int'l v. YouTube, Inc., No. 1:07CV02103, 2007 WL 775695 (S.D.N.Y. Feb. 30, 2007).

169. *Id.* at 10-11.

170. *Id.* at 16.

171. *Id.* at 16. The allusion in the complaint is that this functionality is not the result of some technical limitation, but is an intentional attempt to limit copyright enforcement on YouTube.

172. The author of this Note was able to search the entire contents of the YouTube site at the time of writing. *See supra* note 41. It is unclear whether this represents an inaccuracy in the Viacom complaint or a technical change made by YouTube.

that access to a website constitutes a "standard technical measure" could be catastrophic. If these access restrictions are found to be an interference with standard technical measures, many OSPs will be forced to remove them in order to retain their DMCA safe harbor immunity. As a result, user privacy will become an even more challenging issue: how will OSP's protect the identities of their users and the privacy of their user's content if they cannot prevent access? Further, will social networking sites—already challenged by privacy advocates to grant users control over who can see their profiles and content—become an amusement of the past as users flee, fearing that their personal information will be viewable by all?[173]

On the other hand, a decision finding that access is not a standard technical measure, however, may seriously erode the scope of "standard technical measures" and further restrict the copyright owner's ability to police the Internet for infringing uses of his own content. The potentially infringing material in question lurks behind virtual locked doors, hidden from the view of the copyright owners. The availability of civil policing methods to access the content (e.g., a subpoena) fail to be useful when the copyright owner can only contemplate that infringement might be occurring, but cannot be certain where, when, how, or even if it is at all. Complete opacity is possibly the most obvious problem that a complete burden shift creates when implemented. Traditionally, copyright owners deal with opacity by simply ignoring it.[174] Although they pursue copyright infringement when it is visible, open, and notorious, they ignore it when it is secured behind closed doors. The rational basis for this behavior may be found in an economic argument: if copyright infringement is performed behind closed doors, where access by anonymous users (and copyright owners disguised as the same) is heavily limited, then the damages of the infringement must necessarily be limited as well.[175] Put another way, the relative illegality and damages of online copyright infringement are inversely correlated with the level of anonymity that the users accessing it retain. The more identification and credentials that must be acquired to view the infringing content, the less likely it is that the distribution is widespread. The less widespread the distribution, the less actual damages exist.

---

173. *See supra* note 167 and accompanying text.

174. *See generally* Transcript of Deposition of Gary Millin, BMG Canada et al. v. John Doe, Court File No. T-292-04, *available at* http://www.ilrweb.com/viewILRPDF.asp?filename=bmg_doecanada_millindeposition (last visited Nov. 15, 2007) (stating that infringement detection technology only sought to find file-sharing on known peer to peer networks).

175. *See supra* note 167 and accompanying text.

Applied to the current *YouTube* controversy, the most damaging infringing content is the videos that are posted openly, meaning those posted without the aforementioned privacy restrictions. Thus, paradoxically, by potentially interfering with "standard technical measures," the privacy controls are also actively engaged in limiting the damages caused by the inherent posting of infringing content on a Web 2.0 site.

Certainly, this analysis does not imply that hiding material behind layers of access requirements exculpates the infringement. However, it does create a unique situation where a balance between copyright owners and end-users may be properly sought and is almost naturally present. Privacy concerns weigh heavily on one side of that balance, joined by a general concern for the protection of the Web 2.0 schema. As discussed above, user interaction and contribution on networking sites will drop significantly if users are not able to protect some of their content from the eyes of employers, family members, or undesirables.[176] The Constitutionally mandated duty to promote the useful arts and sciences represents the other side.[177] Because copyright enforcement serves an important role in the encouragement of creative endeavors, the potential impact of the unauthorized dissemination of protected materials over the Internet could be disastrous. Part IV will take this balance into account when examining the possibility of a burden shift in online copyright infringement detection.

IV. RECOMMENDATIONS

Written in 1995, the DMCA made it clear that OSPs should not have the burden of policing their own servers.[178] The DMCA was written in response to concerns that a requirement for OSPs to police their own servers would cripple OSP activity, prohibitively raise the costs of doing business on the Internet, and greatly restrict the First Amendment rights of their users.[179] Thus, in an attempt to shift the burden to the least-cost-avoider, Congress held strong to the tradition that a copyright owner should bear the complete burden of policing infringing material.[180] However, secondary liability provided a reservation: Online service providers who induce infringement or profit directly from infringement are liable for copyright infringement. In its various provisions, the DMCA addresses these de-

176. *See supra* note 167 and accompanying text.
177. U.S. CONST. art. I, § 8, cl. 8.
178. *See supra* note 54 and accompanying text.
179. *Id.*
180. *See* S. REP. No. 105-190, at 8 (1998).

fenses by offering what are solely binary rules: do not profit directly, do not have knowledge, and do not block access.[181]

Web 2.0 environments blur these binary environments.[182] It is unclear when an OSP hosting user-generated content is profiting directly from copyrighted material. Further, what happens when an OSP simultaneously profits from user-generated content and yet does not have actual knowledge under the DMCA that it is doing so? Given these concerns, the requirements should be modified. Although the rationale behind the DMCA and its safe harbor provisions is sound in that it simplifies the process of categorizing online service providers and allows a relatively easy determination of where immunity falls, the binary categorization it employs does not adequately reflect the nature of the Internet as it stands now, with Web 2.0 applications, nor how it will stand as it develops further. In order to more adequately address growing technology, this categorization requires more flexibility.

