SAFE HARBORS UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

*Mike Scott**

INTRODUCTION

It has been nearly a decade since the appearance of the first draft legislation that would later become the Digital Millennium Copyright Act (DMCA).[1] The prime movers behind the initial bills touted them as providing an essential foundation for the robust development of the "Information Superhighway"—rechristened the more businesslike "National Information Infrastructure."[2] Congress recognized that this legal foundation needed to strike a delicate balance.[3] On the one hand, there was concern that the "online service providers" (OSPs) that were providing the new technology might become so fearful of incurring liability that they would be reluctant to invest in the sort of technological experimentation and innovation that would ultimately enhance the public benefits of the digital environment.[4] On the other, there was the danger that copyright holders would refuse to make works available online at all unless they were assured of adequate protection of their exclusive rights.[5]

Congress hoped that the DMCA could achieve the proper balance by creating strong incentives for OSPs and content owners to cooperate in an effort to "ensure[ ] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the

* J.D. 2005, New York University School of Law. I would like to thank Niva Elkin-Koren, Diane Zimmerman, George Kuzmowycz, Dan Scott, James Temple, and my classmates in the spring 2005 Colloquium on Innovation Policy for their advice and suggestions regarding this Note and my approach to it. I would especially like to thank my wife, Nalini, and son, Krishnan, for their love, support and patience while I wrote it. All errors and omissions are mine alone.

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

2. *See* S. REP. NO. 105-90, at 1–2 (1998).

3. Indeed, the legislative history is replete with references to this concern. *See, e.g.*, S. REP. NO. 105-190, at 21, 49, 69; H.R. REP. NO. 105-551, pt. 2, at 21, 24–26, 58–59 (1998).

4. S. REP. NO. 105-190, at 8.

5. *Id.*

Internet will expand."[6] One of the central elements in this balance was a system of statutory "safe harbors"—a set of provisions allowing OSPs to immunize themselves from liability for infringement by taking certain specific steps to cooperate with copyright holders in enforcing their rights.[7]

Ten years later, however, it is by no means clear that the statutory safe harbors are having the effect their creators envisioned. One reason may be that the DMCA's drafters, in their efforts to achieve "certainty" in the area of online copyright liability,[8] chose to focus on the particular OSP activities and functions that seemed especially problematic in 1995.[9] These activities were used both to determine whether a particular entity fell within the class of protected OSPs in the first place, and to serve as a proxy for their willingness to cooperate with copyright owners.

The DMCA's heavy emphasis on the particular technology that existed at the time the law was drafted has had two seemingly divergent effects on online copyright enforcement. First of all, by dealing so narrowly with specific tasks of network operation and copyright compliance, the statute created a set of lopsided incentives for OSPs, motivating them to remove online material as soon as it is questioned by anyone so much as claiming to be a copyright holder.[10] At the same time, the DMCA's regime offers OSPs engaged in the design or modification of a digital network little motivation to shape that design in ways tending to reduce infringing behavior by its customers.[11]

These problems were not unavoidable. In fact, the safe harbors represented a major turnaround from the initial recommendations of the White House's Working Group on Intellectual Property (Working Group), which had concluded that such sweeping immunity for OSPs would be a bad thing: "It would be unfair—and set a dangerous precedent—to allow one class of distributors to self-determine their liability by refusing to take responsibility. This would encourage intentional and willful ignorance."[12] The reversal came about because OSPs were powerful enough to force copyright owners and policymakers to ac-

6. *Id.* at 2.
7. 17 U.S.C. § 512 (2000).
8. *See id.* at 2, 20.
9. *See infra* Part IV.
10. *See infra* Part III.
11. *See infra* Part IV.
12. INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 122 (1995) [hereinafter WORKING GROUP REPORT].

knowledge that no law governing online copyright liability could long be effective if it were promulgated without their input and support. A series of intense negotiations among these groups eventually led to a compromise that no one could have foreseen at the outset.[13]

A handful of recent cases suggest that the safe harbors are interacting with the online environment in ways Congress did not foresee. For one thing, the safe harbors utterly failed to accommodate perhaps the most explosive online media application today: the peer-to-peer networks created by Napster and its successors. As the courts have weighed the fate of Grokster in a hugely important series of decisions on the application of digital copyright to one of today's most important classes of OSP, the DMCA has proven to be nearly irrelevant to the outcome.[14] Meanwhile, OSPs innovate and consolidate with abandon, reinventing themselves in a breathtaking variety of ways, and providing services that were completely unknown in 1995.

At the same time, there is mounting evidence that the Working Group's concern that an immunity regime might create a perverse set of incentives may have been prescient, though not necessarily for the reasons the Group suggested. Two recent cases, albeit with different results, suggest some of the unexpected problems raised by the safe harbors. First, in September 2004, Diebold, Inc. became the first copyright "complainant" found liable under the DMCA for abusing the safe harbors in order to suppress non-infringing speech.[15] The company had nearly succeeded in suppressing embarrassing revelations about bugs in its computerized voting machines by falsely claiming that a collection of damning email messages were copyrighted and directing OSPs to remove the messages from the Internet, in accordance with safe harbor eligibility requirements. Second, on May 2, 2005, the Supreme Court declined to hear the case of a website operator who claimed that the Motion Picture Association of America had acted wrongfully when it used the safe harbor provisions to shut down his site, even though a brief investigation would have revealed that the site contained no copyrighted material or links. The Court's decision to deny certiorari lets stand the Ninth Circuit's holding: the DMCA shields copyright owners from liability for shutting down innocent

13. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 134–36 (2001) (discussing negotiations which took place once content owners recognized that "the legislation could not move without a solution to the problem of internet service provider liability").

14. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005), *rev'g* 380 F.3d 1154 (9th Cir. 2004).

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

sites by mistake "even if the copyright owner acted unreasonably in making the mistake."[16]

Part I of this Note reviews the development of direct and secondary liability theories for copyright violations, with particular emphasis on the application of the theories of vicarious and contributory liability to the providers of online digital services. Part II reviews the rationales, as expressed by Congress and copyright stakeholders at the time the DMCA was drafted, for creating the safe harbors for OSPs, and explains the process by which the statutory provisions were created. Part III examines evidence that the safe harbors have had a dramatic and possibly dangerous impact on the ways in which OSPs view their relationships with their customers—specifically, that the promise of immunity from liability has frequently led OSPs to err on the side of removing content, in the process potentially suppressing the legitimate speech of their users. Part IV argues that the safe harbors may not be a much better deal for copyright holders; OSPs are in fact engaging in a widening variety of activities that could be considered contributorily (or even directly) infringing, and the assumption that after-the-fact cooperation with copyright owners is sufficient reason to shield OSPs from all liability has not been sufficiently scrutinized. Two recent cases, *Online Policy Group v. Diebold, Inc.*[17] and *CoStar Group, Inc. v. Loopnet, Inc.*,[18] will be used to illustrate many of these ideas. Finally, Part V examines some options for modifying the existing regime of near-total immunity for OSPs provided by the safe harbor regime.

I.
Theories of Liability for Online Service Providers

A. Direct Liability

Section 106 of the Copyright Act lays out a set of exclusive rights granted to authors of new works. These include the right to reproduce, perform, display, or distribute a work, among others.[19] Individuals who perform any of these acts without the authorization of the copyright holder have directly infringed the corresponding exclu-

16. Rossi v. Motion Picture Ass'n of Am., 391 F.3d 1000, 1005 (9th Cir. 2004), *cert. denied*, 125 S. Ct. 1977 (2005).
17. 337 F. Supp. 2d 1195.
18. 373 F.3d 544 (4th Cir. 2004).
19. 17 U.S.C. § 106 (2000).

sive right, and are considered direct infringers.[20] Direct infringement is generally considered a strict liability offense: knowledge and intent need not be present for liability to be found,[21] though their absence may serve to mitigate damages.[22]

The problems raised by a strict application of direct liability principles to the digital context were thrown into stark relief by cases such as *MAI Systems Corp. v. Peak Computer*, *Inc*.[23] *MAI* concerned a claim by a computer manufacturer that a third-party maintenance provider had directly infringed its copyrights merely by turning on a customer's computer, causing it to automatically load the manufacturer's properly licensed software. The plaintiff's theory was that a copy was made in temporary RAM each time the computer rebooted; while the customer was licensed to use the program in this way, the third-party maintenance company was not, and by causing the copy to be made, had directly infringed.[24] A Ninth Circuit panel found for MAI, holding that an additional copy of a work was fixed each time it was loaded into even the *temporary* memory of a computer.[25]

This principle was applied specifically to an Internet access provider a few years later in *Marobie-FL, Inc. v. National Ass'n of Fire Equipment Distributors*,[26] in which the court held that "[t]he fact that a copy is transmitted after it is created, or even as it is created, does not change the fact that once an Internet user receives a copy, it is capable of being perceived and thus 'fixed' " for purposes of assessing infringement liability.[27]

Given the volume and logistics of communications on the Internet, however, many courts and commentators have been uneasy with the idea of holding all OSPs strictly liable for acts committed by

20. 17 U.S.C. § 501(a) (Supp. II 2003) ("Anyone who violates any of the exclusive rights of the copyright owner as provided by section[ ] 106 . . . is an infringer of the copyright or right of the author . . . .").

21. *See, e.g.*, ABKCO Music, Inc. v. Harrisongs Music, Ltd., 722 F.2d 988, 998 (2d Cir. 1983) (upholding district court finding of "subconscious copying"; "innocent copying can nevertheless constitute an infringement . . . . It is settled that intention to infringe is not essential . . . .") (internal quotations omitted); Olan Mills v. Linn Photo Co., 795 F. Supp. 1423, 1437 (N.D. Iowa 1991), *rev'd on other grounds*, 23 F.3d 1345 (8th Cir. 1994) ("No scienter need be shown to prove infringement.").

22. *See, e.g.*, *Olan Mills*, 795 F. Supp. at 1437 ("Intent is relevant only to the decision whether or not to increase damages.").

23. 991 F.2d 511 (9th Cir. 1993).

24. *See id.* at 517–18.

25. *Id.* at 518 ("a 'copying' for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM").

26. 983 F. Supp. 1167 (N.D. Ill. 1997).

27. *Id.* at 1178 (emphasis omitted).

their subscribers without their knowledge[28] and have suggested that alternative approaches are needed. Attention has therefore also been focused on theories of secondary infringement liability.

B. Secondary Liability

The law of copyright provides that liability for infringement may attach not merely to instances where "the defendant himself violated one or more of the plaintiff's exclusive rights,"[29] but also to acts of parties who did not "tak[e] part in the final act" of infringement.[30] Such secondary liability may attach provided that the acts occurred in the context of an "ongoing relationship" between a direct infringer and a non-acting party who "was in a position to control the use of copyrighted works by [the infringer]."[31] Two types of secondary liability are generally recognized in copyright: contributory infringement and vicarious liability. *Contributory infringement* may exist if a party with knowledge of another party's infringing conduct has materially contributed to that conduct.[32] *Vicarious liability* is often associated with an employment or other relationship to which the doctrine of *respondeat superior* applies; the defendant must have enjoyed a financial benefit from the infringing conduct of another person whose infringing conduct the defendant had the "right and ability to supervise."[33]

Neither of these doctrines is expressly articulated in the Copyright Act of 1976. While the legislative history of the Act suggests that Congress added the words "to authorize" to the list of exclusive rights granted to holders of copyrights by Section 106 in order "to avoid any questions as to the liability of contributory infringers,"[34] the

28. *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1002 (1994) (making bulletin board service (BBS) operators liable for infringing files uploaded by subscribers "seems to impose a near-impossible burden on them" although "scienter is not a normal requirement of copyright infringement"). Hardy later concludes, however, that strict liability is "an appropriate outcome" in copyright cases. *Id.* at 1047.

29. Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004).

30. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 436 (1984) (quoting Kalem Co. v. Harper Bros., 222 U.S. 55, 63 (1911)).

31. *Id.* at 437.

32. *Ellison*, 357 F.3d at 1076.

33. *Id.* (internal quotations omitted).

34. H.R. REP. NO. 94-1476, at 61 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 5659, 5674; *see also* 17 U.S.C. § 106 (2000).

doctrines of secondary liability have primarily evolved under the direction of the courts.[35]

Vicarious liability cases tend to be decided on the basis of analogy to other areas of the law. They are often judged by whether they more closely resemble "landlord-tenant" cases, in which landlords who lack knowledge of infringing acts by tenants and exercised no control over leased premises are held not liable, or "dance hall cases," in which venue operators can be held liable for infringing performances on premises that they could control and from which they received a direct financial benefit.[36]

The paradigmatic contributory infringement cases are "flea market" cases, such as *Fonovisa*. In *Fonovisa*, the operators of a swap meet, aware that vendors participating in the meet were selling counterfeit recordings (thus satisfying the "knowledge" requirement), contributed support services without which the direct infringement would have been severely curtailed or prevented completely (thus satisfying the "material contribution" requirement). The operators were therefore held contributorily liable to the owners of the copyrights in the recordings.[37]

C. Sony-Betamax *and the Staple Article of Commerce Doctrine*

Whatever the merits of these approaches in the context of dance halls or flea markets, courts have had some difficulty applying the same rationales to the actions of device manufacturers or OSPs.[38] One important result of these struggles was the application of patent law's "staple article of commerce" doctrine to copyright in *Sony Corp. of America v. Universal City Studios, Inc. (Sony-Betamax).*[39] In an opinion by Justice Stevens, the Court held that a manufacturer of equipment capable of "substantial non-infringing use" could not be

35. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996) ("Although the Copyright Act does not expressly impose liability on anyone other than direct infringers, courts have long recognized that in certain circumstances, vicarious or contributory liability will be imposed."); *see also* WORKING GROUP REPORT, *supra* note 12, at 109 (1995); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 396 (2003).

36. *See Fonovisa*, 76 F.3d at 262 (citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304 (2d Cir. 1963)).

37. *Id.* at 264.

38. *Cf.* LITMAN, *supra* note 13, at 67–68 n.22 (arguing that "[c]ourts have struggled," because "fact-specific provisions of the statute do not contemplate such exotic creatures" as VCRs, satellites, software, databases, and the Internet).

39. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434–35, 442 (1984).

held contributorily liable for copyright infringement solely because it had sold equipment to the general public which some customers had used to infringe.[40]

Although *Sony-Betamax* was decided well before the advent of online services, the case is central to any discussion of the secondary liability of OSPs two decades later. There are, of course, clear distinctions between the two situations. The asserted basis for contributory liability in *Sony-Betamax* was the manufacture and sale by Sony of equipment (*i.e.*, VCRs) that could be used to infringe copyrighted works, namely broadcast television programs.[41] This meant, among other things, that there was no "ongoing relationship between the direct infringer and the contributory infringer at the time the infringing conduct occurred."[42] By contrast, many disputes in the online context arise from the services provided by OSPs as part of an *ongoing* relationship with an alleged direct infringer.

This distinction does not necessarily mean, however, that the Court's rule in *Sony-Betamax* should not apply to service providers as well as equipment manufacturers. Indeed, the rule the majority applied in *Sony-Betamax* was itself "borrowed" from the law of patents, yet the Court found sufficient commonality in the problem of appropriately protecting both devices and publications to justify applying the same rule to each.[43] More importantly, the Court plainly recognized that *either* "products or activities"[44] could contribute to the unlawful duplication of devices or publications. It would therefore be natural for the *Sony-Betamax* holding to apply to OSP services as well. The case falls well short of providing a bright-line rule for assessing contributory or vicarious liability in all circumstances. Still, its holding that the mere sale of devices capable of infringing use "does not [by itself] constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes,"[45] is clearly relevant to discussions of the liability of OSPs engaged in either the

40. *See id.* at 442 ("[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."); *id.* at 456 ("The Betamax is, therefore, capable of substantial noninfringing uses. Sony's sale of such equipment to the general public does not constitute contributory infringement of respondents' copyrights.").

41. *Id.* at 420.

42. *Id.* at 437.

43. *Id.* at 442.

44. *Id.*

45. *Id.*

one-time sale of software "devices"[46] or the provision of online access or other ongoing services.[47]

On the other hand, *Sony-Betamax* was a very close decision, and some of the objections raised by Justice Blackmun's dissent also have great force in the online context. For instance, the dissent reminds us that "a finding of contributory infringement has never depended on actual knowledge of particular instances of infringement,"[48] or on the defendant's "aware[ness] that the infringing activity violates the copyright laws."[49] Justice Blackmun also matched the majority's extrapolation from patent law with one of his own, suggesting that the Court's apparent approval in *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*[50] of a lower court's decision to hold a manufacturer contributorily liable for trademark infringement for even *implying* that its products could be used to infringe,[51] applied equally in the copyright context.[52] He went on to point to marketing materials promoting the recording of "favorite shows" and "classic movies" with no warning that those activities were potentially infringing as proof that "Sony has induced and materially contributed to the infringing conduct."[53] Most significantly, the dissent suggested that a defendant should only be able to

46. *See* A&M Records v. Napster, 239 F.3d 1004, 1020–21 (9th Cir. 2001) ("We are bound to follow *Sony*, and will not impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights.") Of course, the court later concluded that Napster did, in fact, have actual or constructive knowledge of its users' infringements. *Id.* at 1021. *See also* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1161–62 (9th Cir. 2004), *rev'd*, 125 S. Ct. 2764 (2005) (holding that "the software distributed by each defendant was capable of substantial noninfringing uses" and that *Sony-Betamax* therefore applied); RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000) (analyzing distribution of software tools under *Sony-Betamax*, but concluding that, because tools circumvented technological measures for controlling access in violation of § 1201, they were "not entitled to the same 'fair use' protections the Supreme Court afforded . . . in [*Sony-Betamax*]").

47. *See, e.g.*, *In re* Aimster Copyright Litig., 334 F.3d 643, 647–49 (7th Cir. 2003) (rejecting argument that *Sony-Betamax* did not apply to services); *see also* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1873–74 (2000) (explaining that "*Sony* seems fully applicable to the provision of Internet service," but also concluding that "[t]he requisite level of knowledge, therefore, makes the imposition of contributory liability for the simple provision of Internet services highly unlikely").

48. *Sony*, 464 U.S. at 487 (Blackmun, J., dissenting). Joining Justice Blackmun were Justices Marshall, Powell, and Rehnquist.

49. *Id.* at 489.

50. 456 U.S. 844 (1982).

51. *Id.* at 851–52.

52. *Sony*, 464 U.S. at 489.

53. *Id.* at 489–90.

evade secondary liability where a *significant* portion of a product's use is *non-infringing* and not in cases where "no one would buy the product for noninfringing purposes alone, [and] it is clear that the manufacturer is purposely profiting from the infringement."[54] According to the dissent, the majority's view that the *capability* for significant non-infringing use alone was sufficient to immunize Sony "essentially eviscerate[d] the concept of contributory infringement."[55]

Of course, the dissent's arguments did not win the day, and the staple article of commerce doctrine remains vital today. Nevertheless, many of the arguments asserted by the content industries in recent peer-to-peer networking cases echo the *Sony-Betamax* dissent's claim that the mere fact that an article was "capable" of substantial non-infringing use should not eliminate the possibility of contributory liability for its manufacturer or distributor.[56] The current debate, however, centers not on whether the staple article of commerce doctrine should be abandoned altogether, but rather on the details of how much non-infringing use must be actual, as opposed to hypothetical. This view was clearly reflected in the oral arguments before the Supreme Court in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* case, in which several Justices questioned both parties about the relative levels of infringing and non-infringing use that *Sony-Betamax* should require.[57] The Court ultimately held that the protection afforded by

54. *Id.* at 491.

