Harvard Journal of Law & Technology
Volume 19, Number 2 Spring 2006

A HISTORY OF ONLINE GATEKEEPING

*Jonathan Zittrain**

TABLE OF CONTENTS

I. INTRODUCTION

The brief but intense history of American judicial and legislative confrontation with problems caused by the online world has demonstrated a certain wisdom: a reluctance to intervene in ways that dramatically alter online architectures; a solicitude for the collateral damage that interventions might wreak upon innocent activity; and, in the balance, a refusal to allow unambiguously damaging activities to remain unchecked if there is a way to curtail them.

The ability to regulate lightly while still curtailing the worst online harms that might arise has sprung from the presence of gatekeepers. These are intermediaries of various kinds — generally those who carry, host, or index others' content — whose natural business

* Professor of Internet Governance and Regulation, Oxford University; Jack N. & Lillian R. Berkman Visiting Professor for Entrepreneurial Legal Studies, Harvard Law School. I thank William Fisher, Wendy Seltzer, and Rebecca Tushnet for helpful comments on earlier drafts, and Erin Ashwell, Bryan Choi, Jacob Mermelstein, Christina Olson, K. Joon Oh, and Elizabeth Stark for outstanding research assistance.

models and corresponding technology architectures have permitted regulators to conscript them to eliminate access to objectionable material or to identify wrongdoers in many instances. The bulk of this Article puts together the pieces of that history most relevant to an understanding of the law's historical forbearance, describing a trajectory of gatekeeping beginning with defamation and continuing to copyright infringement, including shifts in technology toward peer-to-peer networks, that has so far failed to provoke a significant regulatory intrusion. I argue that the U.S. Supreme Court's *Grokster* decision[1] upholds this tradition of light-touch regulation that has allowed the Internet to thrive. The decision thus is not a landmark so much as a milestone, ratifying a continuing détente between those who build on the Internet and those in a position to regulate the builders.

Grokster may have achieved such a fit with its ancestors by avoiding a set of now-pressing issues about gatekeepers. This avoidance is revealed by looking at *Grokster's* outcome: a loss for Grokster Ltd. that has no practical impact on the distribution and use of the sort of PC software that got Grokster Ltd., in trouble. The most recent peer-to-peer technologies eliminate a layer of intermediation from the networks they create; there are often no longer central websites or services that can be blamed, and then shut down or modified, to dampen the objectionable activities that they enable. Even decentralized Internet service providers may prove unable to intercede much as new overlay networks cloak users' network identities in addition to their personal ones.

The loss of these natural points of control will cause those with challenged interests to foreground a new and less palatable set of intermediaries: software authors. These authors may be asked to write their software in such a way that it can be recalled or modified after it has been obtained by a user and then put to an undesirable purpose. They may even be asked to program their software to disable the installed software of others. Control over software — and the ability of PC users to run it — rather than control over the network, will be a future battleground for Internet regulation, a battleground primed by an independently-motivated movement by consumers away from open, generative PCs and toward more highly regulable endpoint platforms.

II. TWO KINDS OF GATEKEEPERS

Regulators faced with difficulties in getting behavior to accord with law might elect instead to change the law to accord with the be-

1. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. (*Grokster III*), 125 S. Ct. 2764 (2005).

havior, especially for "parking ticket"-style wrongs that are closer to malum prohibitum than malum in se.[2] One might put the flagstones on a grassy quadrangle precisely where people tend to walk, rather than trying to convince people to use paths that do not track where they would like to go, to mitigate the damage to the turf. But when the wrongs are more serious (or at least the lawmakers more determined) pointing out enforcement difficulties simply asks regulators to be more insistent and creative in influencing behavior.

Efforts such as the No Electronic Theft (NET) Act[3] lie in the camp for greater online regulation in the face of new challenges. Before the advent of modems and networks, major physical-world infringers typically needed a business model because mass-scale copyright infringements required substantial investment in copying and distribution infrastructure. With the advent of the Net, large-scale infringements became possible through the sum of minor favors among friends and strangers.[4] The NET Act newly permitted the criminal prosecution of individuals who willfully made software or other copyrighted works available over networks without permission, regardless of whether they sought to profit from the infringement.[5] However, without a correspondingly heightened investment in, or at least prioritization of,[6] law enforcement and prosecutorial funding, insistence alone was not enough to return the level of infringing activity to what it had been prior to the advent of the networks themselves.

To the extent that the Internet empowered individuals — enabling them to produce substantial harm at a distance without being readily identified, much less punished — direct forms of behavioral regulation like the NET Act became less effective and therefore less appealing. Increased barriers to direct enforcement against individuals have been addressed primarily in two alternative ways: first, through efforts to enlist intermediaries to assist in regulating individuals ("traditional gatekeepers"); and second, through efforts to change the technology itself to facilitate direct identification and regulation of individuals

2. Malum prohibitum offenses are those that are wrong because the law prohibits the behavior, while malum in se wrongs are acts that are inherently immoral or evil. BLACK'S LAW DICTIONARY 978–79 (8th ed. 2004).

3. Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amended in scattered sections of 17 U.S.C., 18 U.S.C., and 28 U.S.C.).

4. *See* Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1206 (2000) ("The growth of the Net raised the level of copying exponentially, since it made copying so much easier, the possibility of detection, prosecution, and punishment so much more remote, and successive generations of copies as perfectly copyable as originals.").

5. *Id. See generally* Stephanie Brown, Legislative Update, *The No Electronic Theft Act: Stop Internet Piracy!*, 9 DEPAUL-LCA J. ART & ENT. L. & POL'Y 147 (1998) (explaining the history of the NET Act and detailing its provisions).

6. *See* Piracy Deterrence and Education Act of 2004, H.R. 4077, 108th Cong. (as passed by House, Sept. 28, 2004) (calling for enhanced criminal enforcement of copyright laws).

("technological gatekeepers"). Each is grounded in the recognition that direct regulation of wrongdoing parties is not easy.

The first effort — developing strategies to use human or institutional intermediaries — traces its basis as far back as the emergence of tort doctrines of vicarious liability.[7] Reinier Kraakman catalogued the limits of direct "primary enforcement" in an influential 1986 article,[8] advancing a general framework for when to invoke gatekeeper liability. Such liability asks intermediaries who provide some form of support to wrongdoing to withhold it, and penalizes them if they do not.[9] Kraakman advanced four criteria for evaluating the propriety of compelled gatekeeping: "(1) serious misconduct that practicable penalties cannot deter; (2) missing or inadequate private gatekeeping incentives; (3) gatekeepers who can and will prevent misconduct reliably, regardless of the preferences and market alternatives of wrongdoers; and (4) gatekeepers whom legal rules can induce to detect misconduct at reasonable cost."[10] He also factored in the costs of gatekeeping to innocent third parties — the ways in which an undertaking of gatekeeping duties could create friction in relationships that gatekeepers have with others.[11] While Kraakman's own work was directed at financial and other white-collar wrongdoing that might be curtailed through the gatekeeping functions of lawyers and accountants, many cyberlaw disputes are amenable to exactly this sort of framework. The project of creative regulators has often been to see if gatekeeping can successfully be applied to achieve a regulatory end on the Internet.

A second effort to indirectly regulate individual behavior — changing the technology itself — crystallized as a theory roughly ten years after Kraakman's article, as legal systems experienced the first wave of problems arising from the use of the Net. Lawrence Lessig specifically addressed regulability issues in cyberspace, emphasizing that code too could be law.[12] Not only did a technology's very functionality define the range of behaviors in which people could engage (including the range of regulatory options reasonably available to a

7. Vicarious liability provides incentives for the one held liable for the actions of another to serve as a de facto "cop-on-the-beat," a metaphor that can be traced to Jeremy Bentham's conception of respondeat superior. Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 53 & n.1 (1986).

8. *Id.* at 54–55.

9. *Id.* at 53–54.

10. *Id.* at 61.

11. *Id.* at 75–78.

12. *See* Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 761–62 (1999) [hereinafter Lessig, *Limits in Open Code*]. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) [hereinafter LESSIG, CODE AND OTHER LAWS]. While Lessig made famous the idea that "code is law," credit for the original conception goes to Joel Reidenberg. *See* Lessig, *Limits in Open Code*, *supra*, at 761–62.

sovereign) but technologies built by people could also be changed by people. Thus, to speak of "natural unregulability" was to mistake an eminently revisable instrumentality for a force of nature.[13] If regulators could induce certain alterations in the nature of Internet technologies in a way that others could not undo or widely circumvent, then many of the regulatory puzzles occasioned by the Internet would evaporate. Lessig went on to worry greatly about such changes, fearing that blunderbuss technology regulation by overeager regulators would unduly disrupt legitimate uses of such regulation and intrude upon the creative freedom of technology makers.[14]

These themes — looking to control individual behavior by altering the incentives of intermediaries and by changing the operation of technology — can be found in almost every doctrinal area implicated by cyberlaw. What is not often understood is how *limited* the use of these tools has been so far despite their potential. To understand why is to understand whether such forbearance will continue, and if not, what to expect next and how to normatively assess and deal with it.

III. EARLY APPLICATIONS OF GATEKEEPING ONLINE: SUPPLEMENTS TO EXISTING PRIVATE MONITORING AND ENFORCEMENT REGIMES

Evolving policies toward cyber-defamation and children's access to online pornography in the United States provide useful, intertwined examples of regulatory forbearance early in cyberlaw's intellectual history, showing interventions only in places where regulators saw intermediaries already filtering.

As soon as significant numbers of consumers were online — at first through proprietary information services — they enjoyed a significant amount of power and freedom to post information to the public at large, or at least to other subscribers of their respective proprietary networks. These technologies were highly generative[15] regarding the transmission, use, and reuse of content, if not code: people could interact with each other in novel ways, inventing new forms of conversation at a distance and among groups through predeveloped applications such as text-based chat, public message boards, and electronic file and document libraries. This generativity also permitted undesirable uses, such as the dissemination of defamation and the transmission of pornography to children. Such behavior

13. LESSIG, CODE AND OTHER LAWS, *supra* note 12, at 24–25 (describing the fallacy of "is-ism").

14. *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 236–39 (2001).

15. *See generally* Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006).

initiated by hard-to-find and likely judgment-proof individuals quickly gave rise to questions of third-party liability.

Two common law cases stand out: 1991's *Cubby, Inc. v. CompuServe, Inc.*[16] and 1995's *Stratton Oakmont, Inc. v. Prodigy Services Co.*[17] In each case, a proprietary "online service provider" ("OSP")[18] facilitated the posting of actionable speech by its subscribers. In the *CompuServe* incident, an allegedly defamatory newsletter was uploaded to a CompuServe data library;[19] in *Prodigy*, a message was placed on a "Money Talk" bulletin board that was said to defame an investment bank in the midst of underwriting a stock offering.[20] The threshold decisions on liability turned on the application of a preexisting distinction in common law defamation doctrine between booksellers/distributors and newspapers/publishers.[21] Although both groups can be found liable for the third party works they make available to the public, the threshold for distributor liability is much higher.[22] This is grounded in the idea that distributors are passive conduits. They do not undertake to edit their offerings in any fine-grained manner and thus are not asked to screen such materials for defamatory statements.[23] Publishers, on the other hand, by undertaking to edit, are given more responsibility for the ultimate results.[24]

The facts in *CompuServe* were found to lend themselves more to a distributor configuration, because the court credited — wrongly, as a factual matter — that no pre-screening of uploaded materials was possible within CompuServe's forums, making the service a passive conduit.[25] Prodigy, on the other hand, had styled itself as a family-oriented service and had undertaken to screen out objectionable material, even after it had already been posted.[26] The *Prodigy* court, then, while indicating complete agreement with the reasoning in the *CompuServe* case, came to a different outcome on its set of facts: Prodigy acted as an editor, and thus undertook more responsibility for the contents of its electronic bulletin boards than CompuServe did for the contents of its electronic file libraries.[27] The *Prodigy* court ac-

16. 776 F. Supp. 135 (S.D.N.Y. 1991).

17. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Telecommunications Act of 1996 (Communications Decency Act), Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133–43 (codified at 47 U.S.C. § 230 (2000)).

18. OSPs store information for consumers for mass distribution to others. *See infra* text accompanying notes 67–68.

19. *CompuServe*, 776 F. Supp. at 138.

20. *Prodigy*, 1995 WL 323710, at *1.

21. *See CompuServe*, 776 F. Supp. at 139–41; *Prodigy*, 1995 WL 323710, at *1–5.

22. *See CompuServe*, 776 F. Supp. at 139–41; *Prodigy*, 1995 WL 323710, at *3.

23. *See CompuServe*, 776 F. Supp. at 139–41; *Prodigy*, 1995 WL 323710, at *3.

24. *See CompuServe*, 776 F. Supp. at 139; *Prodigy*, 1995 WL 323710, at *3.

25. *See CompuServe*, 776 F. Supp. at 140–41.

26. *Prodigy*, 1995 WL 323710, at *2–3.

27. *Id.* at *5.

knowledged that for future liability avoidance, Prodigy might want to structure its operations to become more passive.[28] Such a decision, it reasoned, would rest on an economic assessment of whether public demand for Prodigy's publisher-like filtering services would result in enough increased revenue (compared with no filtering and thus "distributor" status) to offset insurance costs for possible liabilities should those filtering services fail to screen out actionable material.[29]

At first glance, this distinction between publishers and distributors readily accords with Kraakman's gatekeeping theory, since those who are already closely editing might be able to serve gatekeeping roles at little additional cost. Kraakman further distinguished different roles a gatekeeper could undertake, including whistleblower, bouncer, and chaperone;[30] publishers are held to the most demanding of these three roles. Simplifying somewhat, whistleblowers alert authorities to possible malfeasance when they detect it;[31] bouncers refuse to deal with parties that are thought to be "bad" along simple dimensions;[32] and chaperones, by dint of deep, ongoing relationships with their clients, perform more complex and nuanced monitoring of, and influence over, their clients' behavior.[33] A gatekeeping regime for defamation, whether that of publisher or distributor, seems to anticipate a chaperone relationship. For professional services such as law and accounting, the corresponding gatekeepers are in ongoing relationships with their clients and come to know their clients' businesses, and thus are in some position to knowledgably chaperone them. Further, it is the business of lawyers and accountants to know the applicable rules and limits upon first-party behavior. Bulletin board operators and other online intermediaries, to fulfill the gatekeeping role, would likewise have to familiarize themselves with the multifaceted content traversing their systems and be in some position to assess its truth — no easy task.