The judicial gateways governing the term "direct financial benefit" have closed tightly around that term, requiring that the infringing material reflect a primary draw to an OSP's customers. This inflexibility might be attributed to the fact that finding such a benefit immediately removes immunity for OSPs that would not be otherwise protected. These two concerns must be taken together when adjusting the statutory language. As such, the author of this Note proposes: 1) changing the term "direct" to "substantial" and 2) appending that requirement with a proviso. The term "substantial" more adequately reflects the behavior of Web 2.0 environments, where several different features work together to attract users. It also adequately addresses the situations (e.g., YouTube) where the site derives substantial profit from infringing material, but where the infringing material may not represent (or is difficult to prove) a "direct" draw to customers.

As noted above, a proviso is required in order to achieve an appropriate balance in this situation. As explored in Section III.A.2, a burden-shift in liability away from copyright owners may be more technically and economically feasible in the pursuit of online infringing material. However, lowering the amount of financial benefit an OSP receives will do nothing but seem like an arbitrary shift. Thus, hand-in-hand with the "substantial" term, there must be a non-binary category, a legal gray area which will allow the judiciary to adapt its application to each new technology it faces.

---

181. Binary in the technical sense. It is either "on" or "off," "yes" or "no."

182. *See generally supra* Sections III.A.2, III.B.2, III.C.2.

If a copyright owner is able to prove that an OSP is receiving a substantial financial benefit from infringing material, then he will have effectively raised a question of affirmative duty on the OSP. In order to move the OSP fully out of the safe harbor protection, the copyright owner will be required to prove that the OSP would not be unduly burdened by implementing certain technological features and thus has not failed to take "good faith" efforts to prevent copyright infringement on its servers.

This standard will require an analysis of several elements of the OSP's business model. It should allow for more flexibility around other concerns explored above, including a showing of whether an OSP has intentionally kept itself from becoming officially aware of infringement and whether it has taken technical measures to restrict access to material. Based on the analyses above, the following elements should be examined in the process:[183]

- Amount of income derived from infringing material
- Amount of damages caused by copyright infringement on OSP's servers
- Amount of properly-constructed notices received and processed by OSP
- Percentage of OSP's hosted content that is infringing
- Popularity of infringing hosted content in comparison with OSP's other content
- Technological sophistication of the OSP's systems[184]
- Presence of existing technology to perform adequate filtration and availability of that technology to the OSP in question
- Efforts by OSP to prevent detection of infringing activity by copyright owners[185]

In many ways, these elements are drawn from the same theory of online infringement posited in Section III.C.2, *supra*. When anonymous and widespread, copyright infringement is more dangerous than smaller and more private infringement.[186] In cases of widespread infringement on extremely popular websites, these balancing factors will weigh heavily against the OSP: they tend to profit more significantly, they cause more damage, and are presumed to have received more notice. In those cases,

183. This list is intended to be illustrative, not exhaustive.

184. Compare, for instance, the technical complexity and sophistication of Google, with the relatively layman-ship of an open-source blog with comments enabled (thus presumably inviting potential third-party infringement).

185. *See supra* Section III.C.2.

186. *See id.*

likewise, it is more reasonable to expect that the OSP might have the resources to implement filtering systems where possible. Smaller cases of infringement, such as servers hosting online "blogs" or low-level commercial websites, will retain their immunity because a burden-shift would likely put them out of business and because the damage caused by the infringement hosted on their servers is not substantial enough to justify that result.[187] However, the copyright infringement aggregated across many of these small sites may still amount to substantial damages. Importantly, this proposal does not offer such sites immunity, but only an exception from having to independently develop filtering technologies. The existing DMCA provisions of notice and takedown, as well as the possibility that such sites could be receiving a "direct financial benefit," will still protect copyright owners from undue infringement.

Although implicated in elements listed above, the DMCA's other bright-line standards do not necessarily need to be changed by the proposed amendment. Just as before, actual knowledge of infringement accompanied by inaction certainly should repeal immunity, as should the direct blocking of standard technical measures used to detect infringing material (i.e., contributing to the infringement directly). However, since the basis of a burden adjustment is necessarily in the economics of more feasible solutions, it seems appropriate that the "financial benefit" requirement be located where this balancing test is nested.

V. CONCLUSION

In conclusion, Web 2.0 websites, particularly those heavily involved in publishing user-generated content, have created a noticeable change in the way the Internet is used to disseminate information. New material is posted nearly every second. Some of that information, however, is copyrighted and used without permission. It is extremely difficult for copyright owners to keep up with this flow of information in order to protect their constitutionally-granted rights.

The root of these difficulties lies in the fact that the DMCA's safe harbors require an analysis that draws a bright line where there should be a dim one. Technology advances far too quickly and far too unexpectedly to wait for Congress to pass new versions of the DMCA, and so the judiciary is left to struggle with language that does not map properly onto the art.

187. *See id.* Small businesses who cannot adequately develop filtering technology would not survive the prospect of liability. The "direct financial benefit" analysis should play a role in the legal resolution of this issue in order to prevent such an unfortunate circumstance.

Additionally, given advances in technology, the copyright owner may no longer be the least-cost-avoider for detecting infringement online. In a Web 2.0 scheme, the possibility that technology can be used to filter out some infringing material is great and, in some cases, economically efficient. The current binary system of the DMCA's requirements does not allow for an adequate determination of that efficiency, and so a balancing test must be implemented in order to allow for an economical and just balance of the burden for preventing copyright infringement.