ARTICLES

REDUCING DIGITAL COPYRIGHT INFRINGEMENT WITHOUT RESTRICTING INNOVATION

Mark A. Lemley* & R. Anthony Reese**

* Elizabeth Josslyn Boalt Chair in Law, Boalt Hall, University of California at Berkeley; of counsel, Keker & Van Nest LLP.

** Thomas W. Gregory Professor of Law, University of Texas School of Law; special counsel, Morrison & Foerster LLP.

Thanks to Jean Camp, Lorrie Cranor, Stacey Dogan, Terry Fisher, Paul Geller, Paul Goldstein, Rose Hagan, Raymond Ku, Doug Laycock, Christopher Leslie, Doug Lichtman, Lydia Loren, Glynn Lunney, Michael Madison, David McGowan, Neil Netanel, David Nimmer, Michael Page, Gigi Sohn, Peter Swire, Ragesh Tangri, Rebecca Tushnet, Fred Yen, and attendees at a lecture at Santa Clara University School of Law, a conference at Cardozo Law School, a panel at the Computers, Freedom and Privacy conference, and workshops at the University of North Carolina and Thomas Jefferson School of Law for comments on the ideas in this Article.

Keker & Van Nest represents a number of innovators currently involved in litigation adverse to the content industries, including some of the parties in cases discussed in this Article. Morrison & Foerster represents or has represented a number of companies involved in litigation alleging indirect liability of innovators, including some of the parties in cases discussed in this Article. Thus, we wish to make it even more clear than usual that our opinions are our own, do not represent those of our firms or our clients, and are not based on confidential information obtained in any representation.

INTRODUCTION

Suing actual infringers is becoming passé in digital copyright law. In the digital environment, the real stakes so far have been in suing those who facilitate infringement by others. Copyright owners tend not to sue those who trade software, video, or music files over the Internet. Indeed, such claims are so rare that the Recording Industry Association of America's (RIAA) recent suits against some actual infringers on peer-to-peer (p2p) networks sent shock waves through the legal community. Instead, copyright owners have mostly sued direct facilitators like Napster;[1] makers of software that can be used to share files;[2] those who provide tools to crack encryption that protects copyrighted works,[3] providers of search engines that help people find infringing material;[4] "quasi internet service providers" such as universities,[5]

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

2. *See In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

3. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); 321 Studios v. Metro-Goldwyn-Mayer Studios, No. C 02-1955 SI, 2004 U.S. Dist. LEXIS 2771 (N.D. Cal. Feb. 19, 2004); Real Networks v. Streambox, No. 2:99CV02070, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000); *cf.* United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (involving criminal rather than civil claims against provider of software tools).

4. *See* Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003). *Kelly* included claims of direct as well as contributory infringement, but they were both asserted against the search engine that made the pictures accessible, not against the end user who sought to download

eBay, and Yahoo! Auction;[6] and even credit card companies that help individuals pay for infringing activity.[7]

Most of these suits rely on theories of secondary liability, focusing on those who provide services or write software that can be used in an act of infringement.[8] In addition, some recent suits appear to be based on a new theory that might be called "tertiary" liability that seeks to reach those who help the helpers. Cases in this vein include lawsuits filed against those who help others crack encryption, for example by providing links to software that can be used to crack encryption,[9] the copyright lawsuit against backbone providers for providing the wires on which copyrighted material flows,[10] the claims filed against the venture capital firm of Hummer Winblad for its role in funding Napster,[11] and (with an unusual twist) the malpractice suit against the law firm of Cooley Godward for advising mp3.com that it could assert defenses to copyright infringement.[12] The anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) provide by statute for one particular type of tertiary liability (for providing tools that circumvent encryption protecting a copyrighted work and that help another get access to a copyrighted work in order to infringe that copyright),[13] and there have even been suggestions that there should be a claim for contributory violation of the DMCA's anticircumvention provisions, which should perhaps be termed quaternary liability for copyright infringement.[14]

---

them.

5. *See MPAA Warns University of Possible Legal Action over Alleged Copyright Infringement*, 9 ELEC. COMM. & L. (BNA) 105 (Feb. 4, 2004).

6. *See* Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal. 2001); Elec. Arts v. Yahoo! (N.D. Cal. filed Mar. 2000).

7. Adam Tanner, *U.S. Sex Site Sues Credit Cards over Pirated Erotica*, *at* http://in.tech.yahoo.com/040129/137/2b6qc.html (last visited Mar. 16, 2004).

8. Secondary liability includes liability for both vicarious and contributory infringement. See *infra* notes 343-46 and accompanying text for a discussion of the legal standards for secondary liability.

9. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (finding liability for linking to websites that post tools that can be used to crack encryption in order to copy copyrighted works).

10. Arista Records v. AT&T Broadband (S.D.N.Y. filed Aug. 16, 2002); *see also* CNET NEWS.COM, *Microsoft Unveils New CD Copyright Protection*, Jan. 8, 2003, *available at* http://news.com.com/2100-1023-981279.html (last visited Apr. 10, 2004) (quoting the head of the RIAA as saying broadband providers should be liable because copyright infringement increases the demand for broadband Internet service).