55. *Id.* at 498.

56. *See, e.g.*, Reply Brief for the Petitioner on Petition for Writ of Certiorari at 3, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005) (No. 04-480) ("Grokster and StreamCast are flat wrong in their claim that *Sony-Betamax* applied a 'mere capability' standard for commercially significant noninfringing uses and prohibited examination of the actual proportion of infringing and noninfringing uses."); Brief of Plaintiffs-Appellees at 24, *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003) (No. 02-4125), 2003 WL 22330732.

> [Appellant] attempts to avoid this indisputable fact by positing an interpretation of Sony-Betamax that *would eviscerate the doctrine of contributory infringement*. Under [Appellant's] theory, even though he did not provide any evidence of actual noninfringing use, he would escape liability merely because he could hypothesize a possible future noninfringing use for the Aimster system.

Id. (emphasis added).

57. *See, e.g.*, Transcript of Oral Argument, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005) (No. 04-480), *available at* http://www.supremecourtus.gov/oral_arguments/argument_transcripts/04-480.pdf. For example, Justice Scalia questioned, "How much time do you give [a new inventor] to bring up the lawful use to the level where it will outweigh the unlawful use?" *Id.* at 12. Also, Justice Souter stated, "Well, there's never evidence [of the relative proportions of infringing and lawful use] at the time the guy is sitting in the garage figuring out whether to invent . . . ." *Id.* at 15. Several Justices also raised questions apparently aimed at formulating a test that would enable courts to decide when non-infringing

Sony-Betamax to technologies capable of substantial non-infringing uses could be limited—if not by proof of the relative amounts of infringing and non-infringing actual use, then at least by evidence of intent on the part of the provider to induce direct infringement by its users.[58] To the extent the Court's majority opinion deals with the volume question discussed at oral argument, it appears to be primarily in the context of satisfying the requirement that some actual direct infringement be proven as a prerequisite for attaching secondary liability. The Court pointed to the plaintiffs' evidence of direct infringement on a "gigantic" scale merely to satisfy this element,[59] and used evidence that the OSPs had sought to actively induce their users to infringe to deny them protection from secondary liability under the staple article of commerce doctrine.[60] However, six Justices split evenly on the issue of whether the relative volumes of infringing and non-infringing use could alone form a sufficient basis for assigning secondary liability,[61] and it therefore remains unclear whether mere capability for substantial non-infringing use will continue to provide the same degree of protection it has since *Sony-Betamax*.

---

use met the *Sony-Betamax* standard of "substantial." The Solicitor General, arguing in support of the content industry, also viewed the key question as the relative proportions, noting that there "should be no liability under the Sony standard" where infringing use fell anywhere under fifty percent. *Id.* at 23–24.

58. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2780 (2005).

> [T]he inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

Id.

59. *Id.* at 2782.

> [T]he inducement theory of course requires evidence of actual infringement by recipients of the device, the software in this case. As the account of the facts indicates, there is evidence of infringement on a gigantic scale, and there is no serious issue of the adequacy of MGM's showing on this point in order to survive the companies' summary judgment requests.

Id.

60. *Id.* at 2781 (noting that OSPs had deliberately sought "to satisfy a known source of demand for copyright infringement, the market comprising former Napster users," had failed to develop software tools to limit infringement, and had employed business model that derived greatest revenue from high volume, infringing use).

61. *Compare id.* at 2785–86 (Ginsburg, J., joined by Rehnquist, C.J., & Kennedy, J., concurring) (arguing that evidence in record raised genuine issue of material fact as to whether sufficiently substantial non-infringing uses had been shown), *with id.* at 2788–90 (Breyer, J., joined by Stevens, J. & O'Connor, J., concurring) (arguing that evidence of non-infringing uses was at least as strong as it had been in *Sony-Betamax* itself).

D. Applying the Theories to Online Service Providers

The first cases to consider the liability of OSPs for copyright infringement sought to apply these doctrines, developed for a bricks-and-mortar world, to the peculiarities of electronic distribution in cyberspace. The fit was not always a comfortable one.

On the one hand, the nature and speed of online digital communications made it possible—even likely—for a single act of direct online infringement to implicate not just the reproduction right, but also the exclusive rights to distribution, performance, and the right to produce derivative works. The infringing acts themselves were generally executed by equipment or software designed, owned, or operated by the OSP—systems to which the OSP provided access in return for some sort of subscription fee. These facts seemed, to varying degrees, to track many of the elements of direct, contributory, and even vicarious liability. First and foremost, cases like *MAI* and *Marobie-FL* suggested that OSPs could potentially be held strictly liable for each and every separate occurrence of copying or propagation performed by their systems, whether at the instigation of their customers or third parties.[62] Given the volume of traffic already traversing the Internet, and the anticipated growth in that traffic, the potential for direct liability therefore seemed to be staggering.[63]

---

62. *See supra* Part I.A. As part of the basic routing and other communication functions undertaken by many nodes on the Internet, OSPs may be called upon to forward messages that neither originate nor terminate on computers owned or operated by their customers. This situation occurs most commonly for so-called "backbone" providers that link different OSPs to one another, but can affect conventional OSPs as well in cases where their connections provide a convenient "hop" between an unrelated source and destination. *See generally* Curt Franklin, How Routers Work, http://computer.howstuffworks.com/router.htm (last visited Oct. 14, 2005); Roozbeh Razavi, How Routing Algorithms Work, http://computer.howstuffworks.com/routing-algorithm.htm (last visited Oct. 14, 2005); *Border Gateway Protocol*, WIKIPEDIA, http://en.wikipedia.org/wiki/BGP (last visited Oct. 14, 2005).

63. *See, e.g.*, *NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, (1996) (written testimony of Scott Purcell, representing Commercial Internet eXchange Association), *available at* http://judiciary.house.gov/legacy/444.htm (last visited Oct. 29, 2005) ("The staggering size of this obligation is clearer when you realize that CIX members alone transmit millions upon millions of messages each day"); *id.* (statement of Stephen M. Heaton, representing CompuServe, Inc.), *available at* http://judiciary.house.gov/legacy/443.htm (last visited Oct. 29, 2005) (arguing that legal requirement that OSPs police "trillions of bits of data—representing millions of individual messages [that] travel across the country and around the world each day. . . . would result in no less than bringing their businesses to a halt"); *id.* (statement of Roy Neel, representing United States Telephone Association), *available at* http://judiciary.house.gov/legacy/4006.htm (last visited Oct. 29, 2005) ("[U]nder the current state of copyright law, ISPs risk being held liable for massive damages for copyright infringement perpetrated by individuals without the knowledge of the ISP.").

Though opinions were mixed about whether OSPs collected the sort of direct financial benefit from infringement the case law required, there was little doubt that they had the ability to control or deny access to their services by infringers for purposes of vicarious liability.[64] It was clear, too, that OSPs materially contributed to online infringement since it was only through their services that such activities were possible; on the other hand, because of the degree of automation involved, all of this was possible with only the barest minimum of knowledge or direct participation by the OSPs. Thus, the OSP cases rarely resembled any of the paradigmatic cases or met *both* the required elements of either form of secondary liability.[65]

Prior to the passage of the DMCA, the most significant cases dealing specifically with OSP liability for copyright infringement were *Playboy Enterprises, Inc. v. Frena*[66] and *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[67] The cases effectively reached opposite conclusions. The *Frena* court found the operator of a dial-up computer bulletin board service (BBS) directly liable for infringing Playboy's copyrights in photos that were scanned and uploaded to (and downloaded from) the system by other BBS users.[68] The court reasoned that circumstantial proof of copying was sufficient: Frena had access to the works, which were widely published, and the digitized images on his computer were substantially similar.[69] Under the circumstances, since the copies infringed on Playboy's exclusive display and reproduction rights, the court felt Frena's liability was clear.

Netcom, too, involved the operator of a BBS who was sued for copyright infringement because of materials uploaded by a subscriber. The district court analyzed Netcom's liability under direct, vicarious, and contributory theories of infringement. The court's approach to the question of direct liability was largely determined by its conclusion that "Netcom's actions, to the extent that they created a copy of plaintiffs' works, were necessary to having a working system for transmit-

64. *See* WORKING GROUP REPORT, *supra* note 12, at 117 (1995) ("[OSPs] are in the position to know the identity and activities of their subscribers . . . [they] reap rewards for infringing activity").

65. *See supra* Part I.B.

66. 839 F. Supp. 1552 (M.D. Fla. 1993).

67. 907 F. Supp. 1361 (N.D. Cal. 1995).

68. *Frena*, 839 F. Supp. at 1559.

69. *Id.* at 1556; *see also* ABKCO Music, Inc. v. Harrisongs Music, Ltd., 722 F.2d 988, 997 ("'[I]t is well settled that copying may be inferred where a plaintiff establishes that the defendant had access to the copyrighted work and that the two works are substantially similar.'" (quoting Warner Bros. v. Am. Broad. Cos., 654 F.2d 204, 207 (2d Cir. 1981))).

ting Usenet postings to and from the Internet."[70] OSPs such as Netcom, the court held, "do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed."[71] The court acknowledged the principle that strict liability applied to instances of copyright infringement, but felt that the distinction between "the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works" and the question of whether "Netcom has caused the copying" warranted requiring "some element of volition or causation" before finding an OSP directly liable for its subscribers' infringing acts.[72]

The *Netcom* court was plainly concerned about the potential impact of a strict liability rule on the development of the Internet as a whole. It repeatedly expressed the view that rigid application of strict liability "could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet."[73] The *Netcom* court ultimately concluded that such an approach "would hold the entire Internet liable for activities that cannot reasonably be deterred."[74]

The *Netcom* court was more receptive to the notion that an OSP might be contributorily liable for its subscribers' infringing acts. Referencing *Fonovisa*, it noted that the sorts of services OSPs provide their subscribers went "well beyond renting a premises to an infringer," and that such a provider "does not completely relinquish control over how its system is used, unlike a landlord."[75] Thus, the court's holding implies that an OSP that, with knowledge of a subscriber's infringing acts, permits her to persist in the infringing conduct, may be liable for contributory infringement.[76]

On vicarious liability, the court found that, despite the fact that Netcom might have had the ability "to exercise control over the activities of its subscribers,"[77] the lack of any convincing proof that the company received a direct financial benefit from the infringing activities meant that the claim failed.[78] The court also specifically rejected the argument that the OSP's promotions, which offered "regulation-

70. *Netcom*, 907 F. Supp. at 1368.
71. *Id.* at 1369–70.
72. *Id.* at 1368–70.
73. *Id.* at 1372.
74. *Id.*
75. *Id.* at 1375.
76. *See id.*
77. *Id.* at 1376.
78. *Id.* at 1377.

free Internet access," resulted in a direct financial benefit in this context.[79]

Although the debate over OSP liability was far from over, the *Netcom* approach was embraced by other courts, while *Frena* was largely brushed aside.[80] However, before the *Netcom* rule could become settled law, the debate moved to a new forum.

II.
Crafting the Safe Harbors

A. The Working Group Report

The judiciary was certainly not the only arm of the U.S. government pondering the liability of OSPs in the mid-1990s. Shortly after his election, President William Jefferson Clinton formed an Information Infrastructure Task Force (IITF) "to articulate and implement the Administration's vision for the National Information Infrastructure (NII)."[81] The IITF sought to produce "comprehensive telecommunications and information policies and programs" covering a wide range of information policy questions.[82] The IITF also created a Working Group, headed by Patent Commissioner Bruce Lehman, "to examine the intellectual property implications of the NII and make recommendations on any appropriate changes to U.S. intellectual property law

79. *Id.*

80. *See, e.g.*, Sega Enters. Ltd. v. MAPHIA (*MAPHIA II*), 948 F. Supp. 923, 932 (N.D. Cal. 1996). The *MAPHIA II* court even distanced itself from its own earlier finding (reached after *Frena* but prior to *Netcom*) that "Sega [had] established a *prima facie* case of direct copyright infringement" against MAPHIA when the dispute had come before it on Sega's motion for a preliminary injunction. Sega Enters. Ltd. v. MAPHIA (*MAPHIA I*), 857 F. Supp. 679, 686 (N.D. Cal. 1994). In the later opinion, Judge Wilken found the *Netcom* reasoning in favor of requiring volition in assessing direct liability sufficiently "persuasive" to justify rejecting direct liability; though the defendant apparently had knowledge that his BBS was being used for infringement and had even solicited uploading by customers, he had not been shown to have "himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur." *MAPHIA II*, 948 F. Supp. at 932; *see also* Marobie-FL v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1178–79 (N.D. Ill. 1997) (adopting *Netcom* view that contributory liability may be found where OSP had knowledge, specifically citing *Netcom* on issue of absence of direct financial benefit); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 512 (N.D. Ohio 1997) (holding that defendant "must actually engage in" infringing conduct to be held directly liable). More recent cases continue to express a preference for *Netcom*. *See, e.g.*, ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 622 (4th Cir. 2001) (finding *Netcom* "more persuasive" than *Frena*); CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 549–50 (4th Cir. 2004) (explaining why *Netcom* approach is better).

81. Working Group Report, *supra* note 12, at 1.

82. *Id.*

and policy."[83] The Working Group engaged in a series of public hearings and reviewed written comments from the public during 1993–1994, releasing its findings and recommendations in the form of a so-called *Green Paper* in July 1994. After soliciting further public comment, the Working Group finalized its findings and recommendations in a *White Paper* (Working Group Report) in September 1995.[84]

The Working Group Report included a discussion of the Working Group's views on OSP liability for copyright infringement that advocated a less flexible treatment than the one toward which the courts then appeared to be moving. Among other things, it was strikingly unsympathetic to the OSPs' claim that strict liability for the infringements of their subscribers would amount to an unbearable burden. It compared the OSPs' situation to that of film developers, book retailers, and other commercial establishments who, according to the Working Group, were subject to strict liability notwithstanding the practical impossibility of monitoring all of the potentially infringing photographs, books, recordings, and other material they handle, concluding that "this problem has been a part of the cost of doing business for many other distributors of material that is provided to them by others."[85]

The Working Group focused on the OSPs' ability to control their subscribers and concluded that, notwithstanding any difficulties they faced, they were "still in a better position to prevent or stop infringement than the copyright owner."[86] The Working Group noted, too,

---

83. *Id.* at 2.

84. *Id.* at 3–5.

85. *Id.* at 116–17. Whether or not the Working Group's conclusion that these organizations are strictly liable is valid, the case law it cites in support of this proposition is misleading. The Working Group Report cites only Olan Mills, Inc. v. Linn Photo Co., 23 F.3d 1345 (8th Cir. 1994) for the contention that such organizations "operate under strict liability standards." WORKING GROUP REPORT, *supra* note 12, at 116. While the defendant in *Olan Mills* was indeed a developer of photographs, the Eighth Circuit's opinion neither specifically mentions nor alludes to strict liability in any way. Rather, it holds the defendant liable for "clearly infringing acts"—specifically, making copies of photographs bearing plaintiff's clear copyright notices *after* receiving earlier requests from the plaintiff to cease copying its photos. Because it had "actual notice" that its own conduct was infringing, the court held that the developer "could not reasonably rely on [an] indemnification agreement" it developed and required customers to sign "in an effort to circumvent liability." *Olan Mills*, 23 F.3d at 1348. *See also* LITMAN, *supra* note 13, at 96 ("The Lehman Working Group's characterization of extant law was dubious, and the majority of copyright scholars criticized it as skewed."); *id*. at 100 n.19 ("The crux of the criticism was that the Working Group had exaggerated the scope of copyright owners' rights while minimizing users' rights and privileges, and ignoring or mischaracterizing judicial opinions that undermined the Working Group's analysis.").

86. WORKING GROUP REPORT, *supra* note 12, at 117.

that OSPs were a disparate group, with "[d]ifferent service providers play[ing] different roles—and those roles are changing and being created virtually every day," making it impossible to distinguish situations where immunity might be appropriate from those in which it might not.[87] Furthermore, because the industry was undergoing such rapid change, the Working Group Report argued that committing "prematurely" to any program of reduced liability for OSPs might adversely impact the direction of development in the field, "chok[ing the] development of marketplace tools that could be used to lessen their risk of liability and the risk to copyright owners," such as contractual, indemnification or insurance solutions.[88] The Working Group concluded that it would be preferable to leave OSPs subject to incentives that would motivate them to enthusiastically enforce the rights of copyright owners.[89]

B. The Legislative Process

The Working Group Report view of the law shaped the first drafts of digital copyright legislation that Congress considered in 1995 at the urging of the White House.[90] Simultaneously, some of the same principles were incorporated into the texts of the WIPO Copyright Treaty and the Performances and Phonograms Treaty, enabling the congressional proposals to be pitched as implementing legislation "required to institute two international treaties."[91] The Senate Report accompanying the final version of the DMCA explained that Congress wished to "set[ ] a marker for other nations who must also implement these treaties."[92] Whether or not international obligations truly were a motivating force behind the DMCA,[93] it is clear that Congress came to believe the legislation was needed "to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[94]

87. *Id.* at 123.
88. *Id.*
89. *Id.* at 124.
90. *See* H.R. 2441, 104th Cong. (1995); S. 1284, 104th Cong. (1995).
91. Editorial, *Protecting Digital Copyrights*, N.Y. TIMES, July 24, 1998, *reprinted in* 144 CONG. REC. H7093 (daily ed. Aug. 4, 1998).
92. S. REP. NO. 105-190, at 2 (1998).
93. Jessica Litman describes the treaty connection as a tactic adopted by Commissioner Lehman to ensure passage of the Working Group Report's recommendations. When presented with a signed treaty committing the United States to digital copyright protection, "Congress would be obliged to adopt implementing legislation in accord with the [Working Group Report's] recommendations." LITMAN, *supra* note 13, at 129.
94. S. REP. NO. 105-190, at 1–2.