In the context of OSPs, then, publisher liability would make such gatekeeping obligations strict, placing the gatekeeper in the shoes of the direct defendant speaker and imposing potentially large costs on the gatekeeper to detect misconduct.[34] On the other hand, distributor liability for defamation is also a gatekeeping regime, but it is likely a much weaker one because it appears to require a showing of fault be-

28. *Id.*
29. *Id.*
30. Kraakman, *supra* note 7, at 58–60, 62–66.
31. *Id.* at 58–60.
32. *Id.* at 62–66.
33. *Id.*
34. *See* Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002) (arguing that applying strict liability to online gatekeepers would produce overdeterrence); *see also* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 404–06 (2003).

fore liability can attach. This standard of negligence is typically couched as requiring the gatekeeper to know or have reason to know that the carried material is defamatory.[35] That level of liability was generous enough to allow CompuServe to win its defense on summary judgment, even if the material it permitted to appear was in fact defamatory, since the court believed CompuServe had no reason to know of the defamatory nature of the material.[36]

As a policy matter, although Kraakman's theory offers some reason why a publisher should be treated less generously than a distributor, screening for defamatory content by OSPs may not call for a gatekeeping regime of any kind — even if the intermediary were already undertaking to edit material, as was the case in *Prodigy* and as, indeed, was also true as a factual matter in *CompuServe* despite the court's belief otherwise. Even under weak distributor liability, for example, OSPs might be asked to take down actionable material after a plaintiff had become aware of it and explicitly flagged its possible defamatory content to the service provider. Such a framework might cast the gatekeeping role closer to that of bouncer than of chaperone, since the OSP would simply be acting at the behest of the injured party in throwing out messages that elicited complaint, or in cutting off subscriptions of posters who continued to post such messages.[37]

While acting as a bouncer is not as onerous to the OSP as acting as a chaperone under these circumstances, such a shift masks the fact that determining wrongdoing for defamation remains difficult, and that substituting the purportedly injured party for the bulletin board operator as the chaperone may be an undesirable solution. Those merely offended, but not truly defamed, would be tempted to put OSPs on false notice that the offending material was defamatory and potentially lead the bouncer to overenthusiastically perform its job.[38]

By the time of the *Prodigy* decision, proprietary OSPs, along with an emerging set of commercial Internet Service Providers ("ISPs"), had acquired some political muscle. They wanted to be able to edit their dynamic offerings — for example, being able to selectively delete undesirable message board postings — without undertaking publisher-level responsibilities for defamation for postings they

35. *See CompuServe*, 776 F. Supp. 135, 139-41 (S.D.N.Y. 1991); *Prodigy*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

36. *See CompuServe*, 776 F. Supp. at 139–41.

37. In *Zeran v. America Online, Inc.*, 958 F. Supp. 1124, 1127–28 (E.D. Va. 1997), the defamatory poster did just that, continuing to post new messages even as America Online ("AOL"), under pressure from the victim, deleted the old ones. It was never clear in that case why AOL did not terminate the victimizing subscriber entirely; it may simply have elected not to, or its habit of granting free trial memberships without requiring any form of identity authentication (something itself revisable, of course) may have made it possible for the subscriber to create a new account every time an old one was barred.

38. *See* Jonathan Zittrain, *Policy Commentary: The Rise and Fall of Sysopdom*, 10 HARV. J.L. & TECH. 495, 506–09 (1997).

overlooked.[39] At the time of the *Prodigy* holding, which apparently denied them such an arrangement (at least under New York law), the U.S. Congress was seized with a seemingly distinct cyberlaw issue: the ready availability of online pornography to children — much greater than that of its physical-world counterpart.[40] Limits on the availability of *offline* indecent materials to children had already been effected primarily through gatekeeper liability; many states had established that such materials could be sold by storekeepers only if they first obtained identification verifying that a young-looking purchaser was over a certain age.[41] In contrast, the Communications Decency Act ("CDA") of 1996[42] fit into the "more insistent direct regulation" camp rather than the third-party gatekeeping camp. It did not require online intermediaries to perform such a gatekeeping function. Instead, the Act simply criminalized "initiat[ing]" the online provision of indecent materials to minors[43] unless the initiator had undertaken a good faith effort to determine the age of the person on the other end of the network.[44]

As a policy matter, a choice to go for direct regulation in this instance could reflect a conclusion that direct penalties ought to be given a chance before a move to gatekeeper regulation is considered. Asking quasi- or entirely passive conduits like OSPs and ISPs to screen for indecent material would create massive friction for innocent third parties,[45] since it could induce OSPs hosting online chat rooms and message boards that thrive on third-party input to shut down entirely, to raise drastically the cost for their services, or to

---

39. *See id.* at 510–13 (noting that Congress apparently recognized a need "to provide some degree of immunity from state law for sysops attacked for poorly managing the dynamic exchange of messages written by others").

40. *See* Communications Decency Act of 1995, S. 314, 104th Cong. (1995); Protection of Children From Computer Pornography Act of 1995, H.R. 2104, 104th Cong. (1995); Protection of Children from Computer Pornography Act of 1995, S. 892, 104th Cong. (1995); Online Parental Control Act of 1996, H.R. 3089, 104th Cong. (1996); 141 CONG. REC. S8268 (daily ed. June 13, 1995) (statement of Sen. Robb); 141 CONG. REC. S9017 (daily ed. June 26, 1995) (statement of Sen. Grassley).

41. *See, e.g.*, MONT. CODE. ANN. § 45-8-206 (2005). It is illegal in Montana for a commercial establishment to disseminate obscene material to minors, though there is an exception for shopkeepers that:

> [H]ad reasonable cause to believe the minor was 18 years of age. 'Reasonable cause' includes but is not limited to being shown a draft card, driver's license, marriage license, birth certificate, educational identification card, governmental identification card, or other official or apparently official card or document purporting to establish that the person is 18 years of age.

Id. See also Ginsberg v. New York, 390 U.S. 629 (1968) (upholding such restrictions).

42. Telecommunications Act of 1996 (Communications Decency Act), Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133–43 (codified at 47 U.S.C. § 230 (2000)), *available at* http://www.epic.org/free_speech/CDA/cda.html.

43. 47 U.S.C. § 223(a) (2000).

44. *Id.* § 223(e)(5)(A).

45. *See supra* note 11.

overblock content in an attempt to avoid any possible suggestion of liability.[46] As a political matter, OSPs and ISPs may simply have prevailed upon Congress to leave them out of the CDA's liability regime for the transmission of materials that could be harmful to minors.

Even in the absence of regulatory mandates on ISPs or OSPs, it was understood that such entities could play a useful role in filtering undesirable content from children. Without requiring filtering by gatekeepers, the CDA expressed a desire to encourage it.[47] To do so, it *loosened* the emerging state-level gatekeeper liability regime for defamation and other common law torts. Stating that "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," the Act preempted the law of the *Prodigy* case, apparently to encourage "'Good Samaritan' blocking and screening of offensive material."[48] OSPs that aggregated content from subscribers were now free to edit their subscribers' work more or less as they pleased, without encountering the concomitant obligation to serve as gatekeepers for the individuals who might use the OSPs' services to transmit actionable speech.[49]

The CDA ended the percolation of common law cases regarding the proper level of gatekeeping for online defamation because the CDA's immunities were thought in early interpretive cases to be broad enough to preclude both publisher and distributor liability.[50] CompuServe and other online intermediaries were no longer under any legal pressure to serve as gatekeepers for defamation in even the weak, "bouncer" sense.

Just as redress for defamation ultimately did not implicate traditional gatekeeper regimes, neither did it implicate technological gatekeeping. Even if one credits the *CompuServe* court's finding that

---

46. Kraakman calls these "tertiary" costs. *See* Kraakman, *supra* note 7, at 75–77.

47. 47 U.S.C. § 230(b) (2000). The CDA began with a preamble containing paeans to the social benefits afforded by the vibrant, rapidly-growing competitive free market in proprietary and non-proprietary information networks — networks "unfettered by Federal or State regulation." *Id.*

48. *Id.* § 230(c)(1).

49. This provision survived the nullification of much of the CDA on First Amendment grounds by the Supreme Court in *Reno v. ACLU*, 521 U.S. 844 (1997).

50. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1027 n.10 (9th Cir. 2003) (noting that "so far, every court to reach the [CDA] issue has decided that Congress intended to immunize both distributors and publishers"). *But see* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (musing in dicta that the CDA should immunize an ISP only "as long as the information came from someone else," and not when the ISP created the objectionable information itself); Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 153–54 (Cal. Ct. App. 2004), *cert. granted*, 87 P.3d 797 (Cal. 2004) (noting that *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), "immunized providers and users of interactive computer services from liability not only as *primary publishers* but also as *distributors*," but "declin[ing] to accept *Zeran's* construction of the [CDA]" (emphases in original)); Additional Development, Barrett v. Rosenthal, 20 BERKELEY TECH. L.J. 333 (2005).

subscribers' uploaded files were made available to other subscribers immediately upon submission, CompuServe could surely have changed its perceived regime to the one that was actually in place: such submitted files were parked in a purgatorial "preview" area where only CompuServe employees and contractors could view them in order to decide whether to make them widely available.[51] Prodigy permitted messages to be posted immediately, but that too could have been recoded: Prodigy could have made messages await moderator approval. The implication of the two decisions, mooted by the CDA's immunities, was that the gatekeeper was entitled to decide how active or passive to be, and that this decision would in turn set the rules by which the gatekeeper might be found to have certain obligations. Liability, whether stemming from a company's actions as a publisher or a distributor, focused on a gatekeeper's conduct within its own chosen technical regime, rather than alternative regimes it might be able to employ. Law followed code and code followed business model, rather than the other way around.

IV. LIMITED GATEKEEPING CONTINUES AS THE INTERNET MATURES: COPYRIGHT INFRINGEMENT, ISPS, AND OSPS

Defamation was the early 1990s' litmus test for the proper role of intermediaries in preventing individual online activities that were objectionable. Infringement of others' copyrights followed, increasingly consuming the attention of regulators and legal scholars.

As a political matter, content owners were a substantially more organized, and arguably more demonstrably harmed, group than those who had been defamed or those who believed their children had been inappropriately exposed to indecent content.[52] Harm to publishers from network-enabled copyright infringement was more visible and more capable of ready economic accounting, and the publishers' interests were predictable and ongoing in a way that was not true of many would-be defamation plaintiffs. The publishers were out to prevent a structural sea change that would enable their works to be consistently pirated, and they demanded legal redress as the deck tilted beneath them.[53]

---

51. *See* Robert B. Charles, *The New World of On-line Libel*, MANHATTAN LAWYER, Dec. 1991, at 40.

52. For a possible explanation of this phenomenon, see Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95 (1974).

53. *See* Michael D. McCoy & Needham J. Boddie, II, *Cybertheft: Will Copyright Law Prevent Digital Tyranny on the Superhighway?*, 30 WAKE FOREST L. REV. 169 (1995) (discussing proposals for copyright reform given the potential for electronic theft on the Internet, and concluding that current copyright law can be adapted to the Internet age); Robert A. Cinque, Note, *Making Cyberspace Safe for Copyright: The Protection of Elec-*

The publishers' first move was to seek gatekeeping liability as well as direct liability. The latter was reflected in the aforementioned NET Act,[54] but intermediaries seemed to hold greater promise for reducing infringement. Early skirmishes with the owners of individual electronic bulletin board systems ("BBSs") that enabled the illicit swapping of copyrighted software resulted in a mix of decisions that roughly tracked the underlying equities of *CompuServe* and *Prodigy*, notwithstanding the doctrinal stovepiping of common law defamation and federal statutory copyright law.[55] Individual bulletin board operators who seemed aware of specific pirating activity taking place through their systems were vulnerable to claims of contributory infringement;[56] enterprises that were more remote from the activity, or that supported a large volume and variety of activity of which the infringing material was only a part, were excused.[57] The publisher/distributor distinction thus roughly mapped to the judicially invented requisites for the establishment of intermediary liability through contributory or vicarious copyright infringement. While the definitions themselves have been in flux among various cases, contributory infringers are generally those who know about infringing activity and who materially assist in it, and vicarious infringers are thought akin to employers in a traditional respondeat superior situation — those who have the right and ability to control the activity, and

---

tronic Works in a Protocol to the Berne Convention, 18 FORDHAM INT'L L.J. 1258 (1995) (examining the benefits and drawbacks of strong international enforcement measures for digitally-transmitted works); John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, *available at* http://www.wired.com/wired/archive/2.03/economy.ideas.html (arguing that old laws are ill-equipped to govern information in the digital age, and predicting that new technologies, like cryptography, will be essential to the protection of intellectual property).

54. *See* Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amendments to 17 U.S.C. §§ 101, 506 and 18 U.S.C. § 2319).

55. *See generally* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 666–67 (2003).

56. *See* Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 512 (N.D. Ohio 1997) (finding liable for copyright infringement a BBS that offered incentives for subscribers to upload copyrighted images, screened the images, and moved the images to where other subscribers could download them); Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 931–32 (N.D. Cal. 1996) (contemplating contributory liability for BBS operators who provided trading areas for copyrighted video games); Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (finding liability where the defendant BBS operator charged subscribers, even though it may have been unaware of the copyright infringement).

57. *See* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distrib., 983 F. Supp. 1167, 1178–79 (N.D. Ill. 1997) (holding that the person placing unauthorized copyrighted images on a website, but not the website hosting service, might be held liable for direct copyright infringement, and finding that contributory liability against the hosting service would depend upon the level and timing of its knowledge of the infringement); Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc., 907 F. Supp. 1361, 1367–73 (N.D. Cal. 1995) (holding that the operator of a BBS was not directly liable for copyright infringement committed by a subscriber who used the BBS to place copyrighted materials onto USENET newsgroups, and expressing skepticism about the liability of upstream ISPs).

who financially benefit from it.[58] The more an intermediary acted as a mere passive conduit, the less likely it would be pressed into service as a gatekeeper through a finding of infringement, whether contributory or vicarious.

By the late 1990s, proprietary services like CompuServe and amateur BBSs were giving way to the Internet at large, and Internet Service Providers ("ISPs") — those who gave consumers and others access to the Net — came into their own as businesses with political clout. But consumer use of the Internet still followed the hub-and-spoke model of the competing proprietary services: the Internet-aware applications that developed, like web browsing[59] and File Transfer Protocol ("FTP"),[60] continued to employ the notion of consumer PCs asymmetrically accessing powerful servers, whether web or file servers. Consumer PCs were not yet powerful enough to handle very many incoming connections, if they were to try to act as servers themselves, and the absence of always-on connections for such PCs made it sensible to have information hosted elsewhere — by OSPs, who increasingly were also ISPs.