11. *See, e.g.*, Universal v. Hummer Winblad (C.D. Cal. filed Apr. 21, 2003); Amy Harmon, *Universal Sues Bertelsmann over Ties to Napster*, N.Y. TIMES, May 13, 2003, at C6 (reporting that Universal's suit against Bertelsmann asserted vicarious liability for control over a firm that was itself found guilty of vicarious liability).

12. mp3.com v. Cooley Godward, No. CV806837 (Cal. Super. Ct. filed Jan. 18, 2001).

13. 17 U.S.C. § 1201 (2004); *Corley*, 273 F.3d 429.

14. *See, e.g.*, Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users'*

Further, a number of doctrines that were designed to protect these secondary and tertiary "facilitators"—the "safe harbor" for online service providers,[15] the restrictive standard for contributory copyright infringement for equipment providers announced by the Supreme Court in the *Sony* Betamax case,[16] and the requirement that vicarious infringement be limited to cases of direct financial benefit[17]—are under attack. Recent court decisions undo some of the benefit of Section 512's protection for Internet service providers (ISPs),[18] which in any event are not particularly suited to limit secondary liability for p2p providers. *Napster* and *Aimster* rewrite the rule of *Sony* in a way that significantly limits its application.[19] Both *Napster* and *Fonovisa* have all but eliminated the requirement of *direct* financial benefit in vicarious infringement.[20] And proposed legislation would go even further in regulating the behavior of those who do not themselves infringe, injecting Congressional oversight into how software and consumer electronics are built[21] and permitting content owners to unleash destructive hacks of computer networks

and Content Providers' Rights, 49 J. COPYRIGHT SOC'Y U.S.A. 277 (2001) (arguing that the *Elcom* prosecution involved such a claim because of the government's reliance on aiding and abetting liability and criticizing this approach); *cf.* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095 (2003) (noting the potential for litigants to expand the DMCA beyond its scope).

15. 17 U.S.C. § 512 (2004).

16. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

17. *See, e.g.*, Religious Tech. Ctr. v. Netcom On-line Communication Servs., Inc., 907 F. Supp. 1361, 1376 (N.D. Cal. 1995); Artists Music, Inc. v. Reed Publ'g (U.S.A.), Inc., No. CIV.A. 93-3428-JFK, 1994 WL 191643, at *6 (S.D.N.Y. May 17, 1994); Roy Export Co. Establishment v. Trs. of Columbia Univ., 344 F. Supp. 1350, 1353 (S.D.N.Y. 1972); Kelly Tickle, *The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards*, 80 IOWA L. REV. 391, 415 (1995).

18. *See, e.g.*, ALS Scan, Inc. v. RemarQ Cmtys., 239 F.3d 619 (4th Cir. 2001); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002) (misreading Section 512 of the Copyright Act to permit ISP liability based only on generalized knowledge of infringing activity). Jonathan Band and Matthew Schruers note the irony that the Communications Decency Act, which wasn't really designed to protect Internet service providers, has been interpreted to provide them with far more protection than the DMCA safe harbors, which were designed with that aim in mind. Jonathan Band & Matthew Schruers, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L.J. 295, 295 (2002).

19. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003) (rejecting the Ninth Circuit's restrictive interpretation of *Sony* but adopting its own restrictive interpretation). For a fuller discussion, see *infra* notes 42-64 and accompanying text.

20. *See generally Napster*, 239 F.3d 1004; Fonovisa v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996). For a fuller discussion, see *infra* notes 83-87 and accompanying text.

21. Consumer Broadband and Digital Television Protection Act, S. 2048, 107th Cong. (2d Sess. 2002). Congress already slipped one similar provision into the labyrinthine Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(k) (2004) (requiring analog VCRs to have copy control technologies built into them). For criticism of these approaches, see Stacey L. Dogan, *Code Versus the Common Law*, 2 J. TELECOMM. & HIGH TECH. L. 73, 75 (2003).

without fear of liability.[22]

There is of course a good reason copyright owners are suing facilitators. They see themselves as under threat from a flood of cheap, easy copies and a dramatic increase in the number of people who can make those copies. The high volume of illegal uses, and the low return to suing any one individual, make it more cost-effective to aim litigation at targets as far up the chain as possible. From the perspective of the music industry, it was easier and more effective to shut down Napster than to sue the millions of people who illegally traded files on Napster. So far, the courts have been largely willing to go along, shutting down a number of innovative services in the digital music realm. At least one district court refused to ban the provision of p2p software by StreamCast and Grokster, prompting the recording industry to reluctantly begin bringing some suits against users of p2p software and to start selling music online in earnest.[23] But copyright owners are vigorously appealing the decision in favor of the software providers, seeking to convince the Ninth Circuit to hold the software companies liable and thereby eliminate the need to pursue individual infringers.