Nevertheless, these first formulations drew "early and fervent objections" from OSPs and other affected groups.[95] This lobbying pressure persuaded Congress to expand the scope of the legislation. In an effort to come up with an approach to service-provider liability that would be acceptable to OSPs and content owners alike, Congress encouraged a series of intense negotiations between those parties. These negotiations ultimately produced the compromise known as the On-Line Copyright Infringement Liability Limitation Act (OCILLA), which became the safe harbor provisions in section 512 of the DMCA.[96] The Senate Report accompanying the DMCA states that OCILLA was intended to "provide certainty for copyright owners and Internet service providers with respect to copyright infringement liability online,"[97] which the House Report labeled "a controversial issue."[98] The legislative history demonstrates particular concern that the disparate outcomes in *Netcom*, *Frena*, and *Marobie-FL* might not have done enough to clarify the law concerning secondary liability of OSPs. With OCILLA, Congress meant to "codif[y] the core of current case law dealing with the liability of on-line service providers, while narrowing and clarifying the law in other respects."[99] The House Report states clearly that the DMCA was intended to endorse the "fair and reasonable" holdings of *Netcom*, which it explicitly characterized

95. LITMAN, *supra* note 13, at 122.

96. Pub. L. No. 105-304, §§ 201–203, 112 Stat. 2860, 2877–86 (1998) (codified at 17 U.S.C. § 512 (2000)). *See* LITMAN, *supra* note 13, at 134–35. Elsewhere in her book, Litman contends that this approach was typical of the way copyright issues had been handled for the past century: since copyright law "seemed too complicated and arcane for legislative revision," the solution had long been for representatives of interested industries to negotiate acceptable compromises and present them to Congress for more or less perfunctory approval. *See id.* at 36, 63. More significantly, she suggests that the hard line articulated in the Working Group Report and early legislative drafts may have been intended by content owners essentially as an "inspired" political tactic—laying the groundwork for an initial bargaining position so extreme that other stakeholders could be easily pressured into agreeing to any formulation whatsoever, so long as it insulated them from the sweeping liability the content industry sought. *See id.* at 27–28 ("That bogeyman convinced many of the stakeholders to go along with a basic scheme predicated on copyright owners' right to continuing control of each attempt to see, read, hear, or use their works, in return for a specific exemption insulating each of them from liability.") Whether or not one accepts her characterization of the parties' motives, it is beyond dispute that these parties did indeed negotiate the safe harbor compromise under the auspices of the Senate Judiciary Committee. *See* S. REP. NO. 105-190, at 7 (stating that Senate Judiciary Chairman Orrin Hatch initiated negotiations "among copyright owners and Internet and online service providers to resolve the issue of service provider liability" that continued from January to April 1998).

97. S. REP. NO. 105-190, at 1–2.

98. H.R. REP. NO. 105-551, pt. 2, at 49 (1998).

99. H.R. REP. NO. 105-551, pt. 1, at 11.

as "the leading and most thoughtful judicial decision to date" on the subject of *direct* liability for OSPs, while simultaneously overruling conflicting aspects of *Frena*.[100]

This dramatic retreat from the initial, unyielding Working Group Report position on OSP liability makes discerning the legislative intent behind the section 512 safe harbor provisions an uncertain exercise, particularly given the fact that their precise terms were not crafted by legislators at all but instead by private actors taking part in off-line negotiations. The situation is further complicated by the fact that the DMCA itself is actually composed of several distinct Acts, such as OCILLA, each covering disparate subjects related to each other only by their technological focus. For example, the rationale underlying the anti-circumvention provisions codified beginning at 17 U.S.C. § 1201 was that only strong legal protections would deter piracy sufficiently to persuade reluctant authors to disseminate their works on the Internet at all.[101] This principle, however, appears to be somewhat inconsistent with the intent of the section codified at 17 U.S.C. § 117, namely, to permit owners of computers to authorize third parties to turn on their computers without prior authorization from the owners of copyrighted software that would automatically be copied as a result.[102] Consequently, commentators, including federal judges, have sometimes drawn diametrically opposing conclusions about the purpose of the safe harbors from the same legislative reports.[103]

Nevertheless, by endorsing *Netcom* at the explicit expense of *Frena*, the Senate Report clearly rejected the Working Group Report's strict, inflexible application of the law of direct liability to OSPs. Congress was wary, however, of "embarking upon a wholesale clarification of" the doctrines of contributory and vicarious liability, and

100. *Id.*

101. S. REP. NO. 105-190, at 8 ("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.")

102. *Id.* (characterizing provision, rather ambiguously, as "a minor but important clarification").

103. *Compare In re* Charter Commc'ns, Inc., 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting) (arguing that denying record companies benefits of § 512(h) subpoenas to identify infringers using "conduit" OSPs confounds clear intent of Congress to combat "massive piracy" without stifling technological development) *with* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 347 (2004) (arguing that subjecting "conduit" OSPs to subpoena power plainly exceeds intent of Congress, which "had no reason to foresee the application of § 512(h) to P2P file sharing").

elected instead "to create a series of 'safe harbors,' for certain common activities of service providers. A service provider which qualifies for a safe harbor receives the benefit of limited liability."[104]

Specifically, the statute provides that an OSP qualifying for one of the safe harbors "shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright."[105] Thus, while an OSP could still conceivably be found to have directly or secondarily infringed a copyright, so long as its infringing activities did not violate the relevant procedural requirements of section 512, it would not have to pay damages. By immunizing OSPs in this way, Congress hoped to provide "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[106]

C. Stakeholder Input into the Drafting of the Safe Harbors

In crafting the safe harbors, Congress heard testimony from a collection of individuals primarily representing the views of large-scale copyright owners and OSPs. While the early efforts of congressional committees to elicit the views of interested parties ostensibly included "libraries, educators, and beneficiaries of the public domain" as well as the "copyright" industries,[107] the hearings held as the bill neared completion featured precious little testimony from noncommercial groups.[108] In addition, no such groups were invited by Senate Judiciary Committee Chairman Orrin Hatch to take part in the off-line negotiations over the detailed mechanics of the safe harbors in early 1998.[109] Professor Jessica Litman has described the bargaining process used as:

> "overwhelmingly likely to appropriate value for the benefit of major stakeholders at the expense of the public at large. There is no overarching vision of the public interest animating the Digital Millennium Copyright Act. None. Instead, what we have is what a

104. S. REP. NO. 105-190, at 19.

105. 17 U.S.C. § 512(a) (2000). Sections (b), (c), and (d) contain identical language. *Id.* § 512(b), (c), (d). Section 512(j) authorizes courts to enjoin otherwise qualifying OSPs to deny access to infringing content or individuals. *Id.* § 512(j).

106. S. REP. NO. 105-190, at 20.

107. *Id*. at 2–3.

108. *Id.* at 3–7 (listing witnesses offering testimony at hearings held by the Senate Judiciary Committee); H.R. REP. NO. 105-551, pt. 1, at 12 (1998) (listing witnesses offering testimony at hearings held by House Subcommittee on Courts and Intellectual Property).

109. *See* S. REP. NO. 105-190, at 7 (indicating that sessions were organized "among copyright owners and Internet and online service providers" only).

> variety of different private parties were able to extract from each other in the course of an incredibly complicated four-year multiparty negotiation."[110]

In short, the implications of these procedures for the rights of consumers and other individual end users of the Internet were scarcely considered.

D. Key Provisions of the Safe Harbors

Section 512 of the statute ultimately identified safe harbors for five specific categories of OSPs: (1) those involved in "transitory digital network communications;"[111] (2) those providing "system caching" services;[112] (3) those providing space on their systems or networks for the storage of digital material "at the direction of users;"[113] (4) those providing "information location tools;"[114] (5) and nonprofit educational institutions providing such services to its faculty and graduate students.[115] In order to qualify for *any* of the safe harbors, an OSP is required to satisfy certain threshold eligibility requirements laid out in section 512(i).[116] Specifically, the OSP must have adopted and published a policy of terminating users guilty of repeat infringement, and its systems must be able to accommodate "standard technical measures" when implemented by copyright owners.[117]

In defining these categories, Congress recognized that OSPs in the first category, acting as "mere conduits"[118] for their users' activities, presented a set of liability issues that were quite distinct from those of the OSPs falling into the other four categories, and therefore

---

110. LITMAN, *supra* note 13, at 144–45.

111. 17 U.S.C. § 512(a) (2000).

112. *Id.* § 512(b).

113. *Id.* § 512(c).

114. *Id.* § 512(d).

115. *Id.* § 512(e).

116. *Id.* § 512(i).

117. *Id.* § 512(i); *see* Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004). As used in § 512(i), the phrase "standard technical measures" "refers to technical measures that copyright owners use to identify or to protect copyrighted works." *Id.* at 1080 n.11.

118. *See* BATUR OKTAY & GREG WRENN, WORLD INTELLECTUAL PROP. ORG., WORKSHOP ON SERVICE PROVIDER LIABILITY: A LOOK BACK AT THE NOTICE-TAKEDOWN PROVISIONS OF THE U.S. DIGITAL MILLENNIUM COPYRIGHT ACT ONE YEAR AFTER ENACTMENT 3–4 (1999), *available at* http://www.wipo.int/documents/en/meetings/1999/osp/pdf/osp_lia2.pdf (section 512(a) category "is commonly referred to as the 'mere conduit' limitation").

approached them differently.[119] The key difference in treatment is that OSPs qualifying for the "mere conduit" safe harbor of section 512(a) are effectively immunized with no requirement of further action on their part beyond the threshold eligibility requirements set out in section 512(i). OSPs seeking the protection of one of the other safe harbors, however, must cooperate with content owners in the "notice and takedown" procedures described in section 512(c)(3). The notice and takedown process was modeled on similar practices already followed by some content owners and OSPs on a voluntary basis.[120] OSPs seeking to make use of the safe harbors must publicly designate an agent to receive notices from copyright owners, and provide this contact information to the Register of Copyrights, which is in turn charged with maintaining a publicly available directory of designated agents.[121] Finally, upon receipt from a copyright owner of a signed, written notification clearly identifying an allegedly infringing work, the notice and takedown procedure was intended to require the OSP to "act[ ] expeditiously to remove or disable access to the infringing material."[122]

The safe harbors were made even safer by the addition of a provision expressly immunizing OSPs for any liability to the owners of material removed in good-faith compliance with the section 512(c) takedown procedures.[123] This immunity was intended to apply even in cases where an OSP removed materials later found to be non-infringing on its own initiative, rather than as a result of receipt of a takedown notice from a copyright owner.[124] In an effort to provide some protection for OSPs' customers, Congress also provided for both: (1) a "counternotification" or "put back" procedure whereby the owner of material claimed to be infringing can notify the OSP, who is then required to replace it,[125] and (2) a right of action enabling either

119. *Compare* 17 U.S.C. § 512(k)(1)(A) (defining "service provider" for use in connection with transitory network communications) *with* 17 U.S.C. § 512(k)(1)(B) (applying separate definition, appropriate to all OSPs other than those covered by (k)(1)(A) definition).

120. H.R. REP. NO. 105-551, pt. 2, at 54 (1998).

121. 17 U.S.C. § 512(c)(2); *see also* H.R. REP. NO. 105-551, pt. 2, at 54. The provision leaves open the possibility that OSPs will at some future time be required to pay for the maintenance of this directory by the Copyright Office. 17 U.S.C § 512(c)(2) (stating that Register of Copyrights "may require payment of a fee by service providers to cover the costs of maintaining the directory").

122. H.R. REP. NO. 105-551, pt. 2, at 53; *see also* 17 U.S.C. § 512(c)(1)(A)(iii) (2004).

123. 17 U.S.C. § 512(g); *see also* H.R. REP. NO. 105-551, pt. 2, at 59.

124. *See* H.R. REP. NO. 105-551, pt. 2, at 59.

125. 17 U.S.C. § 512(g)(2)(C) (2000); H.R. REP. NO. 105-551, pt. 2, at 59.

OSPs or copyright owners to recover damages for injuries sustained as a result of an OSP's reliance on knowing misrepresentations by any party making use of the notice and takedown or put back procedures.[126]

Congress also expressed a desire to avoid creating the conditions for "interference with privacy."[127] This intent was codified in section 512(m), which states that OSPs are not required to monitor their services or affirmatively seek facts indicating infringing activity.[128] Notwithstanding the claimed intent, however, the language adopted leaves open the possibility that such activities may be required in the future, if they are introduced as part of a "standard technical measure" by copyright owners.[129]

While Congress stressed that these procedures were to be voluntary for OSPs and copyright owners alike,[130] any OSP wishing to avail itself of one of the safe harbors in sections 512(b)-(e) is effectively required to cooperate, since compliant notice from a copyright owner will be deemed legally sufficient to establish that the OSP had actual or constructive knowledge that its facilities were being used to infringe.[131] An OSP declining to cooperate in the notice and takedown process will have its liability for any infringement decided "without reference to" the safe harbors.[132]

In order to facilitate the prosecution of anonymous infringers, section 512(h) includes a provision authorizing the issuance of a "subpoena to identify infringer," which may be issued to an OSP by the clerk of any district court upon request by a copyright holder.[133] Cop-

126. 17 U.S.C. § 512(f); H.R. REP. NO. 105-551, pt. 2, at 59.
127. H.R. REP. NO. 105-551, pt. 1, at 12.
128. 17 U.S.C. § 512(m)(1) (2000).
129. *See id.*
130. *See* H.R. REP. NO. 105-551, pt. 2, at 54 ("The Committee emphasizes that new Section 512 does not specifically mandate use of a notice and take-down procedure. . . . At the same time, copyright owners are not obligated to give notification of claimed infringement in order to enforce their rights.").
131. The House Report states that "neither actual knowledge nor awareness of a 'red flag' may be imputed to a service provider based on information from a copyright owner or its agent that does not comply with the notification provisions," strongly implying that compliant notice from a copyright owner is tantamount to "actual knowledge." *Id.*; *see also* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 623 (4th Cir. 2001) (holding that service provider, to be eligible under 512(c) safe harbor, must show, *inter alia*, that "it has neither actual knowledge that its system contains infringing materials nor an awareness of facts or circumstances from which infringement is apparent, or it has expeditiously removed or disabled access to infringing material upon obtaining actual knowledge of infringement").
132. H.R. REP. NO. 105-551, pt. 2, at 54.
133. 17 U.S.C. § 512(h)(1) (2000).

yright owners "who have submitted or will submit" a properly formatted takedown notice to an OSP can obtain such an order from the court by filing a copy of that notice, the text of the proposed order, and a sworn declaration that the order will only be used to protect the applicant's copyrights.[134] Assuming the information is in its possession,[135] the OSP must provide it to the copyright holder "expeditiously."[136] The Senate Report says that compliance with a section 512(h) subpoena, unlike compliance with a takedown notification, is not optional: the identity of the alleged infringer must be disclosed "*regardless* of whether the service provider responds to the notification of claimed infringement."[137] Congress also intended that the entire process be simple and quick for the copyright holder's benefit.[138]

III.
IMPACT OF THE SAFE HARBORS ON OSP BEHAVIOR

A. OSP Policies Converge on the Notice and Takedown Model

It is impossible to obtain definitive data on the way in which the safe harbor provisions are being implemented by copyright owners and OSPs today. The very informality of the notice and takedown scheme was meant to encourage "cooperative" efforts by owners and OSPs, and the result has been that most notice and takedown processes are never formally reported. While the Electronic Frontier Foundation (EFF) maintains a database of cease-and-desist notices forwarded to it by recipients, including OSPs who have received section 512(c) takedown requests or section 512(h) subpoenas,[139] these data are clearly incomplete, since only a handful of OSPs are represented in the database. It appears that most OSPs do not forward such

134. S. REP. NO. 105-190, at 51 (1998).

135. *See id.* ("[The order requires only] disclosure of information in the possession of the service provider, rather than obliging the service provider to conduct searches for information that is available from other systems or networks.").

136. *Id.*

137. *Id.* (emphasis added).

138. *Id.* ("The issuing of the order should be a ministerial function performed quickly for this provision to have its intended effect."); *see also In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting).

> Nowhere in the DMCA did Congress indicate that copyright holders should be relegated to such cumbersome and expensive measures [as John Doe lawsuits] against conduit ISPs. The legislative history shows that the purpose of the subpoena power in the DMCA was to obtain the assistance of ISPs in an expeditious process to stop infringement.

Id.

139. *See* Chilling Effects Clearinghouse, Index of Cease and Desist Notices, http://www.chillingeffects.org/notice.cgi (last visited Oct. 15, 2005).

notices and do not advertise the costs they incur in complying with them.

Nevertheless, it is possible to get a general sense of the way in which the DMCA has affected OSP behavior. A comparison of evolving terms of use, copyright, and privacy policies adopted by OSPs shows the convergence on the section 512(c) notice and takedown model that is prevalent today. Prior to the passage of the DMCA in 1998, these policies exhibited a great deal of variability, as one might expect in a competitive service market. For instance, before 1998, the guidelines for end users posted by OSP Bigfoot's mail forwarding service made no explicit mention of third party intellectual property rights, instead merely reserving the right to define something called "offensive content," and terminate any subscribers who "enter content [Bigfoot] deem[ed] offensive."[140] Individuals who came across such "offensive content" were urged to contact the Bigfoot webmaster.[141] Freedrive, an Internet-based online storage provider,[142] made no mention whatsoever of third-party intellectual property rights as late as February of 1999.[143] Internet access providers AOL and AT&T included fairly forceful, but nonetheless rather generic, prohibitions against use of their services to post infringing information.[144]

Strikingly, AOL's prohibition was updated at some point between mid-January and early May of 1998. While the earlier prohibition against violation of third-party intellectual property rights was retained, it was supplemented by an entirely new section labeled "Copyright Complaints," which provided notice that AOL might terminate accounts of infringers "in appropriate circumstances and at its discretion." This new section also provided step-by-step instructions, *closely tracking the language of Section 512(c)(3)*, for individuals

140. Bigfoot, Conditions of Use (Oct. 18, 1996), http://web.archive.org/web/19961018104123/bigfoot.com/Cou2.htm (last visited Mar. 18, 2005). Historical versions of the various policies of OSPs were retrieved from the Internet Archive (www.archive.org), a service that preserves "snapshots" of web pages saved at various times.

141. *Id.*

142. Today Freedrive is a division of Xdrive.

143. Freedrive, Legal Terms and Conditions (Feb. 22, 1999), http://web.archive.org/web/19990222082458/www.freedrive.com/fdlegal.htm (last visited Oct. 15, 2005).

144. *See* AOL.com, Legal Notices (Jan. 11, 1998), http://web.archive.org/web/19980111055255/www.aol.com/copyright.html (last visited Oct. 15, 2005) (prohibiting users from posting "another's proprietary information, including trademarks or copyrighted information, without express authorization from the rights holder"); AT&T Website Agreement (June 6, 1997), http://web.archive.org/web/19970606133141/www.att.com/terms.html (last visited Oct. 15, 2005) (prohibiting posting of information "that would violate the property rights of others, including unauthorized copyrighted text, images or programs, trade secrets or other confidential proprietary information, and trademarks or service marks used in an infringing fashion").

who "believe [their] work has been copied and is accessible on the AOL service in a way that constitutes copyright infringement," including contact information for AOL's designated agent.[145]

Free home page provider Geocities addressed the issue with a policy clearly aimed at curtailing the use of its services for software piracy, defining the types of violations at issue as "including but not limited to offering pirated computer programs or links to such programs, information used to circumvent manufacturer-installed copy-protect devices, including serial or registration numbers for software programs, or any type of cracker utilities (this also includes files which are solely intended for game emulation)."[146]

As of early 1998, search engine Yahoo! focused its legal disclaimers on absolving itself of responsibility for "information [found via its services] that some people may find offensive or inappropriate."[147] Its policy continued: "Yahoo! makes no representations concerning any endeavor to review the content of sites listed in the directory or any of the Materials, and so Yahoo! isn't responsible for the accuracy, copyright compliance, legality or decency of material contained in sites listed in the directory or in the Materials."[148]

Perhaps the most unusual of these pre-DMCA policy statements belonged to eBay. The online auction site joined Yahoo! in disclaiming responsibility for materials posted by individuals using its services,[149] but went well beyond this in specifically addressing the question of infringement of the intellectual property rights of third parties. eBay created something which it then called the "Legal Buddy Program," whereby registered third parties ("Members") were able to work with eBay to identify and remove listings that infringed

145. *Compare* AOL.com Legal Notices (Jan. 11, 1998), http://web.archive.org/web/19980111055255/www.aol.com/copyright.html (last visited Oct. 15, 2005) (including only blanket prohibition) *with* AOL.com Copyright (May 8, 1998), http://web.archive.org/web/19991111022316/www.aol.com/copyright.html (last visited Oct. 15, 2005) (retaining blanket prohibition, but also adding "Copyright Complaints" section).