These technical and market structures were the backdrop as publishers petitioned Congress in 1997–98 for regulatory assistance in limiting piracy. The resulting Digital Millennium Copyright Act of 1998 ("DMCA")[61] contained a number of distinct provisions, with one set bearing directly on gatekeeper liability as a means of controlling copyright infringement.[62] This set of so-called "safe harbor provisions," found within 17 U.S.C. § 512, reflected a political calculus in which publishers and ISPs, whose interests did not well align, both had power.[63]

Parallel to the CDA's provisions protecting information service providers from state suit over such things as defamation,[64] § 512(a) exempted the most passive intermediaries — ISPs — from any responsibility for copyright infringement for the data they carried, so

58. *See* A&M Records, Inc. v. Napster, Inc. (*Napster II*), 239 F.3d 1004, 1019–24 (9th Cir. 2001) (discussing the elements of contributory and vicarious copyright infringement).

59. *See* BILL STEWART, *Tim Berners-Lee, Robert Cailliau and the World Wide Web*, *in* LIVING INTERNET, http://livinginternet.com/w/wi_lee.htm (last visited Apr. 29, 2006).

60. *See* J. Postel & J. Reynolds, File Transfer Protocol (FTP), RFC 959 (Oct. 1985), ftp://ftp.rfc-editor.org/in-notes/rfc959.txt; The FTP Protocol Resource Center, Jgaa's Internet, http://war.jgaa.com/ftp/ (last visited Apr. 29, 2006) (describing one implementation of FTP clients and servers).

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

62. *See id.* § 202, 112 Stat. at 2877–86 (codified at 17 U.S.C. § 512 (2000)).

63. "Rather than embarking on a wholesale clarification of" the various doctrines of copyright liability, Congress opted "to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers." S. REP. NO. 105-190, at 19 (1998).

64. *See supra* notes 42–44 and accompanying text.

long as they were indeed passive[65] and also satisfied the largely untested requirement of having a policy of terminating repeat infringers.[66]

Section 512(c) was directed at OSPs: those who actually stored information for consumers for mass distribution to others, such as GeoCities[67] or Tripod,[68] or today's YouTube[69] or MySpace.[70] Section 512(c) exempted OSPs from liability so long as they acted expeditiously to remove infringing material after being notified of its presence by a copyright holder.[71] So, if a consumer were to upload a digital copy of a copyrighted book to her GeoCities home page, the publisher could send a "DMCA takedown notice" to GeoCities, which the OSP would disregard at its peril. The OSP ultimately might not be found contributorily or vicariously liable, but it would have to face litigation without the benefit of § 512's safe harbor.[72] Section 512(c) made some sense: OSPs did not have to worry about actively chaperoning their subscribers' activities, but if something was called to their attention, they could remove (or demand that their subscribers remove) the offending material and rest assured that they would be free from copyright liability. Section 512(c) represented a trend of encouraging "bouncer" gatekeeping of the sort that might have persisted in the defamation context had *CompuServe*'s distributor liability become the norm for OSPs instead of being trumped by the CDA.

As in the defamation context, a concern existed that offended parties would seek to get neutral bouncers to bounce overzealously. Section 512(f) was designed to limit takedown notices to honest ones, affirming that those targeted by a takedown notice — either the OSP or the individual content provider — could recover damages if a notice-giver knowingly misrepresented the challenged material to be actionable. This provision was tested when electronic voting machine maker Diebold, Inc., found that internal company e-mails discussing its machines' vulnerabilities had been leaked to the public web.[73] Among many other places, copies were placed on a website hosted by

65. *See* 17 U.S.C. § 512(a).

66. *See infra* text accompanying notes 84–92.

67. Yahoo! GeoCities, http://geocities.yahoo.com/ (last visited Apr. 29, 2006).

68. Tripod, http://www.tripod.lycos.com/ (last visited Apr. 29, 2006).

69. YouTube, http://www.youtube.com/ (last visited Apr. 29, 2006).

70. MySpace, http://www.myspace.com/ (last visited Apr. 29, 2006).

71. 17 U.S.C. § 512(c)(1)(A)(iii) (2000).

72. There could well be liability if an OSP were notified about an infringement claim and refused to do anything about it. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995) ("[P]laintiffs do raise a genuine issue of material fact as to their theory of contributory infringement as to the postings made after Netcom was on notice of plaintiff's infringement claim.").

73. *See* Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d. 1195, 1197 (N.D. Cal. 2004); *see also* Online Policy Group, Online Policy Group v. Diebold, http://www.onlinepolicy.org/action/legpolicy/opg_v_diebold/ (last visited Apr. 29, 2006).

Swarthmore College and managed by some Swarthmore students.[74] Diebold fired off takedown notices to OSPs hosting the documents, including Swarthmore, alleging that the postings infringed Diebold's copyrights.[75] Swarthmore compelled the students to remove the documents, and in response, the students sued Diebold alleging, inter alia, a violation of § 512(f).[76] The court agreed,[77] and Diebold paid $125,000 in damages for knowingly misrepresenting the status of the documents,[78] which were copyrighted but precluded from a finding of infringement by an obvious defense of fair use.[79]

Short of filing a lawsuit for damages under § 512(f) when takedown notices were thought to go too far, § 512(g) provided an alternative remedy for those posting information online: "counter-notifications." When an OSP notified a content-providing subscriber of a copyright-related complaint that had been lodged about her material, the subscriber could avow a good faith belief that her material was not indeed infringing — or more precisely, that it had been targeted as a result of "mistake or misidentification of the material to be removed or disabled."[80] The actual text of § 512(g) seemed oddly narrow, but if one construed "mistake" to include the idea of targeting noninfringing material in order to take it down, then §§ 512(g), 512(f) and 512(c) together evinced nuanced appreciation by Congress of the ways in which OSPs could make good gatekeepers — and the ways in which they should be left alone.

Section 512(d) offered nearly identical conditional protections to those available to OSPs under § 512(c), but here they were directed to those running "information location tools" that merely linked users to infringing content elsewhere online.[81] This safe harbor may have overreached a bit as a policy matter, unduly encouraging the blocking of innocent content by parties truly removed from the content's production or storage. Search engines, after all, are not in an explicit relationship with most of the websites they index — the way that OSPs are with their subscribers — which makes it harder for them to find

74. *See Diebold*, 337 F. Supp. 2d. at 1197–98.

75. *Id*. at 1198.

76. *Id.* at 1199.

77. *Id.* at 1204–06.

78. *See* Online Policy Group, *supra* note 73.

79. *See Diebold*, 337 F. Supp. 2d at 1204.

80. 17 U.S.C. § 512(g)(3)(C) (2000). Section 512(f) also provides for damages from those who knowingly misrepresent the state of affairs in their counter-notifications. *Id.* § 512(f).

81. In the absence of any safe harbor provisions, websites have been found to be contributory infringers of copyrighted works when providing links to that material. *See, e.g.*, Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290, 1292–95 (D. Utah 1999) (granting a preliminary injunction where the defendant's website had three links to other websites housing copyrighted material, and encouraged visitors to go to those sites, print the material, and send it to others).

and communicate with the creator of material under challenge. Moreover, given the absence of a contract, the directory service may have far less incentive to keep the owner of an excluded link in the loop. Information location tools are not at all like Kraakman's financial services gatekeepers, who are in privity with the clients that they are opportunistically asked to monitor. OSPs, on the other hand, better fit Kraakman's mold, presumably wanting to retain the subscribers whose material they host by allowing that material as much exposure as legal prudence dictates. Further, the volume of the sites that search engines typically index makes it manifestly labor-intensive to assess the credibility of takedown notices demanding removal of particular links from search results. Of course, as a safe harbor, § 512(d) was more an encouragement than a requirement; like the other provisions of § 512, it did not provide for liability if its conditions were not met, but only for the possibility of liability depending on how the judicially created law of contributory infringement developed. In the few U.S. cases on the subject, liability for mere hyperlinking has been applied delicately, if at all.[82]

In practice, it appears that search engine services such as Google have routinely abided by takedown notices in recent years, likely in order to enjoy the safe harbor for directory services of § 512(d). Google tempers the removal of directory results by concomitantly notifying a nonprofit website clearinghouse called "Chilling Effects" that the removal has taken place, and placing a referral to that clearinghouse in Google's results to indicate that there is missing information.[83]

The safe harbors for ISPs, OSPs, and search engines were further premised by § 512(i) on these entities having "adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers . . . who are repeat infringers."[84]

---

82. *See id.*; Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 341 (S.D.N.Y. 2000) (holding that granting an injunction or finding liability for linking is only proper when there is "clear and convincing evidence that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not be lawfully offered, and (c) create or maintain the link for the purpose of disseminating that technology"); Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828 (C.D. Cal. 2006) (denying in part a preliminary injunction against Google from linking to copyrighted images, and adopting a "server test" that limits direct infringement to websites "on which content is stored and by which it is served directly to a user"); Bernstein v. JC Penney, Inc., No. 98-2958 R Ex, 1998 WL 906644 (C.D. Cal. Sept. 29, 1998) (dismissing with prejudice where plaintiff sued Elizabeth Arden and JC Penney for copyright infringement, when Arden's perfume was promoted on the JC Penney website, which was linked to the Internet Movie Database website, which was linked to other websites, one of which contained an infringing photo of Elizabeth Taylor, Arden's spokesperson).

83. Chilling Effects, http://www.chillingeffects.org/ (last visited Apr. 29, 2006). The author is one of the founders of Chilling Effects.

84. 17 U.S.C. § 512(i)(1)(a) (2000).

This requirement suggested a role of bouncer not simply vis-à-vis a particular set of information in controversy. Rather, it anticipated identifying bad *people* rather than just bad acts, and it encouraged ISPs and OSPs to act against those people, truly serving as bouncers the way bouncers at night clubs and bars do, ejecting recidivist troublemakers. Must subscribers banned under such circumstances be banned for life in order to be true to the provision? Does "repeat infringer" mean a truly adjudged one — i.e., a court has so determined for a given defendant — or is the ISP to make the judgment of infringement, at least in obvious cases, when a third party brings alleged infringement to the ISP's attention? Is the threshold of repeat infringement met if a subscriber maintaining a home page has successive complaints lodged against her on Monday and then again on Wednesday? No authoritative answers to these questions have been generated. The House and Senate reports concerning § 512(i) are identical studies in ambiguity:

> [T]he Committee does not intend this provision to . . . suggest[] that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing. However, those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.[85]

In practice, it appears that those accused of persistent copyright infringement through their ISPs do not have their accounts terminated, even though the ISPs aspire to conform to the safe harbor's requirements. The publishers largely have not forced the issue of demanding such terminations through claims that the safe harbor has been forfeited when threatening a lawsuit for contributory or vicarious copyright infringement. The only notable case has been *Ellison v. Robertson*, in which a well-known science fiction author objected to AOL's apparent retransmission of pirated copies of his work through "Usenet," a chaotic, decentralized newsgroup system that forwarded messages from individuals around the world from one subscribing host to another.[86] Like most ISPs, AOL was a subscribing host to many Usenet groups; it made the groups' constantly-updated content available to its subscribers, who were then able to access copies of

85. H.R. REP. NO. 105-551, pt. 2, at 61 (1998); *see also* S. REP. NO. 105-190, at 51–52 (1998).

86. *See* 189 F. Supp. 2d 1051 (C.D. Cal. 2002), *rev'd*, 357 F.3d 1072 (9th Cir. 2004).

Ellison's work, among many other things.[87] AOL invoked the § 512 safe harbor, and claimed it met the requirements of § 512(i) for implementing a policy to terminate repeat infringers, despite apparently never having terminated a single subscriber for such infringements.[88] The district court agreed.[89] On appeal, the Ninth Circuit found that AOL's fidelity to § 512(i) was a jury question, but on the narrow basis that AOL had changed its e-mail address for receiving infringement notifications without providing sufficient notice to aggrieved authors like Ellison.[90] AOL and Ellison settled on remand before trial.[91]

OSPs like GeoCities, which are less passive than ISPs, might also terminate free home page accounts for any number of reasons, including outsiders' claims of copyright infringement, but little prevents a subscriber so terminated from simply establishing a new free account with the same OSP. Thus, while the "repeat infringer" provision of § 512(i) could in theory drastically increase the degree of intervention asked of intermediaries, especially of passive ISPs who must satisfy the provision to enjoy their safe harbor of § 512(a), it has not to date resulted in significant bouncer-like activities by either ISPs or OSPs.[92]

OSPs, ISPs, and search engines dominated the technological landscape of 1996–97, and the DMCA and CDA were designed to encourage these companies to act only in ways that would not drastically alter their business models or technological architectures. Aggrieved parties might allege and bring about the takedown of individual instances of flagrant copyright infringement, or even abuse the system to cause the removal of perfectly legal material, but determined individuals could repost such material elsewhere. In the meantime, most Internet authors would not encounter gatekeeping by the intermediaries through which their information flowed.

---

87. *Id.* at 1053–54.

88. *Id.* at 1064–66.

89. *Id.* at 1066.

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

91. *See* Jim Hu, *AOL Settles Copyright Claim*, CNET NEWS.COM, June 10, 2004, http://news.com.com/AOL+settles+copyright+claim/2110-1025_3-5230737.html.

92. One possible exception is universities, which are not in the profit-making business of selling Internet access. When students are said to be infringing copyrights through university access, some universities have demanded that the students stop on threat of losing that access, apparently to ensure that the university remains within the requirements of the § 512 safe harbors. *See, e.g.*, Matthew S. Lebowitz, *RIAA Targets Harvard Student*, HARVARD CRIMSON, Mar. 18, 2005, *available at* http://www.thecrimson.com/article.aspx?ref=506523 ("[T]he University does not actively look for students who are violating copyright law, but . . . it occasionally discovers such cases 'when there's a lot of bandwidth being used.' In these situations, a series of warning letters is sent to the student involved."); Letter from Courtney Bickel Lamberth, Allston Burr Senior Tutor, Winthrop House, Harvard Univ., to Aaron Koller, Undergraduate Student, Harvard Univ. (Oct. 17, 2001) (on file with author), *available at* http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=212. While the author has anecdotally heard of students' access actually being terminated, commercial ISPs apparently do not even pass along threats of termination to their customers.

V. LIMITED GATEKEEPING IS TESTED AS THE INTERNET DEVELOPS FURTHER: COPYRIGHT INFRINGEMENT, PEER-TO-PEER SERVICES, AND RENEWED CONSIDERATION OF DUTIES TO PREEMPT OR POLICE

Uses of the Internet soon evolved beyond the simple world of ISPs (passive conduits for others' material) and OSPs (hosts of others' material) contemplated in 1998's § 512 safe harbors. These developments have led to a new and more difficult set of puzzles about the proper use of both institutional and technological gatekeeping to cabin individuals' activities.