In this Article, we focus on one strand of these cases against those who allegedly facilitate copyright infringement—those dealing with distribution of digital content over p2p networks. Unrestricted liability for anyone who is in any way involved with such copyright infringement is a bad idea. Indirect liability is a continuum in which acts most closely related to infringement and with the fewest affirmative benefits are the easiest to condemn. Napster was relatively easy to condemn because the service was limited to trading music files and virtually all of the files actually traded at the time of the suit were traded illegally. The *Grokster* case is a substantial step further removed from infringement, both because the defendants' involvement is less (indeed, resellers like Grokster are arguably merely conduits for providing software, an activity which should be legal under most circumstances)[24] and because the actual noninfringing uses of Kazaa and similar software involved in the case are greater. Lawsuits against Internet service providers, search engines, telephone companies, and other indirect providers, while not the focus of our attention here, are even more problematic because of the many legal uses of these services. The key policy point is that going after makers of technology for the uses to which their technologies may be put threatens to stifle innovation. Similarly, going after necessary third parties like investors and law firms will stifle investment in innovation. The fundamental difficulty is that while courts

22. *See* H.R. 5211, 107th Cong. (2d Sess. 2002).

23. *See, e.g.*, Benny Evangelista, *Online Music Finally Starts to Rock 'n' Roll*, S.F. CHRON., Dec. 29, 2003, at E6 (documenting number of paid music downloads); Alex Veiga, *Music Industry Starting to Prevail*, S.F. CHRON., Jan. 12, 2004, at E3 (noting that legal online music sales are increasing sharply).

24. The district court so concluded. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

can make decisions about direct infringement on a case-by-case basis, lawsuits based on indirect liability sweep together both socially beneficial and socially harmful uses of a program or service, either permitting both uses or condemning both.

A middle ground has so far largely been lacking in this debate.[25] Our aim in this Article is to seek such ground. Optimal digital copyright policy with respect to p2p networks would do two things: deter technological innovators as little as possible and permit cost-effective enforcement of copyright in the digital environment.[26] Economically, one can estimate the cost to society from enforcement of the indirect liability rules against p2p providers as a function of the legal uses that that law effectively forbids, plus the foregone efficiency of the p2p distribution mechanism relative to industry-driven distribution of copyrighted content, plus the social value of foregone innovation that results from deterring would-be innovators. If we compare this cost to the benefits accrued by giving digital copyright owners another, more convenient, forum in which to sue, it is not at all clear that the benefits of the new, expanded indirect liability rules exceed the costs in most cases.

Moreover, we might not need to make this difficult tradeoff at all if copyright owners have effective alternatives to suing facilitators.[27] And the basic economics of copyright enforcement do suggest alternative approaches. It is not currently cost-effective for copyright owners to sue individual infringers, because there are tens of millions of them, because lawsuits are expensive, and because many infringers would only be liable for (or able to pay) minimal damages. Copyright owners are happy to sue facilitators instead, because there are fewer of them and both damages and the benefits of injunctive relief are substantial. Copyright owners have no incentive to permit optimal innovation by facilitators, because they do not benefit from that innovation, except indirectly. Individual infringers in turn have no incentive to change their

25. *See* Jane Ginsburg, *How Copyright Got a Bad Name for Itself*, 26 COLUM.-VLA J.L. & ARTS 61 (2002) (blaming copyright owners and consumers in equal measure for the current problems with copyright law generally); Cynthia M. Ho, *Attacking the Copyright Evildoers in Cyberspace*, 55 SMU L. REV. 1561 (2002) (noting that each side tends to demonize the other in this debate); *cf.* Michael J. Madison, Sharing in Copyright: Language and Practice (2003) (unpublished manuscript, on file with authors) (arguing that the rhetoric employed by both sides in the debate—"theft" versus "sharing"—tends to incline the courts toward a particular result). Neil Netanel and Terry Fisher, in recent innovative and insightful work on using levies to compensate copyright owners for unauthorized use of their works, have also sought a middle ground. We discuss these proposals *infra* Part III.B.1.

26. As the Supreme Court noted in *Sony Corp. of America v. Universal City Studios, Inc.*, the goal is to "strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce." 464 U.S. 417, 442 (1984).

27. *See* Dogan, *supra* note 21, at 73 (arguing that the case for moving to secondary liability though new legislation imposing levies or mandating technical controls has not yet been made).

behavior or to subscribe to fee-based services, because they suffer none of the costs of infringement, except indirectly. In this Article, we suggest three possible alternatives that might provide ways out of the digital copyright morass.