146. GeoCities Page Content Guidelines and Member Terms of Service (Jan. 23, 1998), http://web.archive.org/web/19980123232600/www.geocities.com/members/guidelines/ (last visited Oct. 15, 2005).

147. Yahoo!: Important Disclaimers and Legal Information (Feb. 10, 1998), http://web.archive.org/web/19980210204825/www.yahoo.com/info/misc/disclaimer.html (last visited Oct. 15, 2005).

148. *Id.*

149. *See* eBay, User Agreement (Apr. 21, 1999), http://web.archive.org/web/19990421071501/pages.ebay.com/aw/user-agreement.html (last visited Oct. 15, 2005) ("For legal reasons, we cannot nor do we try to control the information provided by other users which is made available through our system.").

their intellectual property rights.[150] As early as 1999, eBay's end user policies reserved the right to suspend or terminate the accounts of repeat infringers of the intellectual property rights of third parties, apparently including not only Legal Buddy Members, but also outside parties.[151]

Today, by contrast, nearly all OSPs whose policies were reviewed for this Note use extremely similar language in their end-user policies to address issues of third-party intellectual property rights. Not surprisingly, the language around which these companies have converged essentially parrots the text of the DMCA's description of notice and takedown procedures in section 512(c)(3).[152] Probably the two most striking changes are the near-universal inclusion of step-by-step instructions for filing a notice of infringement,[153] and the incor-

150. *See id.*

151. *Id.*

152. 17 U.S.C. § 512(c)(3) (2000).

153. *See, e.g.*, AOL.com, Procedure for Making Claims of Copyright Infringement, http://site.aol.com/copyright/infringement.html (last visited Oct. 15, 2005). The AOL document reads:

> If you believe that your copyrighted work has been copied and is accessible on this site in a way that constitutes copyright infringement, you may notify us by providing our copyright agent with the following information:
>
> 1. the electronic or physical signature of the owner of the copyright or the person authorized to act on the owner's behalf.
> 2. a description of the copyrighted work that you claim has been infringed and a description of the infringing activity.
> 3. identification of the location where the original or an authorized copy of the copyrighted work exists, for example the URL of the website where it is posted or the name of the book in which it has been published.
> 4. identification of the URL or other specific location on this site where the material that you claim is infringing is located; you must include enough information to allow us to locate the material.
> 5. your name, address, telephone number, and email address.
> 6. a statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law.
> 7. a statement by you, made under penalty of perjury, that the above information in your Notice is accurate and that you are the copyright owner or are authorized to act on the copyright owner's behalf.
>
> The document then provides contact information for AOL's designated agent. *Id.*

Compare the language in 17 U.S.C. § 512(c)(3)(A) (2000):

> 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:

poration of language warning end users that their personally identifiable information may be turned over to third parties if the OSP determines that it is "required" by law to do so.[154] Remarkably, this latter policy has been adopted even by the anonymizer.com service, which exists to allow Internet users to visit sites without revealing their IP addresses (and thus, potentially, their identities).[155]

It is true that one cannot be certain that this trend would not have occurred in the absence of the passage of the DMCA. To some extent,

---

(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.
(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.

Id.

Most OSPs now include strikingly similar instructions in their policy documents. *See, e.g.*, Cingular Wireless Site Access Agreement (Nov. 15, 2004), http://www.cingular.com/legal/ (last visited Oct. 15, 2005) (Cingular acquired AT&T Wireless); Yahoo!, Copyright and Intellectual Property Policy, http://docs.yahoo.com/info/copyright/copyright.html (last visited Oct. 15, 2005); Craig's List, Terms of Use, http://www.craigslist.org/about/terms.of.use.html (last visited Oct. 15, 2005) (online classified advertising service); Earthlink, Policies and Agreements: Notification of Claimed Copyright Infringement, http://www.earthlink.net/about/policies/dmca (last visited Oct. 15, 2005) (Internet access provider).

154. *See, e.g.*, Bigfoot, Privacy Policy, http://www.bigfoot.com/RUN?FN=private_policy (last visited Oct. 15, 2005) ("Bigfoot will disclose User information if . . . we are required to do so by law or regulatory authority."); Xdrive, Privacy Policy, http://www.freedrive.com/privacy.jsp (last visited Oct. 15, 2005) ("Xdrive may disclose or access account information when we believe in good faith that the law requires it."). Note that Freedrive is now a division of Xdrive.

155. *See* Anonymizer Privacy Policy, http://www.anonymizer.com/docs/legal/privacypolicy.shtml (last visited Oct. 15, 2005) ("[W]e disclose personal information only in the good faith belief that we are required to do so by law, or that doing so is reasonably necessary to [ ] comply with legal process . . . .").

the changes appear to reflect industry consolidation and reactions to litigation.[156] Nonetheless, the observed convergence is plainly consistent with the safe harbors' acting to influence the development of OSP policies. Certainly the most logical explanation for the observed trend is that OSPs have concluded that insertion of the stock language from the Copyright Act into their end user policies is the simplest, least expensive, and most certain way to ensure that they are in compliance with the threshold requirements of the DMCA's safe harbor provisions.

To the extent that the requirements of section 512(c) represent "best practices" for the industry, this convergence would be a good thing. Nevertheless, there is evidence that the desire to evade the costs associated with wholehearted participation in the safe harbor procedures may be driving some OSPs to dismantle monitoring capabilities rather than build them up. The EFF has released a document entitled "Best Data Practices for Online Service Providers,"[157] in which OSPs are advised to employ "obfuscation," data aggregation, and frequent deletion of activity logs in order to "simultaneously maximize the privacy of users and protect themselves from the damaging effects of the DMCA . . . and other data disclosure laws."[158] A similar

156. The potential impact of consolidation among OSPs is demonstrated by free web host GeoCities, which replaced its prior terms and conditions documents with those of parent Yahoo! after it was acquired. *Compare* GeoCities Page Content Guidelines and Member Terms of Service (Jan. 23, 1998), http://web.archive.org/web/19980123232600/www.geocities.com/members/guidelines/ (last visited Oct. 15, 2005) (containing prohibition against "acts of copyright . . . infringement"), *with* Yahoo! GeoCities Terms of Service ¶ 21 (Oct. 12, 1999), http://web.archive.org/web/19991012112204/docs.yahoo.com/info/terms/geoterms.html (last visited Oct. 15, 2005) (replacing GeoCities prohibition against copyright infringement with link to Yahoo!'s own copyright policy). A possible illustration of the impact of litigation on such policies is the Internet Movie Database (IMDb.com), whose parent, online retailer Amazon.com, was the target of at least two lawsuits in 2002–2003 alleging vicarious liability for sales of unauthorized DVDs. *See* Hendrickson v. Amazon.com, 298 F. Supp. 2d 914, 916 (N.D. Cal. 2003) ("This court previously granted summary judgment in favor of Hendrickson, in a previous action, Hendrickson v. Amazon.com, Inc., CV 02-07394 TJH (C.D. Cal. 2003). . . ."). It was also 2003 that marked the issuance by affiliate IMDb.com of a policy document entitled "Notice and Procedure for Making Claims of Copyright Infringement," which, like the example from AOL excerpted above, is strikingly faithful to the structure and language of § 512(c)(3). *Compare* IMDb.com, Notice and Procedure for Making Claims of Copyright Infringement (Sept. 8, 2003), http://web.archive.org/web/20030908183856/www.imdb.com/copyright_agent (last visited Oct. 15, 2005), *with* AOL, Procedure for Making Claims of Copyright Infringement, *supra* note 153, *and* 17 U.S.C. § 512(c)(3)(A) (2000).

157. Electronic Frontier Foundation, Best Data Practices for Online Service Providers (Aug. 14, 2004), http://www.eff.org/osp/20040819_OSPBestPractices.pdf (last visited Oct. 15, 2005).

158. *Id.* at 4–6.

article by leading cyberlaw scholar Fred von Lohmann advises erstwhile developers of peer-to-peer products to engineer "plausible deniability" into their architectures and business models, reasoning that "software that sends back usage reports may lead to more knowledge than you want," and that "[i]f you're not collecting information about what [your users are] doing, no one can get that information from you."[159] Whatever the merits of such actions—and it is difficult to view pressure to dispose of system performance and monitoring data as quickly as possible *for the express purpose of avoiding copyright liability* as a constructive development—such advice surely suggests that the safe harbor requirements of the DMCA are having significant influence on the development of the technological underpinnings of the Internet.

B. The Tilt Toward Overdeterrence

In light of their origin in a bargaining process limited to copyright owners and OSPs, it should come as no surprise that the notice and takedown procedures laid out in section 512(c) make it easy to quickly remove materials posted by someone who falls into neither group. For example, under section 512(c) a "sufficiently compliant" notice and takedown request need not contain even the slightest hint of a description of the nature of an alleged infringement.[160]

It is worth considering, by way of comparison, the pleading requirements that exist in other contexts. For example, even the liberal notice pleading requirements of the Federal Rules of Civil Procedure require that a complaint contain "a short and plain statement of the claim showing that the pleader is entitled to relief."[161] It is true that, in the infringement context, pleading requirements can be especially loose,[162] and it can be argued that this is especially appropriate in the case of online copyright infringement because of the potential for overwhelming volume and rapidly shifting locations when the alleg-

159. Fred von Lohmann, IAAL: Peer-to-Peer File Sharing and Copyright Law after Napster (2001), http://www.gtamarketing.com/P2Panalyst/VonLohmann-article.html.
160. 17 U.S.C. § 512(c) (2000).
161. FED. R. CIV. P. 8(a)(2).
162. *See, e.g.*, Swierkiewicz v. Sorema N.A., 534 U.S. 506, 512–14 (2002) ("Given the Federal Rules' simplified standard for pleading, a court may dismiss a complaint only if it is clear that no relief could be granted under any set of facts that could be proved consistent with the allegations.") (internal quotes and citations omitted); Perfect 10, Inc. v. Cybernet Ventures, Inc., 167 F. Supp. 2d 1114, 1120 (C.D. Cal. 2001) ("Copyright claims need not be pled with particularity . . . . [C]omplaints simply alleging present ownership by plaintiff, registration in compliance with the applicable statute and infringement by defendant have been held sufficient under the rules.").

edly infringing works are digital.[163] Still, *these are only the requirements for a claim to survive a motion to dismiss*; they do not result in the automatic granting of the relief the plaintiff is requesting.[164] By contrast, the safe harbor notice and takedown process gives a complainant effectively complete relief without requiring that she formulate a coherent claim.

An additional and possibly more apt litigation analogy would be to the standards for temporary or permanent injunctive relief, which require the movant to establish that she is likely to prevail on the merits of her claim, that she will suffer irreparable harm if the infringement is left unchallenged, or that the balance of hardships in the case tips in her favor, among other things.[165] Presumably, a copyright owner seeking an injunction in court would be required to show some probability of proving ownership of a valid copyright and infringement by a defendant, and the defendant would be afforded an opportunity to raise relevant defenses, before any injunction would issue.[166]

By contrast, we have seen that section 512(c) imposes nothing approaching that burden on a complainant alleging infringement in connection with a takedown request to an OSP. Instead, as long as it satisfies the minimal threshold requirements of section 512(i), the OSP is immunized from liability *to anyone* if it responds to even a "substantially compliant" takedown request by removing or blocking access to the material in question. The OSP thus has a powerful incentive to provide complete relief to complaining copyright owners notwithstanding any shortcomings in the form of their requests. As one OSP employee put it, "Since no subscriber is worth even the price of a phone call to a lawyer to figure out what to do, it is easier just to cancel them."[167]

---

163. *See, e.g.*, *Cybernet*, 167 F. Supp. 2d at 1120–21 (describing "massive infringement" at issue in *Napster*, along with possibility that in peer-to-peer environment, details "could vacillate hour-to-hour, day-to-day").

164. *See, e.g.*, *id.* at 1121 (stating that pleadings alleging copyright infringement were not required to articulate their claims with precision, because "[f]urther details can be elicited during the discovery stage").

165. *See, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1165 (C.D. Cal. 2002) (laying out Ninth Circuit's "two interrelated tests . . . for determining the propriety of the issuance of a preliminary injunction").

166. *See, e.g.*, *id.* at 1168–69 (declining to issue injunction based on direct infringement theory, where plaintiff failed to provide evidence establishing that defendant OSP had infringed its rights of reproduction, distribution, or display or prepared derivative works based upon plaintiff's copyrighted material).

167. *The Wrongs of Copyright*, ISP-PLANET, July 3, 2002, http://www.isp-planet.com/business/2002/copyright_bol.html (quoting posting by "PF").

Even though the DMCA notice and takedown provisions require "a good faith belief"[168] that rights are being infringed, require that statements are being made accurately "under penalty of perjury,"[169] and warn of liability for damages and costs both to the alleged infringer and the OSP in the event of knowing material misrepresentations,[170] there seems to be little real chance that a complaining content owner will face legal consequences for overreaching. For example, in the one case successfully brought under section 512(f) to date, Diebold, a prominent manufacturer of voting machines, was found to have knowingly misrepresented its claim of infringement, yet there is no mention of any penalty for perjury in connection with the case.[171]

Diebold, in a sense, is the exception that proves the rule on the bias of the DMCA in favor of unquestioning removal of content, and its facts are worth reviewing. The case developed after unknown persons obtained, and reproduced on a number of Internet websites, an archive of internal emails concerning electronic voting machines.[172] In response, "Diebold sent cease and desist letters to many ISPs" hosting copies of or links to the archive, requesting removal or disabling of access in accordance with the section 512(c)(3) procedures.[173] The emails included exchanges among Diebold technicians "contain[ing] evidence that some employees have acknowledged problems associated with the [voting] machines."[174] Diebold claimed the emails were copyrighted materials and reminded the OSPs that "they would be shielded from a copyright infringement suit by Diebold if they disabled access to or removed the allegedly infringing material."[175] Many OSPs apparently cooperated with Diebold's takedown request. Nevertheless, the Online Policy Group, which served as OSP for IndyMedia, an online magazine that had linked to the e-mail archive, together with two Swarthmore College students who had re-posted the archive in several locations, sued Diebold for injunctive, declaratory, and monetary relief.[176]

---

168. 17 U.S.C. § 512(c)(3)(A)(v) (2000).
169. *Id.* § 512(c)(3)(A)(vi).
170. *Id.* § 512(f).
171. Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004). In a settlement approved in October 2004, Diebold agreed to pay the plaintiffs $125,000 in damages and attorneys' fees. *See* Online Policy Group, Online Policy Group v. Diebold, Inc., http://www.onlinepolicy.org/action/legpolicy/opg_v_diebold (last visited Oct. 15, 2005).
172. *Diebold*, 337 F. Supp. 2d at 1197.
173. *Id.* at 1198.
174. *Id.* at 1197.
175. *Id.* at 1198.
176. *Id*. at 1197–98.

Reviewing motions for summary judgment, the district court noted that Diebold had never filed any copyright actions over the disputed materials,[177] had never proven that any specific emails contained either copyrighted material or material of commercial value,[178] and had eventually conceded that at least some were subject to fair use,[179] and concluded "that Diebold, through its use of the DMCA, sought to and did in fact suppress publication of content that is not subject to copyright protection."[180] The court held that this amounted to the sort of knowing material misrepresentation identified by section 512(f), pointing out:

> The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions—which were designed to protect ISPs, not copyright holders—as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.[181]

While the result in *Diebold* could in principle be read to suggest that the safe harbor procedures have struck the proper balance between protecting the interests of copyright owners and safeguarding the First Amendment rights of those who wish to publish uncopyrighted material on the Internet, the outcome was probably due more to the high-profile nature of the case than to the inherent effectiveness of the statutory scheme. Had the email archive not concerned such a visible public policy concern (namely, the security of electronic voting machines), or had some of Diebold's targets not been affiliated with an activist organization,[182] the case might not have turned out the way it did. The legal and organizational resources available to the Online Policy Group and IndyMedia, coupled with the obviously political nature of the dispute, probably permitted a much more effective resistance to Diebold's efforts to silence its critics than would have been possible for most website publishers. Indeed, given that many

177. *Id.* at 1198.

178. *See id.* at 1203.

179. *Id.* The court also apparently believed that fair use applied to materials not covered by Diebold's concession. *See id.* ("Finally, Plaintiffs' and IndyMedia's use was transformative: they used the email archive to support criticism that is in the public interest, not to develop electronic voting technology.").

180. *Id.*

181. *Id.* at 1204–05.

182. *See* About the Online Policy Group, http://www.onlinepolicy.org/about.shtml (last visited May 10, 2005) ("The Online Policy Group (OPG) is a nonprofit organization dedicated to online policy research, outreach, and action on issues such as access, privacy, digital defamation, and the digital divide. Additionally, it focuses on Internet participants' civil liberties and human rights . . . .").

OSPs responded to Diebold's letters by taking down the named sites,[183] Diebold may well feel that $125,000 was not too great a price to pay for at least partly containing some very embarrassing revelations. All in all, it seems unlikely that *Diebold* will deter other companies from similar abuses of the DMCA's notice and takedown procedures.

By contrast, the DMCA's counter notification procedures,[184] which were touted as a tool to protect users whose works are wrongly removed via the notice and takedown process,[185] are much more demanding on website operators than the section 512(c) procedures are on copyright holders. First, the site operator must wait until material has already been removed before taking any action at all.[186] Second, section 512(g) counter notification requires that the target of the takedown be willing to swear, *under penalty of perjury*, that the material in question was *removed* as the result of "mistake or misidentification."[187] Finally, it is by no means clear that "mistake or misidentification" covers situations where the complainant was simply wrong about the claim of infringement, or where the infringement was not one to which the safe harbors apply.[188]

This last problem—that is, the possibility of mistake as to whether a particular type of infringement is subject to the notice and takedown process—is especially significant. The DMCA safe

183. *See* Press Release, Rep. Dennis Kucinich, Kucinich Requests House Judiciary Committee Hearing on Diebold's Abuses of Digital Millennium Copyright Act (Nov. 21, 2003), *available at* http://www.house.gov/apps/list/press/oh10_kucinich/031121judcmtediebold.html (last visited Oct. 30, 2005) ("Diebold invoked the DMCA to pressure many ISPs and universities into removing websites and hyperlinks.").

184. 17 U.S.C. § 512(g)(3) (2000).

185. *See* S. REP. NO. 105-190, at 50 (1998)

> The put back procedures were added as an amendment to this title in order to address the concerns of several members of the Committee that other provisions of this title established strong incentives for service providers to take down material, but insufficient protections for third parties whose material would be taken down.

Id.

186. *See* 17 U.S.C. § 512(g)(3)(C).