First, PC hardware horsepower grew. Hard disk storage capacities continued to double every eighteen months or so,[93] and raw processor speeds remained remarkably true to Moore's law,[94] named after the Intel engineer who predicted exponential growth.[95]

Second, Internet bandwidth grew,[96] including Net bandwidth available over the "last mile"[97] to many consumers.[98] From 1998 onwards, increasing numbers of people obtained broadband or migrated

93. Hard drive capacity doubled at a yearly rate from 1997 to 2001, before slowing down to the pre-1997 rate of 40 to 60 percent (doubling every eighteen months). *See* Brian Hayes, *Terabyte Territory*, 90 AM. SCI. 212, 214 (2002); Ed Frauenheim, *Midlife Crisis for the Hard Drive*, CNET NEWS.COM, Aug. 11, 2003, http://news.com.com/Midlife+crisis+for+the+hard+drive/2100-1008_3-5061923.html; *see also* Michael Singer, *Home Storage to Bolster Hard-Drive Growth*, CNET NEWS.COM, June 29, 2005, http://news.com.com/Home+storage+to+bolster+hard-drive+growth/2100-1041_3-5768676.html.

94. *See* Herb Sutter, *A Fundamental Turn Toward Concurrency in Software*, DR. DOBB'S J., Mar. 2005, at 16, 18, *available at* http://www.gotw.ca/publications/concurrency-ddj.htm.

95. *See* Wikipedia, *Moore's Law*, http://en.wikipedia.org/wiki/Moore's_law (as of Mar. 23, 2006, 09:48 GMT) ("Moore's law is about the empirical observation that at our rate of technological development, the complexity of an integrated circuit, with respect to minimum component cost, will double in about 18 months.").

96. *See* A. M. Odlyzko, *Internet Traffic Growth: Sources and Implications*, 5247 PROC. SPIE 1 (2003), *available at* http://www.dtc.umn.edu/~odlyzko/doc/itcom.internet.growth.pdf (estimating that Internet traffic has doubled every year since 1997); *see also* K. Satya Sai Prakash & S. V. Raghavan, *Analysis of the Web, Processor Speed and Bandwidth Growth: Impact on Search Engine Design*, 2003 PROC. IADIS INT'L CONF. WWW/INTERNET 137, 142 fig.10, *available at* http://nsl.cs.iitm.ernet.in/publications_files/pub/sai/analysis_of_web.pdf (charting the exponential growth in Internet bandwidth from 1992 to 2002).

97. *See* Wikipedia, *Last Mile*, http://en.wikipedia.org/wiki/Last_mile (as of Feb. 8, 2006, 03:26 GMT) ("The last mile is the final leg of delivering connectivity from a communications provider to a customer. Usually referred to by the telecommunications and cable television industries, it is typically seen as an expensive challenge because 'fanning out' wires and cables is a considerable physical undertaking.").

98. *See* Coastal Carolina Univ., Technology and Instruction Course Module, Accessing the Internet, http://www.coastal.edu/education/ti/internetaccess.html (last visited Apr. 29, 2006) (observing that "[a]s of August, 2004, roughly 40% of Internet subscribing households use broadband connections, and most pundits have noted that this trend will only increase as demand grows for more bandwidth-intensive content, especially music and video").

to it from dial-up access,[99] making not only for faster connections but also for always-on connections, since, unlike the modem, the high speed connection did not occupy a household's telephone line.[100]

In 1998, PCs out of the box could recognize and play audio compact discs ("CDs"), but offered no option to copy them to a PC hard drive. Much as independent programmers developed the first software allowing PCs to easily connect to the Net,[101] outside developers wrote simple code enabling "digital audio extraction" of standard music CDs onto PCs.[102] The resulting files could be quite large, especially for hard drive capacities of the era, but clever algorithms for digital music compression emerged, including the independently patented "MP3" standard.[103] It was now feasible to store high-quality copies of one's CDs on a PC.[104]

These MP3 files could be distributed via e-mail or even posted on the web. Should they be posted on a home page hosted in the typical subscriber/OSP configuration, they would be vulnerable to OSP takedown, since the OSP would want to retain the § 512(c) safe harbor, just as the 1998 DMCA intended. Thus aided by OSP gatekeepers, recording industry publishers engaged in a sufficiently rapid cat-and-mouse game with those posting MP3 files online, and battled at least to a stalemate, if not better.[105] At that time, there were no easy, continuous, reliable sources for pirated music on the Net at large.

---

99. *See id.*; *see also* JOHN B. HORRIGAN & LEE RAINIE, PEW INTERNET & AMERICAN LIFE PROJECT, THE BROADBAND DIFFERENCE 4–5 (June 23, 2002), http://www.pewinternet.org/pdfs/PIP_Broadband_Report.pdf.

100. *See* ROUZBEH YASSINI ET AL., PLANET BROADBAND 91–93 (2003), *available at* http://www.informit.com/articles/article.asp?p=101402&seqNum=2 (describing the "anthropology" of always-on Internet connections in daily life).

101. *See* Trumpet Software International, History, http://www.trumpet.com.au/history.html (last visited Apr. 29, 2006); Zittrain, *supra* note 15, at 1992.

102. *See* BRUCE FRIES, THE MP3 AND INTERNET AUDIO HANDBOOK (2000) 169–80, *available at* http://www.teamcombooks.com/mp3handbook/15.htm ("Digital audio extraction (DAE), commonly referred to as ripping, is the process of copying audio data directly from a CD. Because it bypasses the sound card, ripping normally results in a perfect copy with no introduction of noise or loss of fidelity."). For an example of an open source digital audio extraction software application, see Ripoff: Python Tools for CD Ripping, http://ripoff.sourceforge.net/ (last visited Apr. 29, 2006).

103. *See also* FRIES, *supra* note 102, at 1, *available at* http://www.teamcombooks.com/mp3handbook/Intro.htm ("MP3 (technically, MPEG Audio Layer-III) is a standard format for compressing digital audio. MP3 squeezes audio files to about one tenth of their original size, while maintaining close to CD quality.").

104. *See id.*

105. JOHN ALDERMAN, SONIC BOOM: NAPSTER, MP3, AND THE NEW PIONEERS OF MUSIC 30 (2001); Janelle Brown, *Heat Turned Up on Digital Music Pirates*, WIRED NEWS, Feb. 12, 1998, http://www.wired.com/news/culture/0,1284,10234,00.html; *see also* FRIES, *supra* note 102, at 43–56, *available at* http://www.teamcombooks.com/mp3handbook/5.htm (discussing hypothetical scenarios regarding use of digital music and copyright laws).

Subsequent innovations clouded such gatekeeping operations. In May 1999, teenager Shawn Fanning founded Napster.[106] Napster was three things, together representing the emerging PC/Internet grid. First, Napster was a piece of software that one could download to a PC running recent versions of the Windows operating system.[107] Second, it was a website, which one could visit in order to get the software, and a corresponding Internet server that one's PC could access once the software was running.[108] And third, more inchoately, it was a "network" — a set of virtual connections among people running the Napster application on their networked PCs, brokered by the Napster server through the Internet.[109]

Napster users could denote areas of their PC hard drives containing MP3 files that they wished to make available to other Napster users.[110] When running the software, each PC would check in to the central Napster server over the Internet and alert it to the contents of these shared directories.[111] Users wanting to find MP3 files held by others could then ask the central Napster server whether particular files, identified by name or parts of a name, could be found on anyone's drive.[112] When the Napster server found a match between someone desiring a file and someone offering that file, the Napster software on the respective machines would then orchestrate a direct PC-to-PC connection so that the file could be transferred.[113] The increasing number of always-on consumer connections meant that PC owners could leave Napster running twenty-four hours a day, providing others with constant access to their files and incurring no special charge, since broadband access within the U.S. is typically metered at a flat rate regardless of the amount of data transferred.[114]

---

106. Wikipedia, *Napster*, http://en.wikipedia.org/wiki/Napster (as of Mar. 24, 2006, 18:26 GMT); s*ee also* STUART BIEGEL, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 286–90 (2001). *See generally* JOSEPH MENN, ALL THE RAVE: THE RISE AND FALL OF SHAWN FANNING'S NAPSTER (2003).

107. Susan Crosse et al., *Napster*, *in* P2P NETWORKS (TCD 4BA2 PROJECT 2002/03) ch. 4 (2003), http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p4.html (explaining the basic structure of Napster).

108. *See id.*

109. *See id.*

110. WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT 111 (2004).

111. *Id.*

112. *Id.*

113. *Id.*

114. *See, e.g.*, BroadbandReports.com, http://www.broadbandreports.com/dosearch?cheap=1 (last visited Apr. 29, 2006) (listing broadband providers by monthly charge). *But see* Jo Twist, *Goodbye to a Flat Rate for Broadband?*, BBC NEWS, Sept. 15, 2003, http://news.bbc.co.uk/2/hi/technology/3109146.stm (discussing the possibility of replacing flat rate broadband pricing with tiered pricing depending on usage).

PC data storage; file searching; file transfer — the building blocks of Napster simply awaited someone like Fanning to put them together into a service whose whole would yield an impact greater than the sum of its parts. Fanning needed no gatekeeper's permission to open shop at Napster.com or to write an application that could run on a massive percentage of existing consumer PCs. Consumers found no barrier to the addition of Napster software to their generative machines, nor to the use of their network connections to transmit Napster-related data. Network and PC generativity enabled modern file-sharing to go from nonexistent to ubiquitous in a stunningly short period of time. Napster's popularity blossomed, and the more popular Napster became, the more valuable it became to consumers because more files were available on its network.[115]

The U.S. recording industry's trade association sued Napster, Inc., to try to shut down its service through an injunction and perhaps incapacitating damages.[116] The lengthy litigation itself spawned a number of new technologies to fill Napster's shoes,[117] and in turn a new round of lawsuits designed to stymie Napster's successors.[118] The judicial opinions rendered in these lawsuits sought to apply doctrines of contributory and vicarious copyright infringement to new fact patterns. With concomitant legislative activity, these opinions represented traditional regulatory efforts to prune away undesirable applications of network and PC generativity without requiring undue gatekeeping by intermediaries. Such efforts showed the judicial sys-

---

115. *See* BIEGEL, *supra* note 106, at 421 n.12. Napster's popularity grew quickly. When the program started in September 1999, the number of users was doubling every five to six weeks. Matthew Green, Note, *Napster Opens Pandora's Box: Examining How File-Sharing Services Threaten the Enforcement of Copyright on the Internet*, 63 OHIO ST. L.J. 799, 801 (2002). As of December 21, 2000, Napster had more than 40 million registered users. Damien A. Riehl, Note, *Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?*, 27 WM. MITCHELL L. REV. 1761, 1767 n.30 (2001). At Napster's height of usage in February 2001, Napster had more than 80 million registered users. Green, *supra*, at 802; Matt Richtel, *Upheaval at Bertelsmann May End Plans for Acquisition of Napster,* N.Y. TIMES, July 31, 2002, at C1. In January 2001, it was estimated that approximately 1.6 million users were connected to Napster at all times and 2 billion songs were downloaded. Green, *supra*, at 802; Jefferson Graham, *Napster Moving Toward Monthly Fee: Song-Swapping Service Could Set the Tone for Internet Music Sales*, USA TODAY, Jan. 30, 2001, at A1.

116. Notice of Joint Motion & Joint Motion of Plaintiffs for Preliminary Injunction, *In re* Napster, Inc. Copyright Litig., 191 F. Supp. 2d 1087 (N.D. Cal. 2002) (No. C-99-5183 MHP), 2000 WL 34016493.

117. *See* Leander Kahney, *Still Plenty of Music Out There*, WIRED NEWS, Feb. 13, 2001, http://www.wired.com/news/business/0,1367,41775,00.html.

118. *See, e.g.*, Katie Dean, *P2P Whipping Boy: Know the Risks*, WIRED NEWS, May 10, 2003, http://www.wired.com/news/print/0,1294,58783,00.html; Brad King, *Kazaa: A Copyright Conundrum*, WIRED NEWS, Mar. 4, 2002, http://www.wired.com/news/print/0,1294,50788,00.html; Brad King, *File Trading Sites in Crosshairs*, WIRED NEWS, Oct. 3, 2001, http://www.wired.com/news/mp3/0,1285,47296,00.html; *Play it Again RIAA: Sue Morpheus*, REUTERS, June 3, 2003, *available at* http://www.wired.com/news/digiwood/0,1412,59097,00.html.

tem struggling with questions of regulability of individual behavior, and of the extent to which various service providers (traditional gatekeepers) and technology creators (technological gatekeepers) should be enlisted to halt — or stop enabling, depending on one's baseline — undesirable user behavior.

The district court issued a preliminary injunction against Napster, the core of which was upheld on appeal.[119] As a doctrinal matter, the Ninth Circuit first determined that the unauthorized swapping of copyrighted files among strangers was a direct infringement — a finding that perhaps lent too little weight to fair use considerations.[120] Once direct infringement was established, the court turned to the question of whether Napster was contributorily and vicariously responsible for aiding the infringing activities.[121] The Ninth Circuit opinion in this respect was careful and measured.

The court reasoned that the § 512(d) safe harbor for information location tools probably would not apply, but recognized that the question would be more fully developed once the case reached trial.[122] Such a judgment is not surprising because, in the district court, Napster had only weakly claimed in the alternative to fall under § 512(d).[123] Instead, Napster had pinned its hopes on § 512(a),[124] wanting to be characterized as a passive conduit ISP and thereby avoid the notice-and-takedown predicates of § 512(d), which it apparently had not met.[125] Napster was not an ISP — indeed, neither plain-

---

119. *Napster II*, 239 F.3d 1004, 1027 (9th Cir. 2001).

120. *See id.* at 1013–16; *see also* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1400 n.222 (2004) ("While the Ninth Circuit gave short shrift to Napster's claims that its users were engaged in 'space-shifting' (downloading songs they already owned in order to play them at a different location) or 'sampling' (downloading a song in order to decide whether to buy the CD) and found that many Napster users did not engage in these practices, any copyright infringement claim against particular downloaders themselves would have to contend with these arguable fair use defenses. The Ninth Circuit had earlier endorsed the practice of space shifting in *Recording Industry Association of America v. Diamond Multimedia Sys., Inc.*, but that occurred in the context of a device that permitted personal space shifting without making files accessible to others.") (citations omitted).

121. *Napster II*, 239 F.3d at 1020–23.

122. *Id.* at 1025.

123. *See* A&M Records, Inc., v. Napster, Inc. (*Napster DMCA*), No. C 99-05183 MHP, 2000 WL 573136, at *5 (N.D. Cal. May 12, 2000) (noting that "defendant maintains that, even if the court decides to analyze the information location functions under 512(d), it should hold that the 512(a) safe harbor protects other aspects of the Napster service"), *available at* http://www.eff.org/IP/P2P/Napster/DMCA_Ruling.pdf.