One solution is to change the incentives of individuals potentially engaged in copyright infringement. Because individual users of p2p networks know that it is extremely unlikely they will be sued, economic theory suggests that the only way to effectively deter infringement is to increase the effective sanction substantially for those few who are caught and prosecuted.[28] Were the government to criminally prosecute selected users of p2p services, or were copyright owners to sue those users and obtain extremely large monetary judgments, we suspect there could be a substantial deterrent effect on many illegal users. The recording industry has tentatively begun to pursue this path, but would clearly prefer to rely instead on suits against facilitators, and may still be able to persuade courts to let it do so. Selective enforcement has other advantages as well—the suits could target the relatively few keystone providers of illegal files on p2p sites, precisely the users whose activities are most likely infringing. While particular prosecutions will not stop illegal file trading altogether, copyright owners have never been able to prevent all infringement. All they need to do is reduce infringement enough that they can make a return on their investment.

Another solution is to change the incentives for copyright owners to pursue remedies against individual infringers by reducing the cost of enforcement against those infringers or otherwise facilitating compensation from them. One such approach to providing compensation would be a levy system of the types proposed independently by Neil Netanel and by Terry Fisher.[29] Levies on equipment or services have the virtue of permitting automatic collection of royalties and reducing the enforcement cost dramatically but at the price of taxing legal as well as illegal uses. A levy solves the enforcement problem at the front end, but, as with the current approach of suing facilitators, it imposes burdens of copyright enforcement on innovators. The main difference is that under a levy system the copyright owner is protected by a compulsory license rather than a property rule.

Another way to reduce the cost of enforcement is to create some sort of quick, cheap dispute resolution system that enables copyright owners to get some limited relief against abusers of p2p systems and to deter others from such abuse. The existing arbitration system for trademark conflicts over domain

28. Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176-77 (1968). For further discussion, see *infra* notes 198-244 and accompanying text.

29. *See* WILLIAM FISHER, PROMISES TO KEEP: TECHNOLOGY LAW AND THE FUTURE OF ENTERTAINMENT ch. 6 (forthcoming 2004); Neil W. Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J. L. & TECH. 2 (2003); *cf.* Lionel Sobel, *DRM As an Enabler of Business Models: ISPs As Digital Retailers*, 18 BERKELEY TECH. L.J. 667 (2003).

names is a model in some respects—its speed and low cost—but a cautionary tale in others—its lack of some important procedural safeguards.[30] Digital copyright law also differs in some significant ways from the law governing domain names, and the design of a dispute resolution system would have to reflect those differences. For example, because there is no private agency with central authority over all Internet users, the system should be implemented by the Copyright Office. Copyright owners could opt into this administrative dispute resolution system rather than going to court. The system could also be designed to improve precision relative to the essentially binary choice the courts face in indirect infringement cases today. We could design the system so that it is limited to "clear cases"—say uploading more than 50 files to a network in a 30-day period. We could also build in a defense for arguable fair uses, so that a user who could prove she was uploading only out-of-print works, was engaged in critical commentary, or was space-shifting CDs she already owns might have a defense.[31] Such a system would permit low-cost enforcement of copyright law against direct infringers, reducing the need for content owners to sue facilitators. Relative to levies, a dispute resolution system would trade off some increase in cost for precision, targeting only those making illegal uses rather than all users of computers or p2p networks. It would be more fair than selective criminal or civil prosecution, because the burden of paying the penalty for infringement would fall more evenly on each wrongdoer, rather than imposing stark punishment on a few in order to serve society's interest in deterring the rest.

None of these approaches is perfect. Each has its advantages and disadvantages and is likely to work better in some contexts than in others. But it is clear that something must be done to escape the current linkage between reducing copyright infringement over p2p networks and stopping technological innovation in such networks. The economics of copyright enforcement suggests two basic types of alternatives—raising the cost of direct infringement or lowering the cost of enforcement. Pursuing a combination of these approaches—selective enforcement, levies, and an administrative dispute

30. Internet Corporation for Assigned Names & Numbers, *Uniform Domain Name Dispute Resolution Policy* (Oct. 24, 1999), *available at* http://www.icann.org/udrp/udrp-policy-24oct99.htm (last visited Apr. 4, 2004). For a fuller discussion of the UDRP and its problems, see *infra* notes 266-70 and accompanying text.

31. This assumes that space shifting, which seems a paradigmatic fair use offline, should continue to be a fair use when it occurs over a public network and so gives others access to copies of the space-shifted work. We are dubious that such a use would ultimately be considered fair. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (rejecting such an argument in cursory terms). Thus, a user of a system like mp3.com's "My Locker," which limits the number of people who have access to an uploaded file, might have a stronger claim of fair use than an uploader on Napster or another p2p network would have. *But see* UMG Recordings, Inc. v. mp3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000) (rejecting the space-shifting fair use argument on rather doubtful grounds); *cf.* Dogan, *supra* note 21, at 89 (distinguishing between changes facilitated by digital technology, like copies for space-shifting, and changes wrought by the Internet).

resolution system—is preferable to the status quo.