187. *Id.*

188. *See* JAY DRATLER, JR., CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 6.03 n.312 (2005) ("The language of Subparagraph (C) restricts counter-notifications to assertions of mistake or misidentification of the material at issue. It does not permit counter-notifications based on disputes, whether or not in good faith, over ownership of copyright or copyright infringement (for example, based on a belief that an exception such as fair use applies)."). *But see* Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660(SHS), 2002 WL 1997918, at *2 (S.D.N.Y. 2002) (noting that defendant had submitted counter notification, and OSP had responded by restoring access to site).

harbors, on their face, apply only to allegations of direct infringement, as defined in 17 U.S.C. § 501. This includes violations of the standard set of exclusive rights included in 17 U.S.C. § 106, along with the rights outlined in sections 106–122 and a scattering of other provisions of the Copyright Act.[189] It does *not* include violations of the anti-circumvention provisions, any rights granted by the Lanham Act (covering trademarks), patent laws, nor laws governing rights of privacy or publicity. Yet, despite the limited set of rights protected by the DMCA, the Act's notice and takedown process includes no requirement either that a complainant identify the rights allegedly infringed or that the OSP verify that these are among the rights covered by the safe harbor notice and takedown procedures. Thus, even if we assume that all complainants act in good faith, mistakes seem likely. Suppose, for example, that the holder of a trademark is concerned about dilution or initial interest confusion, has a good faith belief that her rights in these areas are being violated, initiates a notice and takedown procedure based on a good faith (but incorrect) belief that these rights are covered by the DMCA, and receives full compliance from the OSP. Despite the complainant's clear mistake, the DMCA's counter-notification procedures would probably offer the target of the complaint no recourse at all.

These possibilities are not at all farfetched. In fact, review of a database of notice and takedown notifications maintained by the Chilling Effects Clearinghouse suggests that such "mistakes" are routine. Many notifications specifically allege infringements of rights not covered by section 512, such as the anti-circumvention provisions,[190]

189. 17 U.S.C.A. § 501(a) (Supp. II 2003) ("Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122 or of the author as provided in section 106A(a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer . . . .").

190. *See, e.g.*, E-mail from Microsoft Corp. to Blogger [Google, Inc.] (Dec. 21, 2004), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=1561 (last visited Oct. 15, 2005) (requesting removal of links to blog publishing software activation keys). Although part of the Copyright Act—indeed part of the DMCA itself—the anti-circumvention provisions represent a distinct statutory restriction, and violations of those provisions do not constitute copyright infringement as defined under 17 U.S.C. § 501. RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *6 (W.D. Wash. 2000) (claims "aris[ing] under section 1201 of the DMCA . . . do not constitute copyright 'infringement' claims"); *see also* MELVILLE B. NIMMER & DAVID NIMMER, *The Defense of Fair Use*, *in* NIMMER ON COPYRIGHT § 13.05, § 13.05(F)(6) (2005) ("As elaborately discussed previously, Section 1201 of the Act defines the anti-circumvention as something distinct from copyright infringement.").

trademark rights,[191] trade secrets,[192] rights of publicity,[193] or rights of privacy.[194]

Although there is no reason to suspect that Congress intended the notice and takedown procedures to extend beyond the Copyright Act, there is probably nothing unlawful about an OSP choosing to use the same procedure to handle allegations of infringement of other intellectual property rights that it uses for copyright infringement. The larger point, however, is that the procedures laid out in section 512 leave all the incentives in favor of takedown on the strength of mere allegation.[195] This imbalance, in turn, raises the strong possibility of abuse.[196] There is clear evidence that some individuals and organiza-

191. *See, e.g.*, Fax from Creative Crystal Co. to Google, Inc. (Aug. 22, 2003), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=842 (last visited Oct. 15, 2005) (requesting takedown of sites which use Creative Crystal's registered trademarks "in metatags and keywords up to 39 times on one page"). *But see* OKTAY & WRENN, *supra* note 118, at 14–15 ("Trademark infringement claims, for example, are less likely to result in take down compared with copyright infringement claims at Yahoo! because there is no specified procedure at law and no statutory safe harbor to encourage processing in a particular manner.").

192. *See, e.g.*, Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1197 (quoting Diebold as claiming that contested email archive contained "trade secret information").

193. *See, e.g.*, E-mail from [Private] to Google, Inc. (Mar. 15, 2004), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=1179 (last visited Oct. 15, 2005) (requesting removal of links to allegedly unauthorized photos of sender); Fax from [Private] to Google, Inc. (Apr. 12, 2004), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=1230 (last visited Oct. 15, 2005) (same).

194. *See, e.g.*, Fax from [Private] to Google, Inc. (Apr. 16, 2004), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=1233 (last visited Oct. 15, 2005) ("The image on the above link has my photo. I do not want people to search my name and see my photo. I feel uncomfortable."); Fax from [Private] to Google, Inc. (Apr. 9, 2004), http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=1219 (last visited Oct. 15, 2005) ("This site has pictures of me with out permission, that were taken from my website . . . .This site also has false information about me being convicted of crimes that I was never convicted of."). Admittedly, it is not certain that the senders of these notices do not own the copyright in the images at issue. However, it appears from the texts of the letters sent that the gravamen of the complaints is that the images are *of them*. It is likely that these are effectively privacy or publicity disputes, which should not be covered under § 512.

195. *See* Transcript of Oral Argument at 9, *Diebold*, 337 F. Supp. 2d 1195 (2004) (No. C 03-04913 JF), *available at* http://www.eff.org/legal/ISP_liability/OPG_v_Diebold/20040209_transcript.txt (last visited Oct. 15, 2005) ("ISPs don't have any incentive under this law to protect speech rights . . . . Their incentives, in fact, in the statute go all the other way.").

196. *But see* Dr. Nils Bortloff & Janet Henderson, World Intellectual Prop. Org., Workshop on Service Provider Liability: Notice and Take-Down Agreements in Practice in Europe– Views from the Internet Service Provider and Telecommunications Industries and the Recording Industry 18 (Dec. 1, 1999), http://www.wipo.int/documents/en/meetings/1999/osp/doc/osp_lia3.doc (discussing anecdotal evidence from U.S. sources that U.S. OSPs will simply return incomplete notice and takedown re-

tions are using the liberal takedown procedure to silence critics.[197] There is also evidence that the ease of the DMCA's takedown procedures, when coupled with the comparative difficulty of counter notification, has in fact led to widespread deterrence of the speech of end users. Speaking about the impact of the safe harbors on Yahoo!, an in-house counsel for the OSP explained:

> As a practical matter, notice and take down begins and ends the debate over whether a site stays up. Most service providers have little incentive to incur the costs and risks of litigation and will opt for the safe harbor, taking the site down. Users can provide a "counter notification" giving the copyright owner 10 days to obtain a court order to keep the site down, but very few users choose this option in Yahoo!'s experience. . . . This may be expedient and efficient, but to some extent it represents a "might makes right" resolution that gives little or no consideration to the validity of the copyright interest being asserted, its ownership, the permissible scope of protection, or defenses such as parody, fair use, de minimis use, and so on.[198]

In one of the very few reported cases in which an end user targeted by a takedown notice challenged the removal of his material in court,[199] counsel for the Motion Picture Association of America

---

quests to sender "with a firm refusal to take action"); CHRISTIAN AHLERT ET AL., HOW 'LIBERTY' DISAPPEARED FROM CYBERSPACE: THE MYSTERY SHOPPER TESTS INTERNET CONTENT SELF-REGULATION 19–23 (2004), http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf (noting that one U.S. OSP surveyed in blind test refused to take down material when notice submitted failed to meet section 512(c)(3) requirements).

197. *See, e.g.*, *Diebold*, 337 F. Supp. 2d 1195; TRICIA BECKLES & MARJORIE HEINS, FREE EXPRESSION POLICY PROJECT, SECOND PRELIMINARY REPORT ON FAIR USE AND "CEASE AND DESIST" LETTERS, http://www.fepproject.org/commentaries/ceaseanddesist2.html (last visited Oct. 15, 2005). Beckles and Heins describe the experience of former Mormon Roger Loomis, who complied with a cease and desist notice challenging his right to post excerpts from official church materials on his website critical of The Church of Jesus Christ of Latter-day Saints despite the fact that he believed he was entitled to use them in this way.

> When asked why he acquiesced and removed the quoted text, Mr. Loomis said that it was much easier to remove the material than to get into a 'big battle,' especially since he was worried about paying the IRI's legal fees if he received an unfavorable ruling. The risk of paying those fees was not worth the 'emotional time commitment.'

Id. The Church of Scientology has embraced this use of the DMCA as well. *See* Declan McCullagh, *Google Yanks Anti-Church Sites*, WIRED, Mar. 21, 2002, http://www.wired.com/news/politics/0,1283,51233,00.html (last visited Oct. 15, 2005) ("DMCA threats from the church seem to be becoming so common that Dave Touretzsky, a scientist at Carnegie Mellon, has even drafted a form letter that can be sent in reply.").

198. OKTAY & WRENN, *supra* note 118, at 17.

199. Rossi v. Motion Picture Ass'n of Am., 391 F.3d 1000 (9th Cir. 2004), *cert. denied*, 125 S. Ct. 1977 (2005).

hinted at the scale of this activity: "Not one time out of 38,000 [ ], and this goes to, I would submit, good faith, other than from Mr. Rossi, has our client been sued—either under the DMCA, or under state law."[200]

Some observers have suggested that these effects fall disproportionately on individual speakers, as opposed to institutions. In an early assessment of the practical operation of the safe harbors, it was noted that "[m]ost of the sites about which content providers have contacted service providers through the DMCA notice and take down procedure are free sites."[201] More recently, a survey of European service providers revealed that "[t]he size and customer structure seems to influence the number and type of complaints ISPs receive. Whereas corporate orientated ISPs received almost zero complaints, large consumer orientated ISPs receive sometimes hundreds per month in 2003."[202] While the OSPs surveyed were obviously not subject to the requirements of U.S. copyright law, at least some of these apparently received a large volume of copyright complaints from U.S. copyright holders.[203]

Finally, the online context of the DMCA raises special problems for certain particularly vital areas of free speech doctrine. For example, the ease with which copyright holders are able to obtain the identification of alleged infringers[204] threatens the ability of individuals to speak anonymously on the Internet. As some commentators have noted, "[T]here are many reasons for anonymity, including political reasons; anonymising services are used by dissidents under oppressive regimes for example."[205] The DMCA promises similarly repressive effects on fair use, which the Supreme Court has held to be an essential mechanism for effecting protection of First Amendment rights in the context of copyrighted material.[206] Although the fair use defense is still in theory available to the targets of notice and takedown requests, the DMCA's section 512(c) procedure affords speakers an opportunity

200. Audio file: Audio Transcript of Oral Argument at 28:15–28:30, *Rossi*, 391 F.3d 1000 (No. 03-16034), *available at* http://www.internetmovies.com/rossi-vs-mpaa-03-16034.wma 28:15-28:30.

201. OKTAY & WRENN, *supra* note 118, at 12 (describing these free sites further as "a 'breeding ground' for infringing material").

202. AHLERT ET AL., *supra* note 196, at 15.

203. *See id.*

204. *See supra* notes 133–138 and accompanying text.

205. Bortloff & Henderson, *supra* note 196, at 29.

206. *See* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) (stating fair use and idea/expression dichotomy are Copyright Act's embodiments of First Amendment protection).

to air any fair use claims only *after* their material has already been taken down.

IV.
Culpable OSPs? System Design and Secondary Infringement

Statutes tailored too precisely to the problems raised by the technology of the time can easily fall short when applied to the technologies of the present or future. This process may already be underway with the safe harbors. The D.C. Circuit has already recognized this in the context of the Recording Industry of America Association's (RIAA) effort to enforce a section 512(h) subpoena to identify an alleged infringer against an OSP qualifying as a "mere conduit" under section 512(a).[207] Although the court was "not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights,"[208] it noted that "the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works,"[209] and concluded accordingly that "Congress had no reason to foresee the application of section 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along."[210] As drafted, the statute not only fails to address technologies that have developed since its passage, but also embodies particular normative and descriptive notions about how digital networks should work, as well as how they actually do work, notions which are liable to become obsolete.

Scholars have often observed that the designs of particular technologies embody value choices made, consciously or otherwise, by their designers.[211] Most, however, have focused on the impact of design on end users themselves—what might be called a demand-side emphasis. This work has typically been intended either as a normative call to developers to make software more appealing to end users gen-

207. *See* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1237–38 (D.C. Cir. 2003), *cert. denied* 125 S. Ct. 347 (2004).

208. *Id.* at 1238.

209. *Id.*

210. *Id.*

211. *See generally* Helen Nissenbaum, *How Computer Systems Embody Values*, Computer, Mar. 2001, *available at* www.nyu.edu/projects/nissenbaum/papers/embodyvalues.pdf.

erally[212] or more sensitive to individual liberties,[213] or, alternatively, as an untapped tool for policymakers to use in shaping the private behavior of individuals.[214] The underlying assumption in most of this work appears to be that the important question is the effect the values implicit in a given technology may exert on the behavior (and rights) of the technology's end users.

In this part, I will address a different side of the question—namely, the interaction between the law, new technological design, and the behavior of the *providers*, rather than the users, of such technology. New design choices that fail to track the DMCA's assumptions may frustrate the purposes of the Act. In some cases, these choices may even be taken *in order* to frustrate those purposes.

A. Changing OSP Roles

1. Network Design as Conduct

The possibility that an OSP might knowingly *operate* its facilities in a manner conducive to copyright infringement is clearly contemplated in section 512. The statute repeatedly conditions the availability of safe harbor protection on an OSP limiting its involvement with infringing acts to the carrying out of "automatic technical processes"[215] or acts undertaken "at the direction of users."[216] The implication of these provisions is that OSPs will not be liable for infringement that occurs "automatically," but that efforts to intervene actively in particular transactions may carry a risk of liability. This approach is consistent with the view of the opinion Congress labeled the "most thoughtful judicial decision to date"[217]—namely, *Netcom*, which reasoned that in order to have "a working system for transmitting . . . to and from the Internet," it might well be "necessary" for OSPs to "make[ ] temporary copies of . . . works."[218] Both the

212. *See, e.g.*, Mitchell Kapor, *A Software Design Manifesto*, *in* BRINGING DESIGN TO SOFTWARE (Terry Winograd ed., 1996), *available at* http://hci.stanford.edu/bds/1-kapor.html.

213. *See, e.g.*, Lawrence Lessig, *Architecting Innovation*, 49 DRAKE L. REV. 397 (2001).

214. *See, e.g.*, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

215. *See* 17 U.S.C. § 512(a)(2) (2000) (stating that transmission of material must be "carried out through an automatic technical process without selection of the material by the service provider"); *id.* § 512(b)(1)(C) (same for caching).

216. *Id.* § 512(c); *see also id.* § 512(a)(1) (transmissions must be "initiated by or at the direction of a person other than the service provider").

217. H.R. REP. NO. 105-551, pt. 1, at 11 (1998).

218. Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., 907 F. Supp. 1361, 1368–69 (N.D. Cal. 1995).

Netcom court and Congress appear to have concluded that there was only one way to participate in the Internet, and that way involves substantial copying that "cannot reasonably be deterred."[219]

To date, the idea that the initial design choices made by the developers and implementers of these technologies might themselves carry implications for primary or secondary copyright liability has not been well explored. Professor Lior Strahilevitz hints at this possibility in arguing that one of the reasons for the surprisingly high rate of file uploading on peer-to-peer networks is that the developers of Napster, Kazaa, Gnutella, etc. have employed what he labels "charismatic code."[220] He argues that the designers of peer-to-peer networks have used this charismatic code to mask uncooperative behavior and magnify cooperative behavior,[221] presenting a distorted image of the nature and amount of file sharing by users of the software.[222] This makes it appear that a social norm of sharing governs on the network, thereby inducing more cooperative behavior (*i.e.*, file sharing) than would naturally result. In short, the design of these networks has engineered an online social environment that leads to more infringement—seemingly a recipe for contributory liability.

For their part, the courts have been mixed in their treatment of the place of network design choices in a copyright liability regime. Prior to the creation of the safe harbors, the Northern District of California, for example, compared Netcom's design of its network to the owner of a copying machine making the machine available for public use, concluding that such acts could certainly not be grounds for direct liability.[223] The Seventh Circuit, by contrast, held that the developers of file-swapping software Aimster had forfeited the protection of the safe harbors in part because they had "invited [users] to [infringe],

---

219. *Id.* at 1372.

220. Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 507–10 (2003).

221. *Id.* at 557 n.177.

222. *Id.* at 551 ("The architecture of the networks is such that although many users on the networks do not share, the networks create an appearance that sharing is the norm.").

223. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1369 (N.D. Cal. 1995).

> The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement.

Id. (citations omitted).

showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement."[224]

Nevertheless, each of these examples ultimately turns on the demand-side impact not so much of the architecture of the peer-to-peer networks involved, but rather of affirmative aspects of the "ongoing relationship" between OSP and end users of which the end users will be aware, and which may actually lead them to choose to infringe. What is largely missing from the scholarly commentary, the statutory text of the safe harbors, and the case law alike is a clear appreciation of the degree to which an OSP can influence the amount and nature of infringement that its services will enable, not merely by inspiring "volitional" infringing conduct by its users, but by predisposing a system to a particular amount of "automatic" copying through the particular design choices it makes at even the "lowest levels" of its internetworking architecture.[225]

2. *What Is an OSP?*

The definition of OSPs included in section 512(k)(1)(B) is broadly stated, and has been so interpreted by courts.[226] The definition has been satisfied not just by conventional OSPs like AOL,[227] but

224. *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003), *cert. denied*, 540 U.S. 1107 (2004).

225. The idea of "higher" or "lower" levels of a networking architecture reflects any of several "layered" models that network engineers often use to describe their designs. Higher layers handle functions most closely related to human (or application) involvement in a transaction, such as screen formatting, while lower layers address fundamental communication tasks such as electrical signaling. The most popular of these models is the seven-layered OSI model. *See generally OSI Model*, WIKIPEDIA, http://en.wikipedia.org/wiki/OSI_seven_layer_model (last visited Oct. 19, 2005).

226. Section 512(k)(1)(B) defines the term "service provider" as "a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A)", and subparagraph (A) defines the term "service provider" as "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." 17 U.S.C. § 512(k)(1) (2000); *see also* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1099–1100 (D.C. Cir. 2004) (recognizing that DMCA's definition of service provider encompasses broad range of activities, including online retailing); *Aimster*, 334 F.3d at 655 ("the definition of Internet service provider is broad"); ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 623 (4th Cir. 2001) (stating DMCA defines OSP broadly).

227. Ellison v. Robertson, 357 F.3d 1072, 1081 (9th Cir. 2004) (affirming district court ruling that AOL was eligible for safe harbor protection as "conduit service provider").

also by online merchants like eBay[228] and Amazon.com,[229] payment processing services,[230] age verification services,[231] and a publisher of online real estate advertisements.[232] Nevertheless, the DMCA suggests that there are essentially only four types of functions performed by these OSPs: transitory communications, system caching, data hosting, and information location.[233] Specifically, the statute purports to distinguish innocent participation in online networks from potentially culpable or complicit conduct aiding and abetting infringement of copyrights based almost exclusively on the overt activities undertaken in the course of providing these four functions. This narrow approach overlooks some of the most significant activities of OSPs: those associated with the design and implementation of digital networks. Creative design efforts by OSPs can deliver significant gains in performance or functionality to end users, but in so doing they can stretch the definition in section 512 to the breaking point.