124. *See id.*

125. *See* A&M Records, Inc. v. Napster, Inc. (*Napster I*), 114 F. Supp. 2d 896, 919 n.24 (N.D. Cal. 2000), *aff'd in part*, *rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) ("This finding also puts an end to defendant's persistent attempts to invoke the protection of the Digital Millennium Copyright Act, 17 U.S.C. section 512. In its opposition brief, Napster, Inc. attempts to persuade the court that subsection 512(d) provides an applicable safe harbor. However, this subsection expressly excludes from protection any defendant who has 'actual knowledge that the material or activity is infringing,' § 512(d)(1)(A), or 'is aware of facts or

tiff nor defendant claimed that Napster was in the business of transmitting files from one user to another — and both the district court and Ninth Circuit properly relied on this fact in rejecting § 512(a) as well.[126]

In the absence of these safe harbors, Napster was now subject to an analysis of contributory and vicarious infringement. Recall that contributory infringers are those who know about infringing activity and who materially assist in it. This standard is met, in the easy case, if one has actual knowledge of infringement and then assists in it or fails to stop assisting. Thus, a copy shop like Kinko's would be asked to serve as a gatekeeper when its employees were explicitly presented with copyrighted material clearly labeled "all rights reserved" and asked to produce copies of it, as for student course packs.[127] This scenario is akin to the defendant-friendly "distributor" level of liability that a bookstore might assume for knowingly stocking and selling defamatory material. OSPs were explicitly exempted from this *CompuServe* level of liability for defamation thanks to the CDA, a distinction from the copyright context that might be understandable if one thinks a gatekeeper would have more difficulty verifying a text's defamatory character than its copyright status.[128]

The easy case of actual knowledge can quickly give way to harder ones. What about copy shops that simply place photocopying machines in the lobby and allow customers to use them on a fee-for-page basis? Appropriately, the availability of machines that could be used for copyright infringement — and no doubt are, over the course of the day, arguably giving rise to *constructive* knowledge of infringement — does not alone give rise to the level of knowledge requisite for contributory liability.[129] One could imagine asking Kinko's to

---

circumstances from which infringing activity is apparent.' § 512(d)(1)(B). Defendant has failed to persuade this court that subsection 512(d) shelters contributory infringers.").

126. *See Napster DMCA*, 2000 WL 573136, at *5; *Napster II*, 239 F.3d at 1025.

127. *See* Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1526 (S.D.N.Y. 1991); *see also* Stephana I. Colbert & Oren R. Griffin, *The Impact of "Fair Use" in the Higher Education Community: A Necessary Exception?*, 62 ALB. L. REV. 437 (1998) (suggesting that universities develop and approve internal policies and procedures that advocate or sanction a broader interpretation of the laws relating to fair use, and engage in collective action to lobby for enhanced use and dissemination of copyrighted material).

128. There are nontrivial problems even in identifying copyright status. *See, e.g.*, Chris Sprigman, *Reform(aliz)ing Copyright*, 57 STAN. L. REV. 485, 497, 515 (2004).

129. While copyright infringement cases have been successfully brought against copy centers with full-service copying functions, *supra* note 127, no reported cases have challenged the mere act of providing self-service copying machines. *But cf.* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distrib., 983 F. Supp. 1167, 1178–79 (N.D. Ill. 1997) (leaving open the prospect of contributory infringement for the defendant web hosting company, whose subscriber placed infringing material on its servers, despite finding defendant not liable for direct infringement because it was "much like the owner of a public copying machine used by a third party to copy protected material"). For more discussion on the parallel services offered by ISPs, see Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J.

monitor its customers' self-service machine use and fitting such gatekeeping liability within the contributory or vicarious copyright infringement framework, but the law rightly stops short in such an instance. Such a regime would impose excessive tertiary costs upon innocent customers, who would be unable to gain access to self-service photocopying because shops would be compelled to charge significantly more to cover monitoring costs, or would simply shut down the service entirely.[130] Exactly where to draw the line is a matter for further cases, but the line-drawing in the copy shop cases exhibits a sensitivity toward eliminating flagrant instances of gatekeeper-aided individual wrongdoing while avoiding excessive burdens on gatekeepers.[131]

Similarly, the upstream *makers* of photocopying machines and similar technologies are insulated from contributory liability for the act of producing and distributing the technologies. The landmark *Sony* case of 1984 imported the "staple article of commerce" doctrine from patent law to apply to copyright law in contributory infringement cases where, otherwise, the manufacturer arguably would have constructive knowledge of the infringing uses to which its product might be put.[132] So long as the product was "merely . . . capable of substantial noninfringing uses,"[133] its maker — in the absence of specifically marketing the product for wrongful uses[134] — would not be found liable for infringement. *Sony* evinced solicitude for new technologies that could find legitimate use once they took hold, and a concern that if the contributory infringement doctrine were applied too broadly, copyright holders could extend their monopolization of the market in their works into monopolization of VCR production itself — an enti-

---

1833, 1874 & n.210 (2000) (suggesting that after *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), most ISPs lack "the requisite level of knowledge" for the imposition of contributory liability).

130. *Compare* Lemley & Reese, *supra* note 120, at 1349–50 (cautioning against unrestricted liability and noting that innovation will be stifled by going after third parties like investors and law firms), *with* Benjamin H. Glatstein, Comment, *Tertiary Copyright Liability*, 71 U. CHI. L. REV. 1605, 1635 (2004) (weighing the arguments for and against extending tertiary liability in copyright law to investors and suppliers of technology, and concluding that "tertiary liability would encourage cost-effective deterrence and monitoring, which would lower overall infringing activity").

131. *Cf.* Alfred C. Yen, *A Preliminary Economic Analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining*, 26 U. DAYTON L. REV. 247 (2001) (arguing that a court should be very cautious about extending copyright liability to makers of technologies like Napster because an injunction does not increase the possibility of meaningful bargaining or decrease transaction costs, and as such, may conflict with Coasean efficiency).

132. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 440–42 (1984).

133. *Id.* at 442.

134. The instruction booklet Sony included with each Betamax video tape recorder contained the statement: "Television programs, films, videotapes and other materials may be copyrighted. Unauthorized recording of such material may be contrary to the provisions of the United States copyright laws." *Id.* at 426.

tlement not granted by copyright law, and one that indeed would be harmful to innovation.[135]

In its application of *Sony*, the Ninth Circuit was laudably careful in distinguishing between Napster as a technology (the client software and the file-matching server) and Napster as an ongoing service.[136] Napster was, in essence, both building a particular kind of photocopying machine out of parts drawn from PCs and the Internet *and* offering a copy-shop-like service by running the server software at Napster.com. The opinion implies that had Napster merely built the Napster server and client software and then conveyed the server operation to someone else, it likely would have escaped liability under *Sony*.

It was Napster as a service that posed the greatest intellectual challenge of the case, and that ultimately landed Napster, Inc., in hot water. If the service operated analogously to a copy shop in important respects, the challenge would be determining whether Napster's operation were more like the copy shop lobby or the activity behind the shop's counter. On the one hand, while the Napster service was partially centralized, no human intervention occurred at the hub to make the service work.[137] The pairing of people looking for MP3 files with those offering them was automatic.[138] This characterization makes Napster seem like the self-service section in the copy shop lobby; as a matter of course, no one in authority watched or intervened in the customers' work once the customers were registered.[139] On the other hand, all requests flowed through Napster's servers, which meant that infringing files could be detected and potentially blocked once

---

135. *Cf.* S.J. Liebowitz & Stephen E. Margolis, *Should Technology Choice Be a Concern of Antitrust Policy?*, 9 HARV. J.L. & TECH. 283 (1996) (discussing the role of "path dependence" and "network externalities" in creating technology monopolies, including VCR production).

136. *See Napster II*, 239 F.3d 1004, 1020 (9th Cir. 2001) ("We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system.").

137. Napster's server maintained a "search index" of Napster's collective directory. The server compiled a list of all MP3 file names from the search index and transmitted the list to users who entered a particular search term. This process was performed by software located on the Napster server. *Id.* at 1012.

138. The Napster servers communicated one user's Internet address to another user. The requesting user's computer then used this information to establish a connection and download a copy of the first user's MP3 file. *Id.*

139. *See Napster I*, 114 F. Supp. 2d 896, 905 (N.D. Cal. 2000), *aff'd in part*, *rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) (noting that registration with Napster does not require the user to provide a real name or address, and that once a user logs on, her physical address information is no longer available to the Napster server); *see also* Reply Brief of Appellant Napster, Inc. at 23, *Napster I*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) (Nos. 00-16401, 00-16403), 2000 WL 34004361 (arguing "the relevant issue . . . is not whether a defendant has any ongoing relationship with consumers, but whether a defendant has a direct involvement such that it can distinguish between infringing and noninfringing uses").

found.[140] Indeed, the record companies themselves could and did detect them with decent, if not complete, accuracy: they simply became Napster users and asked for file names matching the titles of songs whose copyrights they controlled.[141]

The Ninth Circuit fashioned an application of contributory infringement that addressed this situation somewhere between the lobby and the counter. The court said that Napster would not have to ferret out infringing files on its own, but affirmed the district court's finding that, once notified of such files by the record companies, Napster must do everything feasible to block these files from its system.[142] The district court had little patience for the cat-and-mouse game that resulted[143] as Napster tried to modify its service, under the supervision of a special master, to filter out infringing files identified by the record companies, and users allegedly tried to cloak such files from detection through tricks like more creative naming conventions.[144] One could take issue with the district court's application of this standard, but the overall rule showed sensitivity to the technological status quo; the courts did not want to tell software authors how to write their software. To do so, even with a generous standard of liability, would

---

140. The Ninth Circuit noted:

> The district court correctly determined that Napster had the right and ability to police its system and failed to exercise that right . . . however, [the district court] failed to recognize that the boundaries of the premises that Napster 'controls and patrols' are limited . . . the Napster system does not 'read' the content of indexed files other than to check that they are in the proper MP3 format. Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system.

Napster II, 239 F.3d at 1023 (citations omitted).

141. *See Napster I*, 114 F. Supp. 2d at 902–04 (discussing methodologies used by plaintiff's expert); *cf.* Almar Latour, *Firm Touts Technology to Beat Hackers*, WALL ST. J., Nov. 13, 2000, at 1, *available at* http://proquest.umi.com.ezp1.harvard.edu/pqdweb?did=63639308&sid=1&Fmt=3&clientId=11201&RQT=309&VName=PQD ("MediaDefender claims the answer lies in so-called 'spoofing,' a method in which a peer-to-peer entertainment network gets flooded with fake files of a certain title. As soon as an end user tries to download a certain electronic media file, he will actually download a 'spoof' that is titled after the requested song or video but actually contains a message warning the user that he or she has attempted to break copyright law.").

142. *Napster III*, 284 F.3d 1091, 1098 (9th Cir. 2002) (affirming that "plaintiffs bear the burden 'to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content'" (quoting *Napster II*, 239 F.3d at 1027)).

143. *See id.* at 1097 ("The district court was dissatisfied with Napster's compliance despite installation of a new filtering mechanism. . . . The district court ordered Napster to keep the file transferring service disabled until Napster satisfied the court 'that when the [new] system goes back up it will be able to block out or screen out copyrighted works that have been noticed . . . . and do it with [a] sufficient degree of reliability and sufficient percentage [of success]. . . . It's not good enough until every effort has been made to, in fact, get zero tolerance. . . . [T]he standard is, to get it down to zero.'").

144. *See* A&M Records, Inc. et al. & Leiber et al.'s Opening Brief at 5, *Napster III*, 284 F.3d 1091 (Nos. 01-15998, 01-16003, 01-16011), 2001 WL 34094938.

make amateur software writers concerned that any tool they developed could produce a lawsuit.

Rather, the court stuck to opportunistic traditional gatekeeping of the sort found in *Prodigy*, and endeavored to tell service providers how to offer those services that were closely enmeshed with copyright infringement. To expect otherwise would ignore both the politics of the situation and its equities. The Napster service enabled, in plain view of the world, the infringement of millions of copyrights on a daily basis. It appeared to have been founded for that very purpose, and it was promoted using screen shots listing song titles that appeared to be plainly infringing.[145] The initial inability of the service operators to find out the identity of its users or whether a specific file was infringing was something that could be changed, especially if the design decisions behind such limitations were taken precisely to avoid liability: a co-founder of Napster had explained "the need to remain ignorant of users' real names and IP addresses 'since they are exchanging *pirated* music.'"[146] To the extent that the service could be easily changed, the court would require it. To be sure, changing the way the service worked entailed changing its software, but this was still a different matter than changing the fundamental architecture of Napster. At a copy shop counter, changes to service offerings to conform to legal requirements might happen through new instructions to employees; online, the changes are facilitated through new instructions to software. These instructions could be implemented comparatively easily, because the software in question already operated at the level of individual files.[147] File names (and corresponding files) were the units by which Napster operated, and a filter could be interposed that blocked one file name (or file) but not another.[148] The court would not tell software writers how to write their software, but it would tell for-profit service operators how to tweak their software — an astute distinction in a difficult case.

This distinction is sensible because it separates elements of analysis that are otherwise easy to conflate. By the Ninth Circuit's lights, the first question to ask in a contributory copyright infringement case is whether the instrumentality at issue is a product or a service. If it is a product, then the *Sony* rule applies, and so long as the product is capable of substantial noninfringing uses, constructive knowledge of infringing uses will not be imputed and the inquiry ends, preserving maximum freedom for those who write software. If the instrumental-

145. *Napster I*, 114 F. Supp. 2d at 919.

146. *Id.* at 918 (emphasis in original).

147. *See Napster II*, 239 F.3d at 1012.

148. *See Napster III*, 284 F.3d at 1095–96, 1098 (affirming the district court's order that Napster remove from the system's music index any user file that contains plaintiffs' copyrighted works once plaintiffs have given proper notice of specific infringing files).

ity is a service, then the *Sony* rule goes so far as to say that the service provider is under no general duty to monitor for infringing materials. However, if the service operator is told of specific infringing material, then the operator is under a duty to purge such material from its index as much as is feasible — with "feasible" no doubt being a much contested debate between the publisher and the service provider.[149] This duty to feasibly purge attaches even when the service is generally capable of substantial noninfringing uses, since there is now actual knowledge of infringement; constructive knowledge need not be imputed, so the *Sony* defense does not come into play. The Ninth Circuit maintained *Sony's* implicit distinctions between products and services, between distributor and publisher liability, and between traditional and code-based gatekeeping.