These mechanisms for reducing copyright infringement over p2p networks without unduly burdening innovation will work best if they are accompanied by legal alternatives to which users of copyrighted works, facing a higher likelihood of liability for direct infringement, can turn. The enormous popularity of p2p networks indicates significant demand for convenient and affordable access to copyrighted material over digital networks. While much of that demand stems from the availability of content on p2p networks at no charge, some demand has also arisen from what many users see as a new and improved means of getting access to music. If an increased threat of being held liable for infringement on p2p networks is accompanied by the availability of legal, fee-based services that provide many of the desirable features of p2p networks (and perhaps even additional attractions, such as assured reliability, better quality, and so forth), many of those who currently engage in infringing conduct on p2p networks would no doubt be willing to switch to such a service even though it would be more expensive (at least up front). Legal services for accessing music over the Internet that are perceived to provide good value for the cost have been slow to emerge, but they are essential to reducing infringement.[32] Similar services will likely be needed for copyrighted works other than music as the growth of digital networks fuels demand for new and improved methods of access to such works. The specifics of any such services, for music or other content, are beyond the scope of this Article, but copyright owners will have to offer them in order to effectively fight online infringement.

In Part I, we make the case that there has been a seismic shift in copyright infringement in the digital environment, away from suing direct infringers and towards suing facilitators with less and less connection to the act of copyright infringement. Our discussion in this Part focuses on issues relating to p2p networks, though these cases are part of a broader trend towards suing facilitators rather than direct infringers online. In Part II, we examine the economics of digital copyright infringement. This Part explains why copyright owners are suing facilitators, why doing so is bad for society, and outlines the possible alternatives at a theoretical level. Part III makes those alternatives more concrete by applying them to the problem of infringement over p2p networks. Part III.A explores how a system of criminal prosecution of, or

32. Apple's iTunes music service proved extremely popular when it was first launched, though available only to users with Apple computers. The service has expanded to operate on Windows-based computers. Ina Fried, *Apple to Launch iTunes for Windows*, CNET NEWS.COM, Oct. 9, 2003, *available at* http://news.com.com/2100-1027-5088849.html (last visited Apr. 3, 2004). As of March 2004, customers had downloaded 50 million music files. Ina Fried, *Apple's iTunes Sales Hit 50 Million*, CNET NEWS.COM, Mar. 15, 2004, *available at* http://news.com.com/2100-1027-5173115.html (last visited Apr. 3, 2004). Other companies, including Dell, BuyMusic, and Roxio have recently announced or launched digital online music services. John Borland & John G. Spooner, *Dell Tunes in to Musicmatch Launch*, CNET NEWS.COM, Sept. 29, 2003, *available at* http://news.com.com/2100-1027-5083282.html (last visited Apr. 3, 2004).

severe civil penalties against, high-volume uploaders might work and discusses its likely consequences. Part III.B evaluates the pros and cons of a p2p levy system and proposes an additional alternative: an optional dispute resolution system designed to stop large-scale digital infringement, to be implemented by the Copyright Office. Part III also discusses the limitations and potential problems of these approaches. We conclude that implementing a combination of these strategies may offer copyright owners effective protection without unduly hampering innovation in p2p networks.

I. SUING FACILITATORS

Suits seeking to hold someone other than a direct infringer liable for copyright infringement are not new. Although the Copyright Act throughout the twentieth century was essentially silent on the issue of liability for anyone other than a direct infringer, courts read the statute as imposing such liability in certain circumstances, and Congress endorsed that view in the 1976 Act.[33] Two doctrines of secondary liability have emerged in copyright law: contributory infringement and vicarious liability. With respect to contributory infringement, "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[34] With respect to vicarious liability, "one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[35]

The digital era has so far seen an expansion of secondary liability in two main ways. First, producers and suppliers of technology that has both infringing and noninfringing uses have increasingly been held liable for infringements committed by their users. Second, the directness of the financial interest in infringing activity required before a defendant is held vicariously liable for that activity has been significantly loosened. Although Congress has provided some limitations on the liability of online service providers, those limitations have not significantly cut back on *secondary* liability and in any event are often a poor fit for the activities of p2p providers.

33. Kalem Co. v. Harper Bros., 222 U.S. 55 (1911), is the preeminent early Supreme Court case recognizing indirect liability for copyright infringement. The current statute, 17 U.S.C. § 106 (2004), gives copyright owners the exclusive right "to do and to authorize" certain activities using a copyrighted work. According to the legislative history of the 1976 Act, "[u]se of the phrase 'to authorize' is intended to avoid any questions as to the liability of contributory infringers. For example, a person who lawfully acquires an authorized copy of a motion picture would be an infringer if he or she engages in the business of renting it to others for purposes of unauthorized public performance." H.R. REP. NO. 94-1476, at 61 (1976).

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

35. *Id*.