Underlying virtually all of today's digital networks are a variety of standardized communications technologies and protocols that determine much—but not everything—about the way in which computers may be connected and communicate with one another. To use a relatively simple example, the Simple Mail Transfer Protocol (SMTP) specification for electronic mail services describes how my system must format and handle mail messages if it wishes to exchange them with other SMTP servers, but does not dictate what sort of equipment I must use; whether my server should be backed up hourly, daily or weekly; whether it should be connected to the Internet via dial-up, DSL, cable, or satellite link; whether it should scan incoming or outgoing messages for viruses; or an almost limitless collection of other configuration options, including whether I should even have an SMTP server at all. Applying this principle to Lawrence Lessig's formula-

228. Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1088 ("eBay clearly meets the DMCA's broad definition of online 'service provider.'").

229. *Corbis*, 351 F. Supp. 2d at 1100 ("[T]here is no doubt that Amazon fits within the definition.").

230. Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1088 n.8 (C.D. Cal. 2004) ("There is no dispute between the parties that IBill is an internet service provider under the DMCA.").

231. *Id.* at 1099 (holding that age verification service qualified under DMCA's mere conduit and information location tool provisions).

232. *See* CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 556 (4th Cir. 2004). *But see* Arista Records, Inc. v. Flea World, Inc., 356 F. Supp. 2d 411, 418 (D.N.J. 2005) (declining to apply OSP safe harbors to operators of flea market).

233. *See* 17 U.S.C. § 512 (2000).

tion of "code as law,"[234] Professor Tim Wu has concluded that code can "redesign[ ] behavior for legal advantage. . . . shaping behavior into legally advantageous forms" and "defin[ing] behavior to avoid legal sanctions."[235] It is this potential for the process of system design to act as "a mechanism of avoidance rather than a mechanism of change"[236] that section 512's operational focus misses.

The development of peer-to-peer networking technology in the wake of *Napster* provides an apt illustration. One of the principal reasons that Napster was unable to qualify for safe harbor immunity was the court's determination that its architecture included an index of user file names that it had the "'right and ability' to police."[237] Successor applications like Aimster, Grokster, and Gnutella have featured architectures tailored to the lessons the Ninth Circuit taught about avoiding liability for copyright infringement. Aimster, for instance, limited the scope of sharing to predefined "buddy lists," and also sought to avoid actual or constructive knowledge of infringement by encrypting transactions occurring with groups of file sharers.[238] Nevertheless, Aimster's system still included a centrally located server engaged in matching requests with available files.[239] Perhaps more

234. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). Lessig uses the term "code" as a convenient reference to "the hardware and software that make cyberspace what it is." *Id.* at 6. The thrust of his argument is that rules embodied in the form of code have a profound effect on the ways in which we experience cyberspace—an effect rivaling that of conventional law. His primary concern is that the institutions and forces inducing changes in code operate largely out of the reach or view of traditional political institutions and are not necessarily motivated by the public interest, and therefore may be crafting a digital environment that will not be amenable to ordinary citizens. This Note focuses on one particular area of divergence: the divide between OSPs as code designers and copyright owners as "ordinary citizens." Paradoxically (or perhaps not so surprisingly), copyright owners are simultaneously one of the main forces transforming the regulatory powers of code through the development of more refined tools for Digital Rights Management, which is a topic beyond the scope of this Note.

235. Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 707–08 (2003).

236. *Id.* at 708.

237. A&M Records v. Napster, 239 F.3d 1004, 1024 (9th Cir. 2001).

238. *See In re* Aimster Copyright Litig., 334 F.3d 643, 646, 650 (7th Cir. 2003). The Court described Aimster's dependence on and use of the AOL Instant Messaging buddy system to establish connections and limit the scope of file sharing, but noted that "[i]f the user does not designate a buddy or buddies, then all the users of the Aimster system become his buddies; that is, he can send or receive from any of them." *Id.* at 646; *see also* John Borland, *File-Swapping Aimster to Tap Into ICQ, Napster*, CNET NEWS.COM, Sep. 14, 2000, http://news.com.com/2100-1023-245738.html?legacy=cnet (last visited Oct. 20, 2005) ("The Aimster software lets people create limited, trusted groups of 'buddies' with whom they can swap music and other files in much the same way that Napster's tens of thousands of members typically trade anonymously.").

239. *In re Aimster*, 334 F.3d at 646–47.

successfully, Grokster and Gnutella have tried to eliminate the central index server that proved Napster's undoing, replacing it with "supernodes" (Grokster)[240] or something approaching "true" peer index sharing (Gnutella),[241] which will essentially make the resulting peer-to-peer networks self-sustaining, with no ongoing operational role for the developer, and presumably no grounds for forfeiture of the safe harbor protections. Similarly, peer-to-peer clients whose architecture is based on the BitTorrent program, first introduced by Bram Cohen, share a design that *automatically* makes virtually every user participate in the network as both a downloader and uploader, distributes the indexing function among unaffiliated and uncontrolled "trackers," and leaves no centrally controlled role at all.[242]

Assuming a successful, "pure" peer-to-peer system emerges, it seems likely that it would be within the power of its developers to use the safe harbors as a shield against liability for infringing acts of its users. Such a system would most properly be analyzed under section 512(d), the provision immunizing "information location tools."[243] Certainly, such software could fairly be described as "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools."[244] Since all transactions would take place without involvement by any central en-

240. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2771 (2005).

241. *See generally* Wu, *supra* note 235, at 717–37. Wu describes the challenges of designing a "pure" peer-to-peer network that will function on a large scale and characterizes Gnutella, which "delivered a radically decentralized design" in "an intentional effort to create a filesharing protocol that could avoid a lawsuit," *id.* at 731, as the only peer-to-peer network so far that has implemented a truly "pure" peer-to-peer architecture. Other systems are "hybrids that balance control and decentralization" and stand as "programs of great sophistication, attuned carefully to the doctrines of copyright." *Id.* at 720, 734. Wu notes that "the fact that GnutellaNet remains unsued endows it with an aura of continued importance in the filesharing story," but appears to discount the software, and possibly the entire "pure" approach, as a feasible file sharing alternative. *Id.* at 737. He feels that "[t]oday's successful P2P filesharing applications approach, but do not achieve, a pure P2P model." *Id.* at 717.

242. *See* Bram Cohen, Incentives Build Robustness in BitTorrent 2–4 (May 22, 2003), http://www.eecs.harvard.edu/~mema/courses/cs264/papers/bitTorrent-econ2003.pdf (describing architecture and algorithms used in BitTorrent approach).

243. 17 U.S.C. § 512(d) (2000). *But see* Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660(SHS), 2002 WL 1997918, at *10 (S.D.N.Y. Aug. 29, 2002) (suggesting that provision of "services not provided by traditional search engines" may disqualify OSP from immunity under § 512(d)).

244. 17 U.S.C. § 512(d). While the provision goes on to list qualifying tools "including a directory, index, reference, pointer, or hypertext link," this list is clearly non-exclusive, so the absence of a centrally located version of any of these should not automatically disqualify a particular peer-to-peer tool. In any case, "pure" peer-to-peer software would almost certainly work by creating such directories, indexes, or

tity, the provider of such a system would have no idea what materials the individuals using its software were exchanging, much less "actual knowledge" that any of those materials were infringing, thus presumably satisfying the safe harbor's first condition.[245] Avoiding a business model that generates revenue through advertising, or any other method linked to the popularity of infringing uses, would probably enable the OSP to satisfy the second condition, which requires that it derive no direct financial benefit from the infringing conduct of its users.[246] While Aimster's decision to manufacture its own lack of knowledge by engineering encryption into its system was deemed "willful blindness,"[247] such a step would not be necessary in a "pure" peer-to-peer environment. Assuming a mechanism for remotely disabling copies of the software residing on end user computers was simply not present in the system, the OSP would presumably not be disqualified from safe harbor protection on the ground that it failed to remove or disable access to allegedly infringing material, as indicated in sections 512(d)(1)(C) and (d)(3).[248] Even if such a system were held to have violated the expeditious removal condition, it might still be able to qualify for protection as a "mere conduit" under Section 512(a). The text of that section makes immunity available to OSPs responsible for "transmitting, routing, *or providing connections*,"[249] which some courts have interpreted liberally to mean merely making a connection possible.[250] Thus, a peer-to-peer system that

links on a dynamic basis, as end user machines "discover" the locations and contents of their peers on the network.

245. *Id.* § 512(d)(1)(A).

246. *Id.* § 512(d)(2).

247. *In re* Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003).

248. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1166 (9th Cir. 2004) ("[a] duty to alter software and files located on one's own computer system is quite different in kind from a duty to alter software located on another person's computer"). While the Supreme Court, in reversing the Ninth Circuit, did point to the absence of any efforts by the OSPs to "develop filtering tools or other mechanisms" to reduce infringement by their users as evidence of illegal intent, it did not suggest that a duty existed to reach out and alter software that had previously been distributed to users. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2781 (2005).

249. 17 U.S.C. § 512(a) (emphasis added).

250. *See, e.g.*, Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1091–92 (C.D. Cal. 2004) (rejecting argument that § 512(a) safe harbor applies only to OSPs engaged in transmission of infringing material, and holding that payment processing company qualifies, since it "provides a connection to the material on its clients' websites through a system which it operates in order to provide its clients with billing services"). The court used the same reasoning to extend the § 512(a) safe harbor to an age verification service. *Id.* at 1098–99. As expressed by the court, this reasoning would seem to cover virtually any information location tool, as well as transmission facilities. This reading would appear to render § 512(d) superfluous, suggesting that,

meets the functional requirements of section 512(d) is a real possibility.[251]

What this exercise in statutory interpretation misses is the question of *why* such a system would exhibit this particular set of design elements. The motivation of peer-to-peer developers was raised as an issue in the *Grokster* appeal, however. The recording industry, along with some amici, argued that Grokster and Streamcast deliberately built their business models on copyright infringement, and that this fact should preclude them from avoiding liability for contributory infringement.[252] This notion appeared to generate considerable interest among the Justices during oral arguments before the Supreme Court,[253] so it is not surprising that it also seemed to be one of the majority's principal reasons for inferring the defendants' intent to

---

notwithstanding the language actually used by the court, its holding depended also on the fact that access to the infringing material was available *exclusively* via the payment or age verification service, and would not have extended to a conventional search engine like Google. In either case, a peer-to-peer system which provided the only means to access its users' files would qualify for safe harbor protection.

251. It could be, on the other hand, that any system that was sufficiently "pure" to guarantee von Lohmann's "plausible deniability," *see supra* note 159 and accompanying text, would be incapable of qualifying for safe harbor protection for another reason, namely its intrinsic inability to "reasonably implement" the policy of termination for repeat infringers that is a threshold requirement of section 512(i)(1)(a). *See* 17 U.S.C. § 512(i)(1)(a) (2000). While it is easy enough to imagine scenarios where a provider might fall into such a catch-22, it seems rash to presume that technologists will lack the creativity to *ever* fill this apparent gap.

252. *See* Petition for Writ of Certiorari at 5–6, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005) (No. 04-480) (Grokster and Streamcast launched their services expressly "to capture the flood" of Napster users in wake of that service's shutdown); Petitioners' Reply Brief on Petition for Writ of Certiorari at 2–5, *Grokster*, 125 S. Ct. 2764 (No. 04-480) (Grokster's business model, which depends on *maximizing* infringement in order to drive advertising revenue, "is utterly unlike that of one who merely sells a staple article of commerce"); Brief for Progress & Freedom Foundation as Amicus Curiae Supporting Petitioners at 9–10, *Grokster*, 125 S. Ct. 2764 (No. 04-480) (urging distinction between peer-to-peer technology, which "[e]veryone accepts. . . is indeed legitimate and useful," and "the ancillary features wrapped around the core of P2P technology to make it a paying commercial enterprise," which should not be immunized).

253. *See, e.g.*, Transcript of Oral Argument at 26–28, *Grokster*, 125 S. Ct. 2764 (2005) (No. 04-480), *available at* http://www.supremecourtus.gov/oral_arguments/argument_transcripts/04-480.pdf (questioning of Solicitor General by Justices Scalia and Souter on whether it should matter that Napster example preceded development of Grokster, and how "substantive standard" could be articulated that would distinguish between cases like that, and less troubling cases where no prior history of overwhelmingly infringing use existed); *Id.* at 29 (noting by Justice Scalia of significance of fact that Grokster's "[past acts] are what have developed [its] current clientele"); *Id.* at 36 (suggesting by Justice Kennedy that Grokster's position would amount to endorsement of dubious idea that "unlawfully expropriated property can be a legitimate part of the startup capital" of OSP).

profit from their users' infringing conduct. The Court in its decision pointed both to evidence that the OSPs deliberately targeted "a known source of demand for copyright infringement, the market comprising former Napster users,"[254] and the fact that they derived revenue from advertising that increased along with the volume of infringing activity.[255] While none of this analysis suggested that peer-to-peer network design was itself inherently suspect, and no claim of safe harbor protection was before the Court, *Grokster* may pave the way for some courts to engage in a fuller consideration of whether particular technology design choices reflect an intent to infringe.

B. Enhancing the Internet: How New Technology Has Changed the Face of Digital Copyright Infringement

We have observed that the language Congress chose to describe the different OSP functions it wished to privilege reflects the state of the Internet in the mid-1990s, and therefore entirely fails to address some newer technologies—for example, peer-to-peer networks. Nevertheless, even in the limited context of the categories the statute expressly recognizes, the pace of technological development has led to new variations on old networking services that may already sidestep the spirit, if not the letter, of the DMCA. The text of the statute incorporates an implicit assumption that there is essentially one right "division of labor" in communicating data between two points. This implied model is showing signs of strain.

The "conventional" model of Internet communication can be described as follows. Works are uploaded by one party (which we will call the "poster") to a web site that is stored on the computer of a web-hosting OSP. This OSP is providing the function covered by section 512(c). When another party (the "requester") wishes to view the work,[256] its computer sends a request that is passed by its access provider to the web hoster via the Internet. The web hoster then accesses the corresponding file on its system, and transmits a copy of the work via the Internet back to the requester's access provider, which relays it to the requester. In this scenario, the requester's access provider (along with an indefinite number of intermediate OSPs on the Internet path connecting it to the web hoster) is plainly providing functionality covered by the "mere conduit" provisions of section 512(a).

254. *Grokster*, 125 S. Ct. at 2781.
255. *Id.* at 2781–82.
256. The requester may have located the work by utilizing an information location service or search engine.

In addition, since the access provider may have other subscribers interested in downloading the work, it will most likely have activated some form of automatic "caching" functionality whereby temporary copies of works its users frequently seek to access are stored locally on the access provider's system. This will enable the access provider to improve the apparent response time to subsequent requesters of the work by transmitting from the local copy without actually duplicating the entire upload-request-and-download-file process between it and the web host. The caching process is transparent to the requester, who performs precisely the same steps to access the work from cache as to access it all the way from the original host, and in most cases will not know where a particular copy originated. The file access and transmission time saved by skipping these intermediary steps can often be significant. This is the system-caching function protected by section 512(b).[257]

As described, these functions can be—and usually are—carried out via software tools that *operate* without any human intervention, though each requires substantial human effort to design, install, configure and tune for optimal performance. Accordingly, in the interest of "ensur[ing] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand," Congress carved out the particular areas of limited liability they chose.[258] These reflect the understanding that "[i]n the ordinary course of their operations service providers must engage in" these functions.[259]

1. Co-Location

While the description above provides a reasonable sketch of the way the majority of web traffic flowed in the first half of the last decade, the subsequent explosion of web-based development for e-commerce and new media applications quickly began to strain the boundaries of this model. The most important developments resulted from the efforts of the various participants in networking transactions to improve the overall performance and predictability of their portion of the network by redistributing the ownership and control of the familiar functions in ways tailored to the particular needs of the parties involved.

257. Similar automated processes carried out by intermediary OSPs in the interest of performance would also fall within the scope of the § 512(b) safe harbor.
258. S. REP. NO. 105-190, at 8 (1998).
259. *Id*.

The facts of *Diebold* provide a real-world example of one such development, as well as a useful illustration of the sorts of interpretational problems these developments can cause. Two of the OSPs to whom Diebold sent takedown notices concerning the links on the IndyMedia site were Online Policy Group (OPG) and Hurricane.[260] OPG provided what are known as "co-location" services to IndyMedia. Co-location is a popular arrangement in which the OSP simply provides a physical location, power, and a physical connection to the Internet for a server supplied and usually managed by the customer.[261] This sort of arrangement does not fit neatly into the safe harbors laid out in section 512. The closest fit would seem to be the "mere conduit" harbor of section 512(a). Nevertheless, even though none of the contested files in *Diebold* were stored on a computer owned by OPG,[262] the provision of physical space, power, environmental protection, and so forth at least comes close to blurring the distinction Congress sought to make between "intermediaries"—to whom the safe harbor was intended to be available—and the initiators or recipients of transmissions—to whom its protections were to be denied.[263] In addition, the statute imposes no requirement that OSPs qualifying for the section 512(a) safe harbor comply with section 512(c)(3) takedown requests.[264]

Since it "only provid[ed] Internet connectivity to [IndyMedia's] computer through colocation, OPG could not comply [with Diebold's

260. Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1198 (N.D. Cal. 2004).

261. *See* Web Host Industry Review, Glossary of Web Hosting Terms, http://www.thewhir.com/find/web-hosts/articles/glossary.cfm (last visited Oct. 20, 2005) (defining co-located hosting: "You are responsible for providing the physical hardware and network administration; the hosting company will provide you with the rack space and Internet connection."). A related service is known as "dedicated hosting," in which the OSP leases an entire server dedicated exclusively to the web site(s) of a single customer. *See* CNET, Web Hosting Buying Guide: What Types of Hosting Are Available?, http://reviews.cnet.com/Web_hosting_buying_guide/4520-6540_7-5138854-2.html?tag=bnav (last visited Oct. 20, 2005) ("Dedicated hosting means just that: the server is yours and yours alone. . . . Many providers in this space also sell colocation services where you bring the servers and staff, while they provide a secure facility with rack space, electricity, and all the bandwidth you can eat."). Dedicated hosts can be managed by either the OSP or the customer, and the ramifications of such design decisions under the existing safe harbors are at best unclear.

262. This would seem to disqualify the arrangement from the § 512(c) safe harbor for data stored on behalf of users.

263. *See* S. REP. NO. 105-190, at 41 ("In this context, 'intermediate and transient' refers to such a copy made and/or stored in the course of a transmission, not a copy made or stored at the points where the transmission is initiated or received").