Truly passive ISPs likely would not be swept into this application of *Sony*. First, they transmit rather than index or store material, and thus have nothing to purge if they are later told of infringements. Second, § 512(a) specifically exempts them from a claim of infringement, at least so long as they abide by § 512(i)'s curiously untested requirement to terminate repeat infringers.[150] Those offering more generic services that could enable infringement, such as e-mail providers, "file locker" companies,[151] or instant messaging services[152] would also remain off the hook. As a practical matter, so long as *Sony* is thought to preclude the duty to actively seek out infringements, then those infringements would remain private, and publishers would be unable to identify them and bring them to the service provider's attention for action. It is only when a service allows the public swapping of files among complete strangers that the publishers can so cheaply identify infringing materials and ask for intervention. It was this very fact that called for attention as a political matter: Napster was the open air drug market of copyright infringement, and as such, the service it provided had to be stopped.

---

149. *Compare, e.g.*, A&M Records, Inc. et al. & Leiber et al.'s Opening Brief, *supra* note 144, at 5 (arguing that the requirements to provide notice of infringing files to Napster is a burden "akin to trying to prevent a record store from infringing copyrights by ordering the *copyright owners* first to go through all of the record store's inventory, locate the music they own, and then give that information to the store before it has to remove those works . . . . Unlike a record store, however, not only are *millions* of different works available on Napster, but the identities and availability of those millions of works change literally every second" (emphasis in original)), *with* Reply Brief of Defendant/Appellee/Cross-Appellant Napster, Inc. at 3, *Napster III*, 284 F.3d 1091 (Nos. 01-15998, 01-16003, 01-16011, 01-16308), 2001 WL 34095289 ("As far as Plaintiffs are concerned, no amount of policing will suffice — even if additional screening methods result in massive overblocking of noninfringing works, and even if Napster must radically change its architecture by adopting a 'filter in' scheme in which all content is preapproved before being made available.").

150. *See supra* text accompanying notes 84–92.

151. *See, e.g.*, YouSendIt, http://www.yousendit.com (last visited Apr. 29, 2006).

152. *See, e.g.*, AOL Instant Messenger, http://www.aim.com (last visited Apr. 29, 2006).

The Seventh Circuit reached a similar conclusion on slightly different reasoning when it ruled against Aimster.[153] Aimster was very much like Napster.[154] It was marketed to individuals who wanted to trade music files. It comprised a website that one could visit, proprietary software that one could download to one's PC, and a central server accessed by that software that performed the indexing function, as Napster did.[155] In a programming shortcut, at the moment that an Aimster user wanted to download a file from another user, the PC's instant messaging software was invoked to perform the transfer. The Aimster software itself did not perform the peer-to-peer file transfer.[156] The website also offered "Club Aimster," whereby users could pay a fee to find out what the most popular music files were.[157] Of course, the popular files generally turned out to be music under copyright.[158]

Like Napster, Aimster first tried to rely upon a § 512 safe harbor. In a brief and somewhat murky section of its opinion, the Seventh Circuit accepted the categorization of Aimster as worthy of the protections of one of the § 512 subsections,[159] but did not find it necessary to settle on a particular subsection because Aimster did not enforce a policy of terminating repeat infringers as required by § 512(i) — indeed, it appeared to encourage copyright infringement.[160]

The court's description of the scope of contributory infringement was simultaneously narrower and broader than the Ninth Circuit's, averaging out to roughly the same result, but with worrisome implications for IT generativity. The scope was narrower because the Seventh Circuit believed that *Sony*'s limitations on liability applied even in the face of "actual knowledge of specific infringing uses,"[161] stating that the Ninth Circuit erred in holding otherwise. The court based its conclusion on the fact that Sony, Inc., was held not to be an infringer even though the *Sony* majority acknowledged that 25 percent of VCR

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

154. *See* Wikipedia, *Madster*, http://en.wikipedia.org/wiki/Madster (as of Feb. 27, 2006, 00:29 GMT) ("Madster was one of the many P2P file sharing services that appeared in Napster's wake. Initially called AIMster, it allowed users to share their files with others, but only with those on their buddy lists. Aimster did not use the AOL/AIM network for any of its traffic, it used its own servers.").

155. *Aimster*, 334 F.3d at 646.

156. *Id.*

157. *Id.*

158. *Id.* at 652. The court noted, "Club Aimster's monthly fee is the only means by which Aimster is financed." *Id.*

159. *Id.* at 655 (citing to the definition of Internet service provider at 17 U.S.C. § 512(k)(1)(B)).

160. *See id.*

161. *Id.* at 649.

users were said to be using the equipment to infringe copyrights.[162] The Ninth Circuit had the better of this argument, pointing out that the question was not whether a creator of a technology knew of a specific infringement, but rather whether the creator found out at a time when something could be done about that specific infringement. For a consumer to infringe using a VCR, she had to own one, but by that time, it was too late for Sony to try to stop her infringing behavior. Thus, the Ninth Circuit read *Sony* to provide a near-blanket exemption from liability for creators of products, so long as those products were capable of substantial noninfringing uses.[163] Knowledge of the product's infringing uses in the marketplace would not provide a basis to demand that a manufacturer have preemptively designed the product to avoid those uses.

In this respect, the Seventh Circuit treated creators of products and providers of services interchangeably. While this result may have seemed to be a boon to some would-be defendants — giving service providers more extensive protection under *Sony*'s rule than the Ninth Circuit's reading would — the Seventh Circuit then proceeded to broaden the scope of contributory infringement by eliminating "capability of substantial noninfringing uses" as the trigger for *Sony* protection.[164] The only facts developed in the district court were that Aimster was used to trade copyrighted files; while it surely could have been used to, say, trade business documents, as the defendants argued, the court found it significant that there was no evidence that it had actually been so used.[165] Once the simple thought experiment threshold of "capable of substantial noninfringing uses" was read to be a necessary, rather than a sufficient, condition for exemption from contributory liability, a balancing test was added to fill out the picture: "[W]hen a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement."[166] The court then imagined possible noninfringing uses

---

162. *Id.*

163. At least one commentator argues that the *Aimster* ruling was significantly driven by Aimster's failure to produce evidence of substantial noninfringing uses, even though *Sony* suggests that the burden of proof falls to the plaintiff. *See* Elizabeth Miles, Note, In re Aimster *&* MGM, Inc. v. Grokster Ltd.*: Peer-to-Peer and the* Sony *Doctrine,* 19 BERKELEY TECH. L.J. 21, 42 (2004) ("First, and fatally to Aimster, [Judge Posner] proposed that the burden to show substantial noninfringing uses falls on the defendant.").

164. *See id.* at 34; Brandon M. Francavillo, Note, *Pretzel Logic: The Ninth Circuit's Approach to Contributory Copyright Infringement Mandates that the Supreme Court Revisit Sony*, 53 CATH. U. L. REV. 855, 868–69 (2004).

165. *Aimster*, 334 F.3d at 653 ("[D]efendants here have provided no evidence whatsoever (besides the unsupported declaration of Deep) that Aimster is *actually* used for any of the stated non-infringing purposes." (emphasis in original) (quoting *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 653 (N.D. Ill. 2002))).

166. *Id.* at 649.

for Aimster, but denied them weight for lack of any evidence that they were in use.[167]

The principal drawback of the Seventh Circuit's reasoning was that its interpretation of *Sony* provided less of a shield to makers of products as well as service providers. The court noted that the *Sony* opinion did not discuss the possibility that the VCR manufacturer could have preemptively engineered the recorder in a way to preclude some infringement,[168] but that its reasoning did suggest that a test balancing the cost of such engineering against the benefit to be gained would be appropriate in such an instance.[169]

Unlike the Ninth Circuit, the Seventh Circuit conflated the distinction between products and services — the underlying technology and the way the business operates. In doing so, the Seventh Circuit also blurred the distinction between publisher and distributor liability upon which technology companies had come to rely. The Seventh Circuit's approach also exposed technology companies to a new type

---

167. *Id.* at 652–53.

168. The Seventh Circuit noted:

> [A]lthough Sony could have engineered its video recorder in a way that would have reduced the likelihood of infringement, as by eliminating the fast-forward capability, or . . . by enabling broadcasters by scrambling their signal to disable the Betamax from recording their programs (for that matter, it could have been engineered to have only a play, not a recording, capability), the majority did not discuss these possibilities.

Id. at 648 (citations omitted).

169. *Cf.* BIEGEL, *supra* note 106, at 313–20 (discussing code-based regulations regarding copyright infringement, noting that "issues of cost to content providers and convenience to online users had not yet been adequately addressed. But few prognosticators challenged the conventional wisdom that the inevitability of advances in this area will result in more widespread use of these services over time."). One commentator agrees that a balancing test strikes the best balance between technology and music innovators but suggests one different from that proposed by Judge Posner in the *Aimster* opinion:

> Instead of outright exoneration, distributors of such articles should gain only a rebuttable presumption of non-infringement. If plaintiffs can successfully show that current infringing uses of the product outweigh its non-infringing uses, defendants must show that measures to eliminate or reduce infringing uses would be disproportionately costly. In determining whether the cost is disproportionate, however, remedial measures that would impair non-infringing uses of the article should not be considered.

Tom Graves, Note, *Picking Up the Pieces of Grokster: A New Approach to File Sharing,* 27 HASTINGS COMM. & ENT. L.J. 137, 160 (2004). Another commentator argues for a supplement to the *Sony* "staple article of commerce" test: "[S]upplying that article should give rise to liability for contributory infringement if either the magnitude of infringing use is sufficiently large in comparison to noninfringing use, or if the evidence demonstrates that the primary purpose for the product is to facilitate direct infringement." Jesse M. Feder, *Is Betamax Obsolete?* Sony Corp. of America v. Universal City Studios, Inc. *in the Age of Napster*, 37 CREIGHTON L. REV. 859, 910 (2004). *See also* Stacey L. Dogan, *Is Napster a VCR? The Implications of* Sony *for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939, 942 (2001) (advocating a "context-specific approach to the staple article of commerce doctrine that invokes it only when necessary to protect consumers' access to markets substantially unrelated to copyright infringement").

of gatekeeping liability that had not been previously recognized in the law: code-based gatekeeping. The Seventh Circuit chose not to respect the traditional, limited gatekeeping obligations that centered on business practices.

The Seventh Circuit's test put all authors of generative technologies at risk of finding themselves on the wrong side of a court's cost/benefit balancing.[170] Indeed, they were asked to actively anticipate misuses of their products and to code to avoid them. Such gatekeeping is nice when it works, but it imposes extraordinary costs not readily captured by a single cost/benefit test in a given instance.[171] Those who code for fun might simply cease to do so in order to avoid threats of liability under such a scheme.[172] And those who code *more* generative technologies — either by designing, say, operating systems, or by building applications that are themselves recursively generative[173] — are the most at sea as to their potential liability. The more adaptable a technology, the more unpredictable its uses, and therefore the more uncertain the creator is as to her liabilities under the Seventh Circuit test. If one wants to encourage broad information technologies amenable to adaptation by diverse audiences, it may come with the price that flexible technologies can give rise to bad uses as well as good ones. The Ninth Circuit recognized the prospect that seemingly bad uses could turn out to be good, as it later articulated in *Grokster*, noting that "time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine, or an MP3 player."[174]

The Ninth Circuit's test imposed essentially no duty on software makers to preempt bad individual activities; gatekeeping duties only arose when, after the moment of infringement, a service provider was notified of the infringement and asked to act. The Seventh Circuit's

---

170. *Cf.* Jeffrey G. Knowles, *Peer-To-Peer File Sharing: The* Sony *Decision*, *in* PLI'S TENTH ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW 597, 610 (PLI Pats., Copyright, Trademarks, and Literary Prop. Course, Handbook Series No. 2909, 2004), WL 801 PLI/Pat 597 ("The [*Aimster*] court shed little light on how much non-infringing use is enough to shield a P2P operator from liability, but said that it 'is not enough . . . that a product or service be physically capable . . . of a non-infringing use.'" (citation omitted)).

171. *See* BIEGEL, *supra* note 106, at 210 ("Yet the prospective advantages of [the code-based regulation] model may in many cases be outweighed by its limitations and its potentially negative effects. The principle of unintended consequences, for example, certainly comes into play in this context.").

172. *Cf.* Jackson Lenford, *Write Free Software, Pay $203,000 to Patent Holder*, RIGHT TO CREATE, Apr. 29, 2006, http://righttocreate.blogspot.com/2006/04/write-free-software-pay-203000-to.html. *See generally* Jonathan Zittrain, *Normative Principles for Evaluating Free and Proprietary Software*, 71 U. CHI. L. REV. 265 (2004).

173. Recursively generative applications are capable of producing not only new works, but also new generative applications that can then, in turn, be used to create new art. Zittrain, *supra* note 15, at 2027–28.

174. *Id.* at 1167.

test combined preempting a range of types of infringement with pursuing individual infringements after they happened. It contemplated a broad range of sweeping preemptive design changes — analogous to requiring a VCR maker to remove the fast forward or record buttons[175] — if a cost-benefit analysis, including evidence of current uses of the technology in question, pointed the way. Just as prior restraints on speech are disfavored, so too should we view skeptically prior restraints on technology that are intended to preempt infringements that have yet to occur, especially since the activities forestalled by changes to information technologies are themselves quite frequently speech-related.[176]

VI. GATEKEEPING ON THE GRID: *GROKSTER* AS FORBEARANCE

Grokster was the natural next step beyond *Napster* and *Aimster*. Napster was ultimately shut down, and its name applied to a licensed pay service along the lines of Rhapsody or Apple's iTunes.[177] But by most credible accounts, unauthorized file sharing continued unabated, and indeed grew, on systems less vulnerable to shutdown than Napster on both a legal and a technological level.[178]

On March 13, 2000, inspired in part by Napster's legal troubles and the corresponding implications for file sharing, Justin Frankel and Tom Pepper of the small startup Nullsoft, Inc., which had recently been bought by America Online, released Gnutella to the public at large.[179] Gnutella was Napster shorn of the Napster service. It was software that one could download to a PC, run, and then use to con-

175. *See supra* note 168 and accompanying text.

176. *See* Klaus M. Schmidt & Monika Schnitzer, *Public Subsidies for Open Source? Some Economic Policy Issues of the Software Market*, 16 HARV. J.L. & TECH. 473, 476 (2003). ("For example, the Free Software Foundation ('FSF'), whose founder and most prominent speaker is MIT's Richard Stallman, argues that 'free software' is, like 'free speech,' a moral principle: 'Free software is a matter of freedom: people should be free to use software in all the ways that are socially useful.' Restricting the use of software and not sharing the source code is unethical, and the ultimate goal is 'that all published software should be free software.'") (internal citations omitted).