A. *Indirect Liability and "Dual-Use" Technologies*

The impact on innovation of imposing indirect liability for copyright infringement is particularly important with respect to what might be called "dual-use" technologies.[36] These are products or services that can be used by the consumer in noninfringing ways but that can also be used to infringe copyright. The phenomenon of dual-use technologies is not a new one. After all, musical instruments can be put to both infringing and noninfringing uses. They can be used for public performances of the performer's own musical works or uncopyrighted works, and for private performances (or licensed public performances) of copyrighted musical works, but they can also be used for infringing public performances of copyrighted musical works. Typewriters, printing presses, and photocopy machines can also be used for both lawful and unlawful purposes. But the question of whether the developer or supplier of such dual-use technology can be held liable for copyright infringements committed by a purchaser of the technology has attracted substantial legal attention only in the last twenty-five years or so, and the principal precedent on the question is the Supreme Court's 1984 decision in *Sony Corp. of America v. Universal City Studios, Inc.*[37]

That decision imposed an important limit on secondary liability in the context of the manufacture and sale of dual-use devices. Universal and Disney, which own copyrights in many motion pictures and television shows, sued Sony over its manufacture and sale of videocassette recorders (VCRs), alleging that people who bought VCRs and used them at home to tape broadcasts were engaged in copyright infringement and that Sony was liable for contributing to that infringement. The Court, by a 5-4 vote, declined to impose secondary liability on Sony, announcing a test borrowed from patent law for holding liable those who manufacture and market devices that buyers might use to infringe copyright: "[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."[38] Because the Court determined that a VCR was capable of substantial noninfringing use, Sony was not liable for the infringing uses committed by VCR owners merely because it made and sold the machine.

The substantial noninfringing use test was designed to reconcile the need to give copyright owners effective protection for their works and "the rights of

36. We use this term by analogy to its use to describe technologies that have both civilian and military uses, leading to efforts to control access to the technologies by those who would use them for military purposes.

37. 464 U.S. 417 (1984).

38. *Id*. at 442. The opinion also speaks of the standard as being whether the equipment "is capable of *commercially significant* noninfringing uses" but does not indicate whether "substantial" and "commercially significant" uses are equivalent. *Id*. (emphasis added).

others freely to engage in substantially unrelated areas of commerce."[39] The Court's concern, easily discernible in its analogy to the "staple article of commerce" doctrine in contributory patent infringement cases, was that copyright owners should not be allowed to control the development of new technologies used in connection with copyrighted works. Although the issue directly before the Court in *Sony* was a claim of contributory infringement,[40] the opinion strongly suggested that its analysis applied to secondary liability for copyright infringement generally and that the principles in its decision would bar using copyright's vicarious liability doctrine to hold Sony liable for infringements committed by VCR users.[41]

The *Sony* doctrine clearly provides significant protection for innovation in technologies that are related to the use of copyrighted material. Where such innovation leads to a dual-use product or service—that is, a product or service capable of substantial noninfringing use—the *Sony* decision was intended to provide assurance that the technology developer will not be held liable for those infringements that consumers commit using the new technology.

In the context of p2p networks, however, lower court decisions have cut back the protection that the *Sony* doctrine offers developers of dual-use technologies, though the courts' opinions leave some uncertainty about how far the cutback goes. The Ninth Circuit's decision in *A&M Records, Inc. v. Napster Inc.*,[42] and the Seventh Circuit's decision in In re *Aimster Copyright Litigation*[43] are emblematic of this trend.

1. *Napster*.

Napster disseminated software that allowed users to connect directly to one another's computers and transfer music files. When a Napster user was connected to the network, Napster's computer servers indexed the music files on the user's computer. Any Napster user looking for a specific file could

39. *Id*.

40. *Id*. at 435 n.17.

41. The Court noted the parties' statements "that the questions of Sony's liability under the 'doctrines' of 'direct infringement' and 'vicarious liability' are not *nominally* before this Court." *Id*. (emphasis added). However, the Court approvingly quoted the district court's observation that "'the lines between direct infringement, contributory infringement and vicarious liability are not clearly drawn.'" *Id*. The Court further noted that "reasoned analysis of [the studios'] unprecedented contributory infringement claim necessarily entails consideration of arguments and case law which may also be forwarded under the other labels." *Id*. The Court's discussion often uses the terms "vicarious liability" and "contributory infringement" rather loosely, primarily as synonyms for "secondary liability" rather than as names of specific and distinguishable theories of liability. *See, e.g.*, *id*. at n.18 (citing and discussing vicarious liability cases as examples of imposing liability on "the 'contributory' infringer").

42. 239 F.3d 1004 (9th Cir. 2001).