264. *See* 17 U.S.C. § 512(a), (c)(3) (2000); *cf.* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1236–37 (holding that mere conduit OSPs need not comply with section 512(h) subpoenas to identify infringer).

takedown request] by merely disabling or removing the hyperlink and related information demanded by Diebold. OPG's only option to comply with the demand was to cut off IndyMedia's Internet connectivity entirely."[265] The court's finding that Diebold had materially misrepresented its claim of copyright in the notices it issued ultimately rendered the precise relationships between the OSPs in the case non-dispositive, meaning that the question of which of these OSPs, if any, would have qualified for (or been barred from) which of the safe harbors remains unanswered. Nevertheless, the district court felt compelled to point out that this "technical distinction does serve to illustrate the ramifications for free speech of Diebold's demands."[266]

2. *Content Delivery Networks and Related Technologies*

Co-location is by no means the only service being offered by OSPs that challenges the statutory safe harbors. New forms of caching have become commonplace as posters, web hosting companies, and other service providers alike have come to appreciate the performance gains that can be enjoyed by the pre-emptive creation and judicious distribution of cached copies of digital works. Rather than depending on the caching capabilities of the various OSPs providing Internet access to their requesters, many posters today choose to use technologies that reduce response time by affirmatively creating additional copies of digital works either on their own or their web hosting OSP's computers (a practice known as "reverse caching"), or on the geographically dispersed servers of another type of OSP known as a "content delivery network" (CDN) provider.[267]

Before exploring why such caching tactics have become so popular, and why they may have implications for copyright infringement, it may be useful to consider by way of comparison the decision facing a "bricks-and-mortar" video rental establishment wishing to make the latest blockbuster available to its patrons. The proprietor of such an establishment must determine how many copies of the video to order. Since a single physical video can only be borrowed by one patron at a time, a store wishing to reduce the average time its patrons must wait for their turn does so by placing more than one copy on its shelves. If there are too few copies, then most patrons will not be able to rent the

265. Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1198 n.2 (N.D. Cal. 2004) (quoting OPG's Complaint).
266. *Id.*
267. *See generally* Carolyn Duffy Marsan, *Cashing in on Internet Caching Services*, NETWORK WORLD, Oct. 25, 1999, http://www.networkworld.com/archive/1999/78080_10-25-1999.html.

video when they wish to, and may turn to the competition for rental services as a result. The more copies the store acquires, the shorter the average wait will be for each customer. In addition, having a larger supply of copies on hand enables the store to handle peak demand that may accompany the initial release of the movie, as well as the risk that some copies will be lost or damaged.

Web posters face essentially the same sort of decision with respect to digital works. By making additional copies of the work available on additional computers or drives at appropriately distributed locations on the Internet—locations that are "closer" to their requesters than the disk drives of their web server—they can reduce the average amount of time requesters must wait in order for their download requests to be serviced and delivered. In much the same way that the requester's access provider reduces the time its subscribers must wait for popular works by caching copies on its local servers and thus bypassing the steps linking it to the web server, the poster reduces the turnaround time by bypassing some of the *other* steps in the path connecting the requester's computer to the work stored in a file on the web server. In a "reverse caching" scenario, this is accomplished with automated processes that create and maintain copies of a site's most popular pages in a server's RAM, from which they can be transmitted without the need to physically open and retrieve an original file located on a disk drive.[268]

Content Delivery Networks (CDNs) extend this principle by an order of magnitude by not only eliminating the transmission steps immediately adjacent to the requester and poster, but also replacing enormous chunks of the publicly-shared Internet with a high-performance, private network. They do this by creating "shadow" networks consist-

268. *See* MICROSOFT, ACCELERATING THE INTERNET WITH ISA SERVER 2004 WEB CACHING 1–2 (2004), http://download.microsoft.com/download/7/a/d/7ad19879-0ca9-4541-890b-8c07887e02ae/ISA2004SE_wp_webcaching.doc ("[The ISA Server 2004 Web cache] improve[s] network performance and the end-user experience by storing frequently requested Web content in a local cache. . . . [Web caching] speeds up Internet access by bringing the cache closer to the user."). For a more detailed discussion of the mechanics of reverse caching functions as implemented with Microsoft technology as of 2004, *see id.* at 4–5. In many instances, the RAM copies will be located on a physically different computer than the one housing the original disk copy. Indeed, the original disk file often will be located on a drive that is not even physically part of the computer acting as the web server at all. While the implications of such arrangements (which are by no means limited to Internet applications) for copyright liability in light of cases like *MAI Systems*, *see supra* Part I.A., are potentially important, they are beyond the scope of this Note. In any event, the implications with respect to the section 512 safe harbors will be the same: performance is improved by moving copies of a site's most popular material closer to the end user on the Internet, cutting out some of the "front end" steps involved in "normal" web transactions.

ing of privately owned nodes dispersed to a variety of geographic locations that are simultaneously connected to both the Internet and the private network. CDNs also deliver higher performance by placing copies of popular material on their own servers, which are physically located close to where requesters are anticipated to be.[269] When a requester in Los Angeles, for example, tries to download a work from the server of a poster located in London, a CDN can seamlessly intercept the request and deliver the desired material from a cached copy located on one of its servers in Los Angeles, thereby eliminating all of the steps required to move data from London to Los Angeles via the Internet. Thus, like the video store owner, a web poster can reduce the wait time for its customers by offering more copies of the material on its website.

Returning to the bricks-and-mortar example, our video store can obtain its ideal supply of tapes and DVDs either lawfully, by purchasing a sufficient number of copies (or licensing the right to make them itself) from the copyright owner, or unlawfully, by making its own unauthorized copies. To the extent that the proprietor is uncertain about the demand for the new movie, or expects that demand will fluctuate greatly, he may be strongly motivated to minimize his risk by ordering only a small number of legitimate copies and planning to make additional copies if and when they are needed. In such a situation, the liability incurred by the store itself for directly infringing the copyright in the movie, or by a duplication service for indirectly infringing by materially assisting in the unauthorized duplication, is reasonably clear. Few would argue that copyright law in any way implicitly authorizes the store to make copies whenever it sees fit simply because future demand for the work is uncertain. The basic principle is straightforward, but still worth repeating: the store can provide better service to its customers (for which it will presumably be compensated) by having more copies of the video in its possession, but a copyright owner has the right to be compensated for those copies.

The same basic performance principles apply to reverse cachers and CDNs. A poster wishing to improve the performance of its website can select from several general approaches, including upgrading

269. *See generally* Doug Kaye, *What Web Hosting Customers Want*, WEB HOST INDUSTRY REVIEW (2005), http://www.thewhir.com/reseller/articles/want.cfm ("[The late '90s] saw the emergence of content delivery networks (CDNs) . . . . [which] bypassed the slow and unreliable core of the Internet, and delivered content from as close to visitors as possible."); Carolyn Duffy Marsan, *Caching Debate Rages*, NETWORK WORLD, Apr. 17, 2000, http://www.networkworld.com/news/2000/0417necp.html (describing one controversial aspect of mechanism used by leading CDNs to bypass public Internet); Marsan, *supra* note 267.

equipment or adding bandwidth to its own Internet connection, among other means of improving the actual capacity of its own system. Alternatively, it could decide to use either reverse caching or a CDN to provide better service to its clientele *by making more copies of a work available to them*. Posters who decide to do this with material they own or are licensed to reproduce are clearly entitled to reap the benefits of such an architectural choice. If, however, the posters do *not* own the rights, there is no obvious reason to presume that the owners of the copyrights involved are not entitled to share in the benefits these additional copies provide.

Similar arguments can be advanced concerning analogous networking technologies and design strategies aimed at enhancing performance or reducing system downtime, such as site mirroring and load balancing—techniques that coordinate the activities of multiple servers hosting copies of a particular web site in order to enable them to perform the same tasks interchangeably and transparently to the end user.[270]

To the extent it considered anything like these technologies at all, Congress lumped them into the "system caching" provisions of section 512(b). The safe harbor for system caching activities eliminated the infringement liability of OSPs who engage in "intermediate and temporary storage of material" being transmitted between two other parties, provided that the act of storage occurs as part of an "automatic technical process" and the OSP doing the caching neither initiates the transmission nor changes the data transmitted in any way.[271] The underlying presumption seems to have been that a certain amount of "passive" copying was an inevitable byproduct of communications on a digital network. In practice, however, this view oversimplifies the ways in which caching technologies like those just described are being applied. Each of these techniques involve storage that is "intermediate and temporary," undertaken by an "automatic technical process" in proximate response to a transaction initiated by either of two third

270. *See* Web Host Industry Review, Glossary of Web Hosting Terms, http://www.thewhir.com/find/web-hosts/articles/glossary.cfm (last visited Oct. 20, 2005) (explaining that "[a] mirror site is an exact copy of another FTP or Web site" that is "used to offset/spread traffic load on busy Web sites," and defining load balancing as: "[d]istributing data across a network of servers in order to ensure that a single Web server does not get overloaded with work, thereby affecting performance").

271. 17 U.S.C. § 512(b) (2000); *see also* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) ("The DMCA was enacted . . . to provide 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.").

parties. These OSPs deliver the same material the poster's web host would deliver.[272] What the statute's definition misses, however, is the fact that these techniques, automatic though they may be in *operation*, represent conscious design and implementation choices reached jointly by the posting parties and their OSPs. The fact that a leading CDN provider like Akamai Technologies offers a shadow network of 14,000 servers to its customers, rather than 4,000 or 40,000, is not forced on these companies by any requirements of the Internet's underlying standards.[273] Rather, it reflects a conscious assessment by the customers and OSPs of the value of the ability, in the words of one

272. In practice, some CDN applications involve assembly of finished web pages from component materials stored on more than one caching server—usually in an effort to customize the resulting page based on the requester's geographic location (for example, by presenting localized advertising). While in one sense such a process seems to violate the statute's directive that the OSP ensure that materials are forwarded "without modification to its content from the manner in which the material was transmitted from the [posting party]," 17 U.S.C. § 512(b)(2)(A), the assembly is performed according to the poster's instructions, so the result is presumably identical to what the poster's web site would send if no CDN services were employed. Such an interpretation may be strengthened by § 512(b)(2)(B), which directs erstwhile system cachers to comply with "rules concerning the refreshing, reloading, or other updating of the material when specified by the [posting party]." *See* S. REP. NO. 105-190, at 43 (1998) ("The Committee intends that this restriction apply, for example, so that a service provider who caches material from another site does not change the advertising associated with the cached material on the originating site *without authorization from the originating site*.") (emphasis added).

273. Indeed, many would argue that such a choice is presumptively invalid, or at least normatively suspect, since it violates the principle of "end-to-end," which "counsels that the 'intelligence' in a network should be located at the top of a layered system—at its 'ends,' where users put information and applications onto the network. The communications protocols themselves (the 'pipes' through which information flows) should be as simple and as general as possible." Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930–31 (2001); *see also* J.H. Saltzer et al., *End-to-End Arguments in System Design* (1981), *available at* http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf (seminal articulation of end-to-end principle). Many observers in both law and technology have advocated a less dogmatic view (and argue persuasively that the end-to-end principle was always *intended* to be flexible in application). *See, e.g.*, SAMRAT BHATTACHARJEE ET AL., ACTIVE NETWORKING AND THE END-TO-END ARGUMENT 1 (1997), http://www.cc.gatech.edu/projects/canes/papers/icnp97.pdf (arguing that active networks, which "can be tailored to the user's requirements," "are a natural extension of [the end-to-end] design principle"); Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate*, 3 J. TELECOMM. & HIGH TECH. L. 23, 26 (2004) (arguing that end-to-end principle was originally intended to be applied only on case-by-case basis). While a detailed discussion of the end-to-end debate is beyond the scope of this Note, it is worth observing (without taking sides) that this is just one more example of the myriad ways in which the practical development of networking technologies is failing to adhere to the "rules" (or "code") as these are understood by particular observers.

content provider, "to enrich the user experience without adding to our infrastructure."[274]

C. Marketing Copyright Infringement?

The increased speed, flexibility, and fault tolerance provided by technologies such as those just described are not an "automatic" requirement of participation on the Internet—indeed, free and low-end web hosting providers typically offer few or none of these benefits, or offer them only at higher subscription costs.[275] This fact raises additional questions: to what extent are OSPs marketing their services based on their potential for infringement, and what are the consequences under the DMCA if they are doing so?

The legislative history of the DMCA makes it clear that Congress was not interested in punishing OSPs who receive from infringing customers "the same kind of payment as [from] non-infringing users of the provider's service."[276] The Senate Report specifically mentions "one-time set-up fee[s] and flat periodic payments for service from a person engaging in infringing activities" as well as "fees based on the length of the message (per number of bytes, for example) or by connect time" as business models that "would not constitute receiving a 'financial benefit directly attributable to the infringing activity'" for purposes of determining safe harbor eligibility under the statute.[277] This would tend to suggest that as long as OSPs apply identical pricing models to their customers regardless of whether their sites in-

274. Akamai Technologies, Power Up Integrated Marketing Campaigns, http://www.akamai.com/en/html/customer/columbia_house.html (last visited Mar. 26, 2005) (quoting statement of Walter Kerner, Vice President, Technical Services, Columbia House).

275. *See* CNET, Web Hosting Buying Guide: What Types of Hosting Are Available?, http://reviews.cnet.com/Web_hosting_buying_guide/4520-6540_7-5138854-2.html?tag=bnav (last visited Oct. 20, 2005) (describing typical features and associated costs for various levels of web hosting service); *see also* CNET, Web Hosting Buying Guide: What Type of Site Do I Want?, http://reviews.cnet.com/Web_hosting_buying_guide/4520-6540_7-5138854-3.html?tag=bnav (last visited Oct. 20, 2005) ("If you're doing business over the Web, you generally need to pay for the privilege. . . . if e-commerce is your organization's lifeline, you'll want the best hosting solution you can afford." Site owners are urged to pay extra to "make sure you have redundant systems in different locations. If your Web server in Los Angeles goes down, the one in Chicago can pick up the slack. You also want to make sure your host has built-in redundancy—multiple high-speed Net connections and power generators, at least."). It is this potential, arising out of such tiered service levels, for discriminatory treatment of Internet traffic by OSPs that Lemley and Lessig find especially troubling, since it may impede future innovations by outsiders. *See* Lemley & Lessig, *supra* note 273, at 932–34.

276. S. REP. NO. 105-190, at 44 (1998).

277. *Id.* at 44–45.

fringe, their activities are of the sort Congress intended to privilege. Nevertheless, while it is true that the services provided by OSPs like CDNs are available on equal terms to both infringing and non-infringing web site owners, it is also true that solutions such as these—designed and tailored from the outset to meet the specific performance needs of an individual customer's particular data, audio, video, or e-commerce application by making and distributing an optimal number of copies—suggest a considerably more active role in any unlawful copying than Congress anticipated for "passive" OSPs. Indeed, in the same discussion of "financial benefit" cited above, the Senate Report concluded that the phrase "*would* however, include any such fees where the value of the service lies in providing access to infringing material."[278]

It is clear, too, that many of today's OSPs are drafting their marketing materials in ways that suggest awareness that their services will be sought after by infringers. One provider of online storage services, for example, invites potential customers to "[b]uild a music library online," noting that their service permits customers to "stream [their] own music," including "songs you'd like to buy" (but have not, and presumably will not).[279] The pitch continues:

> A click of the mouse and you've got music. Collect your favorite songs or whole albums. Upload and store your MP3's in minutes, creating your own personal library . . . . Send a playlist to your web-enabled cellphone. Then listen to your tunes straight from your Xdrive! Now any wireless device can become a traveling jukebox. With Xdrive, the music just doesn't stop![280]

For those who are still unsure, the pitch concludes by distinguishing its services from other free or low-cost options a customer might consider: "Your music collection couldn't be safer. Xdrive backs up digital music files, protects them with 128-bit encryption and stores them in a disaster-proof, state-of-the-art data center. Plus a password protection system puts you in control."[281]

While language like this may be extreme enough to run afoul of the DMCA's requirement that an OSP "do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers,'"[282] since it could fairly be read as "invit[ing] them to do so, [and]

278. *Id.* at 45 (emphasis added).
279. Xdrive, Explore Music, http://www.xdrive.com/explore/music.jsp (last visited Oct. 20, 2005).
280. *Id.*
281. *Id.*
282. *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003) (citing 17 U.S.C. § 512(i)(1)(A)).

show[ing] them how they could do so with ease using its system,"[283] it is not clear whether the violation would actually cost Xdrive anything, so long as the company cooperated with takedown requests. In addition, more subtle marketing appeals are not uncommon.[284]

D. Other Developments

The facts of *CoStar Group, Inc. v. LoopNet, Inc.*[285] provide another illustration of the sorts of differences that may be emerging among OSPs. In that case, the defendant LoopNet was an organization that provided access to online advertising and publishing services to realtors. It described itself as a "web hosting service that enables users who wish to display real estate over the Internet to post listings for those properties on LoopNet's web site."[286] Its customers could submit text-only ads, which would be immediately uploaded to the site. Unlike some web hosting services, however, LoopNet chose to subject each photograph submitted to review by one of its employees prior to final upload.[287] While a majority of the Fourth Circuit panel held that such conduct did not disqualify the OSP from the benefits of the safe harbor, a forceful dissent pointed out that LoopNet's conduct would have clearly constituted secondary infringement in the bricks-and-mortar world, since the provider "remain[ed] the pivotal volitional actor, 'but for' whose action, the images would never appear on the website."[288] The dissent questioned the conclusion that the mere fact that the uploading was initiated by another should alone be enough to absolve the OSP of its active involvement in the infringement.[289] This echoes some of the concerns discussed earlier about the role of caching service providers who actively design and build systems that subsequently automatically make large numbers of copies on behalf of primary infringers with whom they maintain continuing relationships.[290]

Finally, current developments suggest that the very identity or status of OSPs may undergo significant transformation in the near fu-

283. *Id.*
284. *See, e.g.*, Akamai Technologies, Akamai Media Delivery, http://www.akamai.com/en/html/business/media_delivery.html (last visited Oct. 20, 2005) (recommending Akamai's CDN service as ideal for posters whose customers are "[c]onsumers [who] are fickle and want to consume media how they want, when they want, and where they want").
285. CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004).
286. *Id.* at 547.
287. *Id.*
288. *Id.* at 560 (Gregory, J., dissenting).
289. *Id.*
290. *See supra* Part IV.B.2.

ture, as governments in many municipalities begin providing broadband networks to their citizens as a form of public utility.[291] These efforts have so far involved public-private partnerships, with the public entity acting as an upstream bandwidth provider for private OSPs, who resell the bandwidth to private customers packaged along with their other service offerings.[292] As the *Diebold* case demonstrates, however, copyright owners may well seek to act via section 512(c) takedown notices or section 512(h) subpoenas issued to these publicly-operated OSPs.[293] If this happens, the OSP's status as an arm of government could raise a number of difficult questions. Would disabling a website in compliance with a proper takedown notice constitute a First Amendment violation if carried out by a city agency? Would either takedown or denial of access to repeat infringers amount to a "taking" under the Fifth or Fourteenth Amendment? Would federal privacy statutes preclude a publicly owned OSP from complying with a section 512(h) subpoena? Clearly none of these concerns are addressed by the language of section 512.

V.
ALTERNATIVES

On the surface, the two main problems identified in this Note appear to have little in common. On the one hand, I have argued that, by offering near-complete immunity to OSPs who blindly comply with the requests of copyright holders, the procedures outlined in section 512 of the DMCA tilt sharply in favor of the rights of copyright holders, at the expense of the rights of those seeking to use digital networks to disseminate their message. At the same time, I have also observed that the statute was drafted to deal with OSP behaviors and

291. *See, e.g.*, Adam Werbach, *Should Municipalities Get in the Wi-Fi Business? Wireless Wonder at a Fraction of the Cost*, S. F. CHRON., Apr. 15, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/04/15/EDGM7C7UJ11.DTL (arguing for publicly-provided wireless in San Francisco); *Lobbyists Try to Kill Philly Wireless Plan*, MSNBC, Nov. 23, 2004, http://www.msnbc.msn.com/id/6570011 ("[D]ozens of cities and towns have either begun or announced such plans—from San Francisco to Chaska, Minn., to St. Cloud, Fla.").