177. *See* Alex Goldfayn, *New System to Offer Tunes by the Month; Subscriptions Will Give Users Access to a Million Songs*, CHI. TRIB., Jan. 31, 2005, at C1 (discussing Napster.com and FYE.com's music rental business models and anticipating the announcement of new subscription models from MusicMatch and MSN Music).

178. *See* Bryan H. Choi, Note, *The Grokster Dead-End*, 19 HARV. J.L. & TECH. 393, 400–404 (2006) (describing alternative file-sharing technologies like YouSendIt and BitTorrent that are supplanting traditional P2P networks); Saul Hansell & Jeff Leeds, *A Supreme Court Showdown for File Sharing*, N.Y. TIMES, Mar. 28, 2005, at C1 ("While some surveys have suggested that file-sharing activity slowed in 2003, when the Recording Industry Association of America began to sue individual users for trading copyrighted songs, Mr. Garland [chief executive of BigChampagne] said that the number of people logging on to file-sharing networks had risen steadily [since then].").

179. *See* Patti Hartigan, *Cyberlinks: Napster is Stirring Piracy Controversy*, BOSTON GLOBE, Mar. 24, 2000, at E1.

nect over the Internet to other PCs running Gnutella. Once connected, one could search across multiple Gnutella users for files to trade — a sort of bucket-brigade exchange that, like Internet packet routing itself, required no central coordination.

Citing legal concerns, America Online withdrew the program the next day, but within a week, Gnutella had been reverse-engineered and a number of copycat and derivative Gnutella emulations were available and running.[180] Some primarily used the protocols that Frankel and Pepper had conceived for Gnutella, allowing users of different PC applications written by different people to join the same virtual network of "Gnutella" users.[181] Others created similar distributed networks, but ones that were incompatible with Gnutella clients. In March 2001, a Dutch company called Kazaa BV created a competing technology called FastTrack, and then sought to license developers to write compatible PC software that would be able to connect to other computers also using FastTrack technology. Grokster was one of these applications, and its creators (along with Kazaa BV) were sued for copyright infringement by the music publishers that October.[182]

Both Napster and Aimster had run services, and in doing so, could fairly be asked to take some steps to eliminate piracy as they were alerted to specific instances of it. But according to *Napster*, at least, if these companies were no longer running services, and only distributing products capable of substantial noninfringing uses, the analysis would be over and the defendants should prevail — even if the products used the Internet to create their own "service" among users.[183] Demonstrating "actual" infringements to the defendants and demanding action would be like showing Sony instances of its VCR being misused in homes at a point when it was too late to realistically ask Sony to do anything about it, unless one were asking for the kind of preemption in product design that *Sony* eschewed.

---

180. AOL had recently merged with Time-Warner, a member of the Recording Industry Association of America. *Id.* Nullsoft asserted that Gnutella was an "unauthorized free-lance project" of its Winamp programming team. *Program for Sharing of MP3 Files Cut from AOL Website*, WALL ST. J., Mar. 16, 2000, at A10.

181. *See, e.g.*, LimeWire, http://www.limewire.com/english/content/home.shtml (last visited Apr. 29, 2006); Free Peers, Inc., BearShare, http://www.freepeers.com/products.htm (last visited Apr. 29, 2006); Press Release, Free Peers, Inc., BearShare Gnutella Client for Windows (Dec. 4, 2000), http://groups-beta.google.com/group/alt.gnutella/msg/acbe651770f2f47; Slyck's Guide to Gnutella, http://www.slyck.com/gnutella.php (last visited Apr. 29, 2006).

182. *See* Complaint for Damages & Injunctive Relief for Copyright Infringement, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd. (*Grokster I*), 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764 (2005) (No. CV 01-08541 SVW), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20011002_mgm_v_grokster_complaint.pdf.

183. *See supra* text accompanying notes 136, 149.

True to *Napster*, the *Grokster* district court found in favor of the defendants, and the Ninth Circuit affirmed.[184] Grokster was a product, not a service, and *Sony* precluded banning it or insisting that it be designed to preemptively eliminate piracy.[185] While some of the defendants had commercial websites to distribute and advertise their wares, as well as ongoing business models that inserted advertisements directly into the FastTrack-compatible software, the software was coded so as not to require assistance from a central server to function. Constructive knowledge at the design stage could not be imputed thanks to a *Sony* defense, and actual knowledge of specific infringements was only possible once the software had been released and the makers were no longer in a position to materially contribute to the infringement.

Had *Grokster* appeared before the Seventh Circuit, its posture before the Supreme Court might have been significantly different. The *Aimster* balancing test likely would have made a finding in Grokster's favor a much closer call. As the Ninth Circuit observed in a footnote, the *Grokster* defendants were much more effective than the *Aimster* defendants in showing noninfringing uses of the system.[186] Grokster introduced evidence that its software had been enlisted to transmit public domain works, including texts, films, and copyrighted but authorized works such as an album by the band Wilco.[187] However, passing the "capable of substantial noninfringing uses" threshold would not have served as an absolute shield against infringement liability under *Aimster*. Grokster's noninfringing uses would have been balanced against the costs of designing and engineering the software in a different way to preemptively preclude some or all infringement.[188]

When the Supreme Court granted certiorari[189] in *Grokster,* in part to resolve the circuit split between the Ninth Circuit and Seventh Circuit approaches,[190] the stakes in *Grokster* were not limited to which circuit had properly interpreted *Sony*. *Grokster* was an opportunity for the Supreme Court to consider imposing an affirmative duty on software makers like the *Grokster* defendants, and makers of generative

184. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd. (*Grokster II*), 380 F.3d 1154, 1157 (9th Cir. 2004), *vacated* 125 S. Ct. 2764 (2005).

185. *See id.* at 1161.

186. *See id.* at 1162 n.9.

187. *Id.* at 1161–62. Wilco used Grokster to disseminate music and subsequently leveraged its popularity to secure a recording contract. *Id.*

188. *See supra* note 166 and accompanying text.

189. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. (*Grokster Certiorari*), 543 U.S. 1032 (2004).

190. Petition for a Writ of Certiorari at 24–29, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 543 U.S. 1032 (2004) (No. 04-480), 2004 WL 2289200, *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20041008_Grokster_final_petition.pdf.

technologies in general, to serve as gatekeepers. An *Aimster*-like balancing test would force product makers and service providers to preemptively design their offerings to prevent them from being used by bad apples. Fearing that they would fall on the wrong side of such a balancing test, technology providers likely would slow or stop creating generative — and liability-exposing — innovations. The Supreme Court wisely did not take such a landmark step.

Although the Supreme Court unanimously reversed the Ninth Circuit's grant of summary judgment in favor of the *Grokster* defendants, it did so in a way that had little practical effect, and that took no significant step toward curtailing Internet generativity. To be sure, the Supreme Court held that the Ninth Circuit had misapplied *Sony's* "capable of commercially significant noninfringing uses" test.[191] The *Sony* test was found to preclude imputing culpable intent solely based on the "characteristics or uses of a distributed product" or knowledge that the product may be used for infringing purposes.[192] However, intent to infringe could be demonstrated through other extrinsic evidence.[193]

In reversing the Ninth Circuit's decision, the Supreme Court adopted the common law doctrine of inducement as a "sensible one for copyright [law]," 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."[194] Neither knowledge of actual infringing uses — let alone potential infringing uses — nor ordinary business activity such as providing customer support or product updates would subject a distributor to liability in and of itself.[195] "Purposeful, culpable expression and conduct" would be necessary to impose liability under the new inducement rule.[196]

The Court's inducement standard resembles the Food and Drug Administration's policy of looking at how a product or service is marketed and packaged to determine liability. Under FDA rules, a drug company could run into trouble for advertising a drug for a non-approved use, even if it may sell the very same drug for other uses.[197]

---

191. *Grokster III*, 125 S. Ct. 2764, 2778 (2005).
192. *Id.* at 2779.
193. *See id.*
194. *Id.* at 2780.
195. *Id.*
196. *Id.*
197. This type of advertising is referred to as "off-label marketing." Off-label prescriptions account for almost 40 percent of all prescriptions written each year. Daniel Costello, *When Drugs are Used Off-Label*, L.A. TIMES, June 7, 2004, at F1. *See generally* Matthew Herper, *When Doctors Go Off Label*, FORBES.COM, Oct. 5, 2004, http://www.forbes.com/home/sciencesandmedicine/2004/10/05/cx_mh_1005genentech.html. This has caused prob-

Or, a non-drug company could run into trouble if it marketed chicken soup to cure colds, even if it turned out that chicken soup did so. If, after *Sony,* Sony, Inc., were to market a VCR called the "Pirate Box" and tout it using ads that showed people recording pay-per-view programs and selling them to others the next day, it may be found liable for contributory infringement without doing violence to the principles underlying the *Sony* standard, and we need not be troubled by that loss.[198] Lurking in both *Napster* and *Aimster* was the fact that the services in question were so clearly aimed at profiting from the swapping of copyrighted files. Noninfringing uses were truly incidental from the point of view of the service creators and maintainers, making these cases easier to decide. By confining a finding of liability in *Grokster* to its packaging and marketing as a pirate's dream, the Supreme Court allowed those who marketed technologies in more generic ways to remain free of liability, as they should. This was similar to the apparent mechanism of the INDUCE Act introduced in the 108th Congress that would have penalized those who "intentionally" aided infringement, with intent based upon "all relevant information about such acts then reasonably available to the actor, including whether the activity relies on infringement for its commercial viability."[199]

The Supreme Court viewed these successors to Napster as continuing a socially undesirable practice of facilitating flagrant infringements in public view.[200] The Court rightly found that there was evidence of the *Grokster* defendants' intent to induce infringement that extended beyond the design of the product and the knowledge that it could be used for infringing purposes. The cited evidence included the "internal communications and advertising designs" that were targeted at Napster users, the lack of any filtering tools or other preemptive features to curtail infringement, and the financial incentives from selling ads as part of the software.[201] Based on this evi-

---

lems with advertising drugs on the Internet, since drugs may have different approved uses in different countries. Short of emerging technologies that help OSPs determine the country of origin of a web surfer, companies have had minor dilemmas about how to geographically segment their online advertising to suit different regulatory regimes.

198. Recall that Sony's instruction booklet contained the admonition: "Television programs, films, videotapes and other materials may be copyrighted. Unauthorized recording of such material may be contrary to the provisions of the United States copyright laws." Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 426 (1984); *see supra* note 134.

199. Inducing Infringements of Copyrights Act of 2004, S. 2560, 108th Cong. (2004).

200. It is unclear whether the Supreme Court ever considered the emerging evidence that CD sales have, counterintuitively, not been unduly impacted by online file-sharing. *See US Sees Growth in CD Sales Market*, BBC NEWS, Jan. 6, 2005, http://news.bbc.co.uk/2/hi/entertainment/4150747.stm. *But see* Stan J. Liebowitz, *Will MP3 Downloads Annihilate the Record Industry? The Evidence So Far*, 15 ADVANCES STUDY ENTREPRENEURSHIP, INNOVATION, & ECON. GROWTH 229 (June 2003) (suggesting that MP3 downloads decrease sales but not necessarily enough to be fatal to the industry).

201. *Grokster III*, 125 S. Ct. 2764, 2781–82 (2005).

dence, the Court declared that the "unlawful objective is unmistakable."[202]

In the wake of *Grokster*, even software makers without good lawyers will know not to tout the copyright-infringing uses of their generic tools. But the tools themselves seem to have remained largely, if not entirely, protected by *Sony* — so long as they are not wrapped in inducing rhetoric. To be sure, Grokster's own website exhorted users not to infringe copyright, and was otherwise crafted to emphasize valuable uses: "Transform Grokster into a powerful, no cost distribution platform for authors and artists all over the world. Investigative journalists, dissenting activists, and uncompromising creators can take advantage of the fastest growing medium on the planet."[203] But these demonstrations indeed seemed pretextual when juxtaposed with other marketing efforts touting Grokster's ability to direct users to the most popular files, which were often unauthorized copies of copyrighted music.[204] Jane Ginsburg sees *Grokster's* inducement standard as slightly stronger, speculating that a device that "facilitates infringement on a massive scale" can be found inducing under *Grokster* for that alone,[205] but the *Grokster* Court seemed not to go that far. It pointed to a failure to put mechanisms in place to filter out infringing content as "underscoring" Grokster's intentional facilitation of copyright infringement, but then quickly added that such a failure could not be the sole basis for liability.[206]

The practical consequences of the Supreme Court's *Grokster* decision in stemming actual infringement are thus negligible. Grokster as a commercial enterprise and some other similar services have closed their doors,[207] but the demise of Grokster as a firm or as a website has not affected the functionality of its software or the overlay network created by the software. File sharers can continue to use the Grokster software to find and trade music; they simply cannot send friends to Grokster.com to obtain additional copies of the client software. Software with near-identical functionality is available else-

202. *Id.* at 2782.

203. Internet Archive, Grokster, http://web.archive.org/web/20040523211147/http://grokster.com/ (May 23, 2004).

204. *See Grokster III*, at 2774 (noting that "Grokster sent users a newsletter promoting its ability to provide particular, popular copyrighted materials").

205. Jane C. Ginsburg & Sam Ricketson, *Inducers and Authorisers: A Comparison of the US Supreme Court's* Grokster *Decision and the Australian Federal Court's* KaZaa *Ruling*, 11 MEDIA & ARTS L. REV. 1, 7 (2006), *available at* http://ssrn.com/abstract=888928.

206. *Grokster III*, at 2781 & n.12.

207. *See* Grokster, http://www.grokster.com/ (last visited Apr. 29, 2006); *see also* Andrew Orlowski, *Grokster Closes, Goes Legal*, THE REGISTER, Nov. 8, 2005, http://www.theregister.co.uk/2005/11/08/grokster_closes/; Andrew Orlowski, *WinMX and eDonkey: Offline, Doors Closed*, THE REGISTER, Sept. 22, 2005, http://www.theregister.co.uk/2005/09/22/p2p_networks_darken/.

where,[208] and under *Grokster*, releasing such software will likely be found permissible so long as its marketing does not invite copyright infringement. The presence of software authors willing to code and release file-sharing software without any business model at all suggests that this software will continue to exist even if it cannot be marketed formally, much less marketed as a pirate's tool. Software capable of piracy can simply be developed by anonymous amateurs and released onto the Net for general use. The true authors might never be found, and if found, would likely be judgment-proof; in any case, the fruits of their labor would still exist on the Net. While less-than-perfect enforcement is no reason not to apply a wise law where otherwise possible, the ability of underground software to spread overnight undermines most valid applications of *Grokster*'s new inducement rule.