43. 334 F.3d 643 (7th Cir. 2003).

search the index of available files on Napster's server and then connect directly to another Napster user to transfer the file. Music copyright owners sued Napster, charging that users of the Napster p2p network were infringing their copyrights and that Napster was liable for the users' infringements. Napster argued that its software and network were capable of substantial noninfringing use (such as exchanging files of copyright owners who did not object to such dissemination) and that *Sony* therefore shielded it from liability for users' infringements. The Ninth Circuit, however, read *Sony* narrowly. The *Sony* opinion, the court concluded, merely barred a court from imputing to a defendant constructive knowledge of another party's infringement if the defendant was the maker of copying equipment that was capable of "'substantial noninfringing uses.'"[44] Thus, making and selling equipment capable of noninfringing use could still lead to secondary liability for users' infringements if a copyright owner could establish by other means that the maker knew, or perhaps should have known,[45] of the users' infringements, and materially contributed to them. The Ninth Circuit found that Napster had actual knowledge that infringement had occurred on its network and that Napster provided the facilities for that infringement, so Napster could be liable as a contributory infringer.[46]

It is worth noting that it is not clear that Sony itself would have escaped secondary liability under the Ninth Circuit's reading of the Supreme Court's test.[47] The *Napster* court based its finding of actual knowledge on notices

44. *Napster*, 239 F.3d at 1020 (quoting *Sony*, 464 U.S. at 442).

45. Although the Ninth Circuit affirmed the district court's contributory infringement conclusion on the grounds that "Napster has *actual* knowledge that *specific* infringing material is available using its system," *id*. at 1022 (emphasis added), it also approved the district court's conclusions that Napster had both actual and constructive knowledge of infringement. *Id*. at 1020 & n.5. In discussing *Sony,* the court indicated that it could not impute the necessary knowledge to Napster "merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights," *id*. at 1020-21, but it did not suggest that constructive knowledge could not be imputed to such a contributory infringement defendant based on other factors (such as those used by the district court in *Napster*). In addition, the court's emphasis on Napster's actual knowledge followed its discussion of liability standards for operators of computer systems, which the court emphasized allowed liability where the operator learns of infringing material and fails to remove it, but not simply where the system allows for copyright infringement. Both situations leave open the possibility of liability where the defendant does not *actually* know of particular infringing activity using the product or system but had reason—beyond merely knowing that the system was capable of infringing use—to know of the activity.

46. *Id*. at 1021-22. Stacey Dogan suggests that the court did not mean to abrogate *Sony* altogether. Rather, she suggests that "actual knowledge" means knowledge of a specific act of infringement in sufficient time to avert it. *See* Stacey L. Dogan, *Is Napster a VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001). The district court in *Grokster* adopted this interpretation, as discussed below, while the *Napster* district court on remand required Napster to block access to all infringing files.

47. For additional criticism of the reasoning in the *Napster* opinion, see David Nimmer, Codifying Copyright Comprehensibly (2004) (unpublished manuscript, on file with authors).

provided by copyright owners to Napster, charging specific past instances of infringing uses of Napster. It seems quite likely, however, that Disney and Universal would have been able, in the wake of the *Sony* decision, to provide notice to Sony alleging specific infringing uses by particular VCR owners. Survey evidence in the case indicated that "a substantial number of [survey respondents] had accumulated libraries of tapes,"[48] and the Supreme Court's opinion did not address the question of whether library building was a noninfringing fair use. It therefore seems likely that the studios could have given Sony actual knowledge of infringing use of its VCR by some users and thus, under *Napster*'s reading, perhaps overcome the *Sony* court's limitation on secondary liability. Since making and selling a VCR seems likely to be a material contribution to the infringing recording of television broadcasts, the consumer-electronics maker might well have been liable under the *Napster* court's interpretation of *Sony*.[49]

Despite the broad language of the *Napster* court, its decision may have a more limited reach. After concluding that *Sony* prohibited imputing knowledge to Napster, the court focused not on the issue of knowledge for contributory infringements by providers of dual-use technologies generally, but instead on the knowledge specifically necessary for finding contributory infringement by the operator of a computer system. For such a defendant, the court stated that contributory infringement would be established "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system."[50] The court held that the evidence showed that Napster had "*actual* knowledge of *specific* infringing material . . . available using its system" and "that it could block access to the system by suppliers of the infringing material."[51] To the extent that the Ninth Circuit's view that contributory infringement for suppliers of "dual use" technologies turns on both knowledge *and* the ability to act to prevent infringement, then a manufacturer

48. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 423 (1984).

49. Even without notice from copyright owners of actual infringement, Sony probably had constructive knowledge of infringement by VCR users. Some Sony ads for its VCR had suggested that customers use the VCR to "build a library" of recorded programs. Universal City Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429, 436 (C.D. Cal. 1979).

A more nuanced reading of "material contribution" might require that the contribution be made at the time that the defendant knew of the infringing use, which would presumably free Sony from liability for past VCR sales to users later shown to be infringing. As discussed below, the *Grokster* court took this approach to the issue. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003). But if constructive knowledge based on something other than the equipment's capabilities is enough to make an equipment manufacturer a contributory infringer, as the *Napster* decision suggests it might be, see *supra* note 45, then Sony might have been enjoined from further VCR sales.

50. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).

51. *Id*. at 1022 (emphasis added). While this language may suggest that the *Napster* rule applies only to service providers and not to device manufacturers, the court does not explicate this idea, as one might have expected it to do if it intended different tests, since Napster supplied both services and software.

such as Sony would not necessarily be liable under the *Napster* court's interpretation of the *Sony* decision.[52] The Ninth Circuit's decision, however, is not a model of clarity on this point, and the question is at issue in the *Grokster* litigation discussed below, currently before the Ninth Circuit.