292. *See, e.g.*, Wireless Philadelphia Executive Committee, Wireless Philadelphia Business Plan: Wireless Broadband as the Foundation for a Digital City 32–40 (Feb. 9, 2005), http://www.phila.gov/wireless/pdfs/Wireless-Phila-Business-Plan-040305-1245pm.pdf. Wireless Philadelphia proposes a hybrid "Cooperative Wholesale" business model, in which the city would provide inexpensive access to its wireless network to private OSPs on a wholesale basis, who would then contract directly with retail end users. Thus, the city's facilities would most likely provide only "mere conduit" services, and it will be the private OSPs who provide other services, such as system caching, hosting, and information location. *Id.*

293. *See supra* notes 171–182 and accompanying text.

practices as they existed in 1995, and many of today's mainstream networking practices resist the confines of the categories defined a decade ago.

In truth, however, these problems both arise out of the same shortcoming in the DMCA drafting process: it did not include all the parties the DMCA affects today. While section 512 most likely represents a reasonable balancing of the interests of the OSPs of 1995 and the copyright holders of 1995, theirs are not the only interests at stake today. It should come as no surprise that a compromise reached without the participation of end users or newer types of OSPs is ill-suited to their needs and circumstances. At the same time, compromises are hard to come by. Parties that worked so hard to craft and adapt to the current regime will be loath to discard it and start fresh, and it would surely be impractical to embark on a new effort to negotiate a compromise involving even *more* parties with even more divergent interests at this juncture. The next best alternative would be to attempt to adjust the existing regime in order to artificially create incentives to act as proxies for the interests of end users and novel technology implementers.

A. Reducing the Incentives to Overdeter User Infringement

As I have argued, the safe harbor regime makes it easy and often efficient for both OSPs and copyright holders to ignore the interests of Internet users in free, online speech.[294] A solution to this problem would need to address both groups. One objective would be to engender more faithful convergence of the interests of OSPs and their customers.[295] Another would be to give copyright holders strong incentives to seek relief responsibly.

One step that could further both of these objectives would be to convert section 512's reliance on subjective, good faith standards for takedown or counter notification into a slightly more rigorous requirement. The present formulation could be amended by borrowing the

294. *See supra* Part III.B.

295. *Cf.* Block v. Cmty. Nutrition Inst., 467 U.S. 340 (1984). The question in *Block* was whether a dairy regulation statute permitted milk consumers to challenge FDA regulatory actions. The Court held that consumers were precluded from suing under the statute where it expressly granted this right to another identified group with "interests similar to those of consumers . . . [so that the group] can therefore be expected to challenge unlawful agency action and to ensure that the statute's objectives will not be frustrated." *Id.* at 352. While the § 512 safe harbors are a matter of private, rather than administrative, law, the notion that a legal regime may depend on the coincidence of interests of multiple groups in designating one of them to act on behalf of all has obvious applicability in this context.

phrase "formed after an inquiry reasonable under the circumstances" from Rule 11 of the Federal Rules of Civil Procedure.[296] This change would affect the procedural requirements laid out in sections 512(c)(3) (basis for takedown request by copyright holder), 512(g)(1) (basis for actual takedown by OSP), and 512(g)(3) (basis for counter notification by subscriber). Transforming the subjective "good faith" requirement into a more objective form might improve the extra-litigation notice, takedown, and put-back processes in much the same way that the drafters of the 1983 amendments to Rule 11 expected their change to that formulation would "help to streamline the litigation process by lessening frivolous claims or defenses."[297] The proposed change would do this by providing incentives to copyright holders, OSPs, and subscribers alike to refrain from taking hasty or ill-considered actions under the DMCA.

The obvious difficulty with this approach is that, despite the superficial equity of strengthening the good faith requirement for all three parties, the practical effect would clearly be felt most keenly by copyright holders and OSPs, who are substantially more likely to be "repeat players" in the notice and takedown arena. Furthermore, the "reasonable investigation" formulation was certainly known to Congress when the "good faith" standard was selected; indeed, the legislative history suggests that Congress believed that the language chosen struck the proper balance between copyright holders' need "for rapid response to potential infringement" and end users' "legitimate interests in not having material removed without recourse."[298] Perhaps if the proposal for change called attention to the "under the circumstances" part of the requirement, any lingering fears that the more rigorous standard would unfairly hamper policing efforts by copyright holders could be assuaged. As the Federal Rules Advisory Committee pointed out in the context of Rule 11, "what constitutes a reasonable inquiry may depend on such factors as how much time for investigation was available . . . ."[299] This context-sensitive application of the standard could perhaps distinguish cases in which a copyright holder

296. FED. R. CIV. P. 11(b) (stating that allegations, claims or defenses contained in pleadings, motions or other representations to court must be certified to have been "formed after an inquiry reasonable under the circumstances").

297. FED. R. CIV. P. 11 advisory committee's note.

298. S. REP. NO. 105-190, at 21 (1998); *see also* Rossi v. Motion Picture Ass'n of Am., 391 F.3d 1000, 1003–05 (9th Cir. 2004) (rejecting website operator's contention that "good faith" condition implicitly required reasonable investigation, based in part on Congress' apparent awareness of difference between subjective and objective standards of reasonableness).

299. FED. R. CIV. P. 11 advisory committee's note.

is harassing a website operator without reasonable grounds from a case like *Rossi v. Motion Picture Ass'n of America*, in which all overt indications pointed to the site being infringing, and the only way the Motion Picture Association of America (MPAA) could have discovered it was not infringing was to attempt to actually use the site to infringe.[300]

Even if the good faith requirements are strengthened along these lines, so long as unquestioning compliance with properly formatted takedown notices remains a sure ticket to immunity from liability to copyright holder and end user alike, takedown without investigation will remain far and away the most economically rational option for a profit-maximizing OSP. It will remain "easier to just cancel them"[301] than to investigate the merits of complaints against individual customers. For this reason, the absolute immunity from monetary, injunctive or equitable relief currently provided by the safe harbors for commercial OSPs should be eliminated and replaced with a rebuttable presumption of innocence, to which an OSP would be entitled so long as it had no actual or constructive knowledge of the infringing activity and acted toward complainant and subscriber alike in keeping with a "good faith belief after reasonable investigation" standard. If an OSP can make a prima facie demonstration that it meets these conditions, the burden would shift to the copyright holder or subscriber to rebut this presumption with proof of knowledge, inducement, willful blindness, objectively inadequate investigation, or other evidence tending to establish the OSP's volitional participation in the harm to the copyright owner or subscriber.

Under this scheme, the notification procedures currently laid out in section 512 would no longer be hard and fast prerequisites, but an OSP's failure to cooperate in these processes could be used to rebut the presumption. Proof of notice of infringement from a copyright holder, for example, could undermine the OSP's prima facie claim of lack of knowledge, with the strength of this rebuttal tied to the clarity and accuracy of the notice provided. Similarly, failure to notify a subscriber in a timely fashion that a takedown notice had been received, or to provide adequate time for filing of a counter notification, would also undermine the prima facie case. In the absence of such proof, however, the OSP would remain immune from liability. Furthermore,

300. *See Rossi*, 391 F.3d at 1003 ("Rossi contends that if MPAA had reasonably investigated the site *by attempting to download movies*, it would have been apparent that no movies could actually be downloaded from his website or related links.") (emphasis added).

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

it might be desirable to reward OSPs who take proactive steps to facilitate the prevention of copyright infringement. For example, implementation, on an individual or industry-wide basis, of something like eBay's Verified Rights Owner (VeRO) program, in which the OSP cooperates in advance and on an ongoing basis with participating copyright holders to combat infringement on their site through subscriber education and joint policing efforts,[302] should substantially strengthen the presumption that the OSP is neither a direct nor a secondary infringer.

Obviously, the purpose of these changes would be to lessen the attractiveness of a strategy of blind compliance with takedown notices. While even the presumption would be sufficiently appealing to induce many OSPs to continue treating copyright holders quite deferentially, it may be hoped that a more balanced set of duties to both copyright holders and subscribers would enable at least some OSPs to rationally conclude that it was in their interest to conduct some sort of preliminary investigation and to resist takedown or put back notices grounded in obviously frivolous claims.

The objective of motivating copyright holders to act responsibly in seeking relief from OSPs would obviously be furthered by the proposed strengthening of the good faith requirement. This tendency might be reinforced by adopting some measures that have been used overseas, although these may prove too severe to be acceptable in the United States. The first of these would be imposing a requirement that any copyright holder seeking takedown of allegedly infringing material (or denial of access to an alleged infringer) must indemnify the OSP for any liability it might incur to its subscriber if it complies. This requirement was apparently adopted by at least one European OSP, and was defended by one supporter as a way to provide greater protection to OSP's than section 512, in addition to "discouraging bogus or ill-researched claims of infringement (also of benefit to legitimate rights holders who might otherwise be subject to deliberate sabotage attempts by competitors)."[303] As a practical matter, however, it is difficult to imagine how anything resembling such an indemnity requirement could survive the American political process, given the access and power of copyright industry lobbyists. Perhaps the most that could be achieved along these lines would be to permit OSPs to ask for indemnification in exchange for surrender of the presumption of immunity, though even that variant seems farfetched.

302. *See* eBay, eBay's Verified Rights Owner (VeRO) Program, http://pages.ebay.com/help/confidence/vero-rights-owner.html (last visited Nov. 4, 2005).

303. Bortloff & Henderson, *supra* note 196, at 23.

Another European arrangement that might induce more restraint among American copyright holders is the agreement reached between Finland's SONERA/Tele ISP and the Finnish collecting society (TEOSTO), whereby the ISP agreed to conduct subscriber education programs, and to immediately remove materials TEOSTO claimed infringed its members' copyrights as soon as it received notice from the society. TEOSTO collaborates in the subscriber education efforts and, more importantly, commits to investigating the merits of its members' claims before submitting them to the ISP.[304] The two parties mutually indemnify one another for losses incurred by either due to failure of the other to comply with the agreement. A similar arrangement was reached between the Finnish IFPI Group, and Finnish OSPs.[305] This solution has some initial appeal, given the avowed effort to bring coordination and consistency to the assessment of claims of infringement *before* materials are removed. It also demonstrates another apparently workable indemnification approach. Nevertheless, these arrangements were reached as part of a much more comprehensive effort to achieve acceptable compromises on OSP liability legislation (which the copyright holders agreed not to pursue) and Digital Rights Management systems. The U.S. copyright industry may see little reason to tinker with the current scheme, which already addresses these issues largely to their satisfaction. Furthermore, the IFPI arrangement requires the OSP to remove material within twelve hours of receipt of notification,[306] which may explain copyright holders' willingness to participate in the scheme in the first place, but could easily impose a crushing financial burden on smaller OSPs.

Whatever changes are implemented, they would be enhanced by parallel adoption of a proposal by Professors Mark Lemley and Anthony Reese calling for a "streamlined dispute resolution system" for use in cases of large-scale direct infringement.[307] Their proposal would allow "relatively straightforward claims of copyright infringement" to be handled under a fast-track procedure before an administrative law judge operating in the Copyright Office.[308] The proceeding would operate under rules strictly limiting the claims or

304. *Id.* at 7.
305. *Id.* at 7–8.
306. *Id.* at 8.
307. Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1410 (2004).
308. *Id.* at 1413.

defenses that could be advanced in that setting,[309] so that resolution of disputes would presumably be swift and inexpensive. This might help to offset any increase in cost or adverse impact of delay incurred by copyright holders or OSPs as a result of other proposed changes—in particular, the more rigorous investigation requirement, thereby making the overall reform more palatable to the copyright holders. While Lemley and Reese suggest that their fast-track procedure would be aimed primarily at inducing copyright holders to sue direct infringers, rather than "facilitators,"[310] there appears to be no reason to presume that the system would not be applicable to disputes involving OSPs as well.

B. Encouraging Responsible System Design: Secondary Liability and Fair Use

The elimination of the absolute OSP immunity available under the safe harbors might mean that some copyright owners would be tempted to seek relief from the deeper pockets of OSPs, and this could create precisely the sort of impediment to technological progress that the *Netcom* court warned about.[311] On the other hand, it may be that a credible threat of legal liability would provide OSPs with an incentive to develop technologies consistent with the rights of copyright holders. The doctrine of fair use has long provided copyright defendants with an opportunity to present courts with particular facts surrounding their alleged infringement which may establish a defense against liability for primary infringement in a given case. Perhaps such a doctrine, tailored more specifically to act as a defense to *secondary* infringement liability, could make the option of excessive litigation against wealthy OSPs less appealing to copyright holders, while leaving open the possibility of redress for truly objectionable conduct on the part of network operators or designers.

Section 107 of the Copyright Act directs that when assessing infringement liability, a court applying the doctrine of fair use "shall" consider "the purpose and character of the use," the "nature" of the work at issue, the "amount and substantiality" of the copying, and its effect on the market value of the work.[312] The Supreme Court has held that the Act was intended by Congress to provide only "general

309. Parties would, however, be able to preserve such claims and defenses, to be pursued in a declaratory judgment or appeal of the result reached by the ALJ should they so desire. *Id.* at 1415–17.
310. *Id.* at 1410–11.
311. *See supra* 73–74 and accompanying text.
312. 17 U.S.C. § 107 (2000).

guidance" to courts, which must engage in a "case-by-case analysis."[313] The Court has also noted that the list of inquiries included in the text of section 107 was meant to be "'illustrative and not limitative.'"[314] Thus, some minor tweaking of the conventional fair use inquiry need not represent a radical break from established principles.

The "purpose" prong, for example, could be adapted to consider the rationale behind an act or acts of *secondary* infringement. A threshold question, of course, should be whether there is any plausible justification for the unauthorized copying. Was the OSP engaged in an activity aimed primarily at conferring an important benefit in an area, such as network performance or security, that is clearly independent of the material copied? Activities that enhance the performance of the network for all classes of users or traffic on an equitable and rational basis should generally be considered fair uses.

The offer of a justification should not, however, end the purpose inquiry. A court should consider, for example, exactly how "automatic" the processes were that led to the infringing copying. If they resulted from design choices that were made voluntarily by the OSP itself, and that could have been made differently—that is, if other design choices might have led to a lower incidence of infringement—then the OSP may be less deserving of a robust fair use defense. Similarly, courts should consider whether the allegedly offending activity or technology was applied blindly to any and all content or traffic, or was instead confined to a limited subset. Still other questions may be relevant to the inquiry. Does the OSP receive a greater return for more extensive or more serious infringement? Did the OSP have prior knowledge of the infringement? If so, these factors would suggest some measure of complicity in the primary infringer's conduct which should weigh against the strength of the OSP's defense of fair use.

The "nature" prong of a fair use inquiry recognizes that "some works are closer to the core of intended copyright protection than others, with the consequence that fair use is more difficult to establish when the former works are copied."[315] An adapted "nature" prong would incorporate consideration not only of the genre of the protected work, but also the medium in which the work is fixed. Courts generally hold that the more creative or artistic a work, the less susceptible it is to legitimate unauthorized adaptation through fair use.[316] This "genre" focus should be supplemented with consideration of whether

313. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994).
314. *Id.* (quoting 17 U.S.C. § 101).
315. *Id.* at 586.
316. *See id.* (collecting contrasting examples).

the protected work's medium makes fair use adaptation especially problematic. For example, an OSP hosting unauthorized digital photographs of protected sculptures should have a stronger fair use defense than one hosting unauthorized copies of protected digital videos, since digital representations of tangible three-dimensional objects will probably be less effective substitutes for the originals, and therefore less damaging, than would be the case if both original and duplicate were in digital form. While this concern can be addressed at least in part by the "market effect" prong of the analysis, a more explicit recognition under the nature prong would make it less likely to be overlooked in cases involving either works reaching a limited audience or expression that may be fixed but has not been commercially exploited by the copyright holder.

The core of the "amount" prong would remain essentially unchanged: the essential inquiry would be whether the amount or proportion of the source work from which the unauthorized copies have been derived "are reasonable in relation to the purpose of the copying."[317] Nevertheless, it might also be worthwhile to consider the scope and scale of the alleged secondary infringement by examining the number of copies or downloads. For instance, a site that caches a single copy of a protected work for inbound or outbound use may have a stronger claim to the fair use defense than a global CDN that pre-positions tens of thousands of copies in geographically dispersed locations. Similarly, the specific copying approach used by the OSP may be relevant. An OSP caching small, frequently-used portions of a work in ways that make it difficult to assemble a complete duplicate of the whole may have a stronger claim to fair use than one storing entire copies. There is a risk, however, that such factors might be double-counted both here and under the "purpose" prong.

Finally, the "market effect" prong could be modified to require an explicit balancing of the financial impact on the content owner against the cost to the OSP of policing or otherwise avoiding the infringement in question. Thus, just because an OSP *could* acquire and/or implement particular technologies or monitoring practices that might reduce infringing conduct would not necessarily imply that it *must*. Where an OSP could demonstrate that a preventive measure would impose significant costs not only on primary infringers, but also on its entire user community, courts should weigh that harm against the harmful impact claimed to the copyright owner's actual and potential markets. Where the only remedial or preventive alternatives avail-

317. *Id.*

able to the OSP would be unreasonably expensive or burdensome and the risk of harm to a copyright owner's market opportunities would be slight, the case for fair use would be stronger.

OSPs could theoretically advance something like this fair use argument today in lieu of seeking the protection of the section 512 safe harbors. Nevertheless, it is unlikely that any would do so in practice, since the mechanical requirements of section 512 are cheaper and offer greater certainty of outcome. As long as the perceived value to the OSP of an individual end user or website operator remains lower than "the price of a phone call to a lawyer to figure out what to do,"[318] we can expect OSPs to remain committed to user policies that adhere closely to the statutory notice and takedown model. Though more expensive for the OSPs and copyright holders, fair use would probably enable a more equitable balancing of the interests of these groups with those of the consumers and producers of expressive works, by giving more OSPs a reason "to figure out what to do"—whether that means resisting frivolous or abusive takedown requests or designing more effective copyright protections into their networks in the first place.

CONCLUSION

One of the main sources of the power of the Internet as a communicative tool is the ease with which it permits the digital exchange of information. The Internet makes it possible for an individual to create and publish digital content at virtually no cost. As a result, individuals and small organizations have nearly the same capability of making their messages heard as larger, wealthier corporations. However, the DMCA has made it even easier and less expensive to remove content than to post it in the first place. This is intolerable, particularly where many of the primary beneficiaries of the law's provisions are increasingly drifting in the direction of active involvement with infringement. There are, however, ways of rectifying these problems in a manner consistent with the original purposes of the DMCA. Copyright law recognizes a continuum of different forms of direct infringement, and the law does not treat them all alike; similarly, there is a continuum of potentially infringing secondary activities, and we would be well-served to adopt copyright laws that are capable of distinguishing between them.

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