If *Grokster*'s inducement standard were applied too broadly, the resulting software production landscape would be one that metaphorically lacks a middle class. Big software companies could negotiate deals with publishers, or could afford to defend their activities right to the line of legal permissibility; hit-and-run individual coders could write software that ignores the legal line with impunity, so long as they did not need to anchor the software to an ongoing service. Those in the middle — wanting to be law-abiding but lacking the resources to either preempt or contest legal liability — would be the ones frozen out.

Consider LOCKSS, a peer-to-peer system designed for libraries to retain documents for thousands of years and to determine whether a digital copy of a document remains authoritative.[209] The designers of LOCKSS (and their risk-averse academic sponsors) simply would not want to risk a finding that they were intentionally aiding infringers, especially if the publishers were allowed to present "reasonable alternative design" evidence, as in products liability cases,[210] to show that the makers of LOCKSS could have included content or other policing filters and still accomplished most of what they intended. Although makers of physical products have their design decisions routinely second-guessed through products liability cases, the underlying rationales for strict products liability are not persuasive here.[211] Risk-spreading

208. *See, e.g.*, Slyck's Database of File Sharing Programs, http://www.slyck.com/programs.php (last visited Apr. 29, 2006).

209. *See* About LOCKSS, http://lockss.stanford.edu/about/about.htm (last visited Apr. 29, 2006). LOCKSS is an acronym for "Lots Of Copies Keep Stuff Safe." *Id.*

210. *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (1998).

211. *See* Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 440–41 (Cal. 1944) (Traynor, J., concurring).

> [P]ublic policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market. It is evident that the manufac-

can actually work in the opposite direction. Here, a single programmer could be asked to bear the risk of an entire industry's piracy, rather than a powerful company assuming the risk of many small individual injuries corresponding to the number of product units sold. With copyright infringement, no imperative of physical injury calls for judicial intervention.

The right application of *Grokster* will make only the slightest adjustment from *Sony* and continue to accord providers of software products with broad immunity from the misuse of their products, and providers of digital services with only modest gatekeeping liability in keeping with Kraakman's framework.[212]

With the advent of fully distributed peer-to-peer networks that will exist anyway in the post-*Grokster* climate, what will publishers do next? One wishes for the re-laying of flagstones suggested at the very beginning of this Article. Ideas like those of William Fisher[213] and Neil Netanel[214] for alternative compensation schemes could accomplish this goal. Such schemes propose collecting blanket taxes on overall instrumentalities, like ISP services or computer purchases, and directing these funds to creators and publishers in proportion to the popularity of their intellectual fruits. Downloading and sharing would become a blessing rather than a curse, since it would demonstrate popularity and thus win more of the pie for a content creator. Whatever the merits of such a system — and there is of course spirited debate about it — it is not likely that the publishers or the regulators they lobby will soon embrace it. More likely, the publishers will continue to provide comparatively cheap, but still profitable, authorized media through such services as the iTunes music store or monthly subscription services, and many consumers will choose to pay a small fee per download or per month, or watch interspersed streaming ad-

> turer can anticipate some hazards and guard against the recurrence of others, as the public cannot. . . . The cost of an injury and the loss of time or health may be an overwhelming misfortune to the person injured, and a needless one, for the risk of injury can be insured by the manufacturer and distributed among the public as a cost of doing business. . . . [I]t is to the public interest to place the responsibility for whatever injury [such defective products] may cause upon the manufacturer, who, even if he is not negligent in the manufacture of the product, is responsible for its reaching the market.

Id.

212. *See supra* text accompanying notes 30–33. *See generally* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable* (July 2004) (John M. Olin Law & Economics Working Paper No. 217, on file with University of Chicago Law School), *available at* http://www.law.uchicago.edu/Lawecon/WkngPprs_201-25/217-dgl-eap-isp.pdf (arguing that ISPs should be held accountable when their users originate or disseminate malicious Internet code that allows other users to co-opt individual computers).

213. *See* FISHER, *supra* note 110, at ch. 6.

214. *See* Neil W. Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003).

vertisements, rather than undertake the effort to obtain the files for free through a pirate network — especially if there is some prospect of individual liability.

In the medium term, we are likely to see four continuing strategies by publishers. First, direct lawsuits against file swappers will place further pressure on individuals to cease mass infringing activities, since such activity is motivated only by weak altruism to faceless strangers, or by a failure to appreciate or change the default settings in peer-to-peer software. Second, contributory infringement claims will bring increased pressure on ISPs, the only remaining gatekeeper, to terminate their subscribers' Internet access when the ISPs are notified of active file-sharing. Third, self-help efforts by publishers will continue to disrupt public file-sharing networks, such as flooding of networks with decoy files to frustrate searches for particular songs, and so-called interdiction, whereby publishers' computers establish runaway demand for users' shared files so as to fill up the sharer's queue and deny downloads to other users. Fourth, new business models will provide consumers convenient access to content they like and may not have known about otherwise, including the aggregation of content generated by the consumers themselves rather than by professional authors and creators. Juxtaposed with these strategies are two wild cards discussed in the next section: the rise of generic overlay networks, and the amenability of today's PC/Internet grid to regulation of PC software after the software is in users' hands.

VII. THE END OF REGULATORY FORBEARANCE?: FROM KRAAKMAN'S GATEKEEPERS TO LESSIG'S GATEKEEPERS

Ideally, *Grokster* might simply have affirmed the Ninth Circuit's holding below without adding an inducement counterpart to *Sony*. Such a decision would have categorically avoided the possibility of unduly chilling technology development through any future overbroad applications of the inducement standard, at the expense of allowing bad actors like Grokster Ltd. to continue in business, or of provoking Congress to actions that might depart even further from *Sony*'s balance. As it stands, *Grokster* still inherits *Sony*'s wisdom because its inducement theory seems limited enough to rarely offer a path to gatekeeper liability. *Grokster* is therefore well-decided precisely because it is not landmark.

What, then, will be the next battleground if publishers are not able to find accommodation with the problem of piracy through alternative compensation schemes or more limited digital music store schemes like iTunes and Rhapsody? Two phenomena are pulling the tug-of-war in opposite directions. Working against publishers is the rise of new "overlay networks." Internet-aware PC applications are continu-

ing to evolve, and their next step will extend the problems of *Grokster* itself, where a legal win for the industry did not provide any actual way to shut down the Grokster software already running on individual machines. Academic projects like LOCKSS[215] and Publius,[216] and more pedestrian counterparts such as FreeNet,[217] BitTorrent,[218] and eXeem,[219] are helping to create a grid. Files can be stored in bits and pieces on PCs all across the Internet, typically without the PC owners themselves knowing what fragments they hold. The result is a collective hard drive for humanity, accessible by anyone but run by no one: one whose contents cannot be edited piece by piece and can only be degraded through the crude destruction of individual nodes that have volunteered to host such a configuration. A project by which users can lend their spare disk space and processing power to the rest of the world is the apotheosis of generativity and of disruption. It is the embodiment of the "Libertarian gotcha" that James Boyle properly deemed illusory during the mid-1990s: the idea that if a sovereign allows Internet access within its borders, it cannot easily pick and choose which uses to allow and which to deny.[220]

While the development of such grids points to a possible checkmate against the publishers, Internet applications are not the only moving pieces to the puzzle of the Internet's future. The PC, too, is evolving, as is the underlying network, in a way that tilts in favor of regulability. I have written elsewhere that fundamental, discontinuous changes are being wreaked upon the Internet of the 1990s by the makers of information technology: the PC and OS manufacturers, mainstream software authors, and the public interest Internet engineering establishment.[221] These changes stand to invert many of the possibilities described here, allowing for far greater, rather than lesser, gatekeeping control.

So long as code has any generative quality — such as the standard PC operating system that allows third parties to write new software to run on it, or a word processor that allows the composition of the Communist Manifesto as easily as the Declaration of Independence — anticipating ex ante, and building effective barriers against, its misuse will not be easy. Like a child leaving home, the code is first

215. LOCKSS, http://lockss.stanford.edu/ (last visited Apr. 29, 2006); *see also supra* note 209 and accompanying text.

216. Publius Censorship Resistant Publishing System, http://www.cs.nyu.edu/~waldman/publius/ (last visited Apr. 29, 2006).

217. The FreeNet Project, http://freenet.sourceforge.net/ (last visited Apr. 29, 2006).

218. BitTorrent, http://www.bittorrent.com/ (last visited Apr. 29, 2006).

219. *See* Wikipedia, *EXeem*, http://en.wikipedia.org/wiki/EXeem (as of Mar. 10, 2006, 04:54 GMT).

220. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997). *But see* OpenNet Initiative, Case Studies, http://www.opennet.net/ (follow "Case Studies" hyperlink) (last visited Apr. 29, 2006).

221. *See generally* Zittrain, *supra* note 15.

nurtured by its author and then set free to find its life in a larger community. The notion of a distinct phase between the design of code and its broader use and misuse has helped us understand the regulatory forbearance in a decision like *Sony*, which permitted the manufacture of VCRs despite the fact that those recorders could be — and indeed, were, in many instances — used to infringe copyright. The identification of substantial noninfringing uses for the recorders meant they were permissible to distribute, since a ban on distribution would preclude lawful uses as well as unlawful ones. Similarly, in *Grokster*, the code was not to be judged standing alone, but rather by the actions of those who packaged and promoted it. This suggests most code cannot of itself easily be labeled contraband unless it flunks *Sony*'s generous test; only the activity surrounding its promotion can give rise to liability.

However, the rise of always-on, broadband-connected PCs means that software or operating systems need not follow a factory-produces, consumer-inherits sequence. Software can become service,[222] tuned and re-tuned near-instantly by its author, like a child who leaves home but finds the parents not only constantly in touch, but able to set and adjust curfews from afar. Software can now be routinely written to maintain contact with its source: first, to receive updates to functionality, but second, to implement new regulatory mandates. Security software vendors, and operating system makers now undertaking proactive security functions, are not only able to update their own software, but also to affect how other software on the same PC runs — in particular, to disable it should it be deemed a threat.[223] This functionality would enable regulators to insist to a software maker, or alternatively to an operating system vendor, that a given piece of software be disabled or modified to meet regulatory requirements. These are Lessig's gatekeepers, rather than Kraakman's,[224] and a landmark regulatory move will be one that decides under what circumstances they should be enlisted.

How should we think about this possibility? Our look at previous regulatory forbearance on and off the Net offers reasons why ease of regulation should not necessarily prompt it. From the early, simpler configurations of defamation and copyright infringement, we saw courts and Congress ultimately unwilling to ask intermediaries to do more than opportunistic gatekeeping of wrongs in which they were directly involved, or to which they were close enough to efficiently judge and moderate. Demands for intervention did not extend to the creation of new technology architectures. Only when providers were already monitoring, or able to monitor, for their own purposes did

222. *See id.* at 47.
223. *Id.* at 46–48.
224. *See supra* text accompanying notes 7–14.

regulators look to tack on additional obligations — as with Prodigy's decision to screen its message boards, or Napster's decision to offer a centralized directory of file names it could screen and subscribers whose access it could terminate. Similarly, software authors who decide not to implement automatic update functionality in their code should not be required to do so for the sake of future regulability.[225]

The same forbearance should also apply to antivirus and operating system makers who decide to implement functionality allowing updates to their own code and modification of others' code. Suppose a publisher fully litigated the ongoing misuses of a particular piece of software and suggested an alternative way to write it that would preclude its bad uses. Instead of going after the code's author — thereby respecting the author's choice not to embed a way to implement future changes to her code — the publisher could instead seek an order against operating system makers and security vendors to disable the bad code on PCs that receive updates from them. This might appear to be precisely the kind of regulatory piggybacking that the history of online gatekeeping has permitted — and *Grokster* is silent on the issue.

Such gatekeeping should be disfavored. Piggybacking on automatic update functionality might cause consumers to gravitate away from software carrying such functionality once they saw their PCs' behavior modified by government fiat in undesirable or unexpected ways. More fundamentally, such gatekeeping is *too* powerful, permitting short-term regulatory panic to be translated too readily into long-term limitations. Lessig has pointed out that open code — code that programmers can alter and redistribute without undue legal or technical barriers — is harder to regulate than closed code.[226] He lauds that quality as a way of enabling a fundamental check on government's power, and obliquely suggests that check as a good one: "Just as our Constitution embeds the values of the Bill of Rights while also embedding the protections of separation of powers, so too should we think about the values that cyberspace embeds, as well as its structure."[227] Here the fulcrum of control is not open versus closed code. Indeed, open code may actually be more readily modifiable for control purposes than closed code, since its recipe is available to a regulator, necessitating comparatively less cooperation from its authors to change the way it works. Further, security software that has been given orders to eliminate contraband code running on its PC can carry out its task on both open and closed code. However, Lessig's core

225. *See* Zittrain, *supra* note 15, at 49–51.

226. *See* Lessig, *Limits in Open Code*, *supra* note 12, at 764–69 (1999); *cf.* Zittrain, *supra* note 172, at 285–87 (discussing possible explanations for a litigation differential between free software and proprietary software).

227. Lessig, *Limits in Open Code*, *supra* note 12, at 769.

suggestion retains its power: we might prefer a world in which regulation of code is not easy. Ease of implementing a particular regulation is one reason to favor such regulation, but it should not be the overriding one.

VIII. CONCLUSION

The *Grokster* case fits well within a ten-year pattern of forbearance in American legislative and judicial activity that has been appropriately willing to abstain from major intervention in the private development of information technology. This forbearance may soon be put to its most difficult test, as the mechanisms for invasion of legally protected interests defy minor corrective interventions at traditional online points of control,[228] even as they become unusually amenable to a major new one through remote tuning of already-distributed PC software.

The prospect of software as service permits a major regulatory intrusion to be implemented as a technically minor adjustment to code. The history of online gatekeeping is partly one of the exercise of raw political power by intermediaries to limit their responsibilities. But it is also one of policy judgment in the judicial as well as legislative spheres that generative technologies ought to be given wide latitude to find a variety of uses — including ones that encroach upon other interests. These encroachments may be undesirable individually, but particularly in the realm of malum prohibitum wrongs such as those associated with the American intellectual property system — a system primarily conceived to maximize creative output rather than to vindicate moral rights of authors and publishers[229] — they may also point to opportunities to reconceptualize the rights underlying the markets and the business models based upon them. An information technology environment capable of recursive innovation in the realms of business, art, and culture will best thrive with continued regulatory forbearance, carrying forward *CompuServe*, *Sony*, and *Grokster's* insight, applied across very different respective facts, that the disruption occasioned by generative information technology often amounts to a long-term gain even if it causes short-term threat to some powerful and legitimate interests.

228. *See generally* Zittrain, *supra* note 55, at 655–73.
229. *See* Sprigman, *supra* note 128, at 522.