The *Napster* court also limited the protective reach of *Sony* by holding that a product's capability for substantial noninfringing use was entirely irrelevant to the issue of vicarious liability. As noted above, the Supreme Court's opinion in *Sony* suggested that the maker of a product capable of substantial noninfringing use would not be indirectly liable for user's acts of infringement under either a contributory infringement or a vicarious liability theory. The *Napster* opinion, however, suggests that the noninfringing uses to which an innovator's technology can be put are irrelevant to the question of vicarious liability.

2. *Aimster*.

Aimster provided a file-sharing service over the instant messaging (IM) networks of service providers such as AOL, ICQ, and Yahoo!. The IM networks allow users to share files with select lists of "buddies," and Aimster built upon this capability by allowing users to designate all Aimster members as "buddies," thus allowing users to search for files available on any Aimster member's designated space.

Following the *Napster* decision, Aimster filed for declaratory relief and the RIAA and record companies countersued for copyright infringement. When Aimster later filed for bankruptcy, the bankruptcy court ordered an immediate decision on the copyright owners' pending motion for a preliminary injunction. The district court allowed Aimster to continue operations but ordered it to refrain from allowing any uploading or downloading of the record company and music publishing plaintiffs' works.[53]

Aimster argued that the *Sony* doctrine shielded it from liability because the Aimster software could be used for noninfringing purposes, including transferring uncopyrighted files (or presumably files in which the transferring party owned the copyright) to other users. The district court rejected the argument, advancing several grounds for distinguishing *Sony* and concluding

52. This presumes that the necessary ability to act to prevent infringement would not include the ability simply to design the equipment not to allow any infringing conduct. Sony, after all, could have manufactured a VCR that did not allow for recording of television broadcasts, or perhaps could have incorporated technology that would have allowed recording only where the copyright owner of the transmitted audio-visual work consented to recording as indicated by encoded information accompanying the transmission. *See* Dogan, *supra* note 46.

53. *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003); *In re* Aimster Copyright Litig., No. 01 C 1425, 2002 WL 31443236 (N.D. Ill. Oct. 30, 2002).

that the doctrine did not prevent Aimster from being held liable for infringements committed using its software. Most significantly, the court ruled that even though the *Sony* court had framed the question as whether a product was "capable of substantial noninfringing uses," the actual facts in *Sony* established that the VCR's "principal use" was noninfringing, whereas there was no evidence before the court that any Aimster user had *actually* used the software for any of the potential noninfringing uses that Aimster identified. The court further explained that such evidence would have to establish not merely that Aimster was capable of such use, or that it had actually been used for noninfringing purposes, but that such use "constituted Aimster's *primary* use."[54]

The Seventh Circuit affirmed the preliminary injunction issued in *Aimster*, but on different grounds. The Seventh Circuit expressed concern about the impact of secondary liability on the development of new online services. It held that in applying the *Sony* doctrine to the provider of an ongoing service (rather than a discrete product), the service provider's ability "to prevent its customers from infringing is a factor to be considered in determining whether the provider is a contributory infringer."[55] But the court recognized that ability to prevent infringement should not in itself determine liability because such a rule would have "alarming" adverse consequences for the provision of dual-use services:

> If a service facilitates both infringing and noninfringing uses . . . and the detection and prevention of the infringing uses would be highly burdensome, the rule [that imposes liability whenever the service provider knows of infringing activity and could prevent it] could result in the shutting down of the service or its annexation by the copyright owners (contrary to the clear

54. *Aimster*, 252 F. Supp. 2d at 653 (emphasis added). In essence, the District Court read the *Sony* majority to embody an even narrower protection against secondary liability for makers of copying equipment than that proposed by the *Sony* dissenters, who would have ruled that "if a *significant* portion of the product's use is *noninfringing*, the manufacturers and sellers cannot be held contributorily liable for the product's infringing uses." Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 491 (1984) (Blackmun, J., dissenting). None of the verbal formulations used in either the *Sony* majority or dissent indicated that secondary liability could be imposed whenever a product did not have a *primary* noninfringing use.

In addition, the *Aimster* district court suggested that *Sony* only immunized a supplier of copying equipment against private, home-use copying done using its equipment, and not against the "widespread distribution of infringing works." *Aimster*, 252 F. Supp. 2d at 653. The court further suggested that *Sony* did not apply when a product was "specifically manufactured for infringing activity," even if the product did have noninfringing uses, and the court found that Aimster's service was in fact specifically designed to assist users in infringement. *Id.* at 654. Next, the court ruled that *Sony* applied only to a "staple article of commerce," and Aimster was not such an article. *Id.* at 652 (quoting *Sony*, 464 U.S. at 442). A VCR was a "discrete product" that was sold to a buyer who then used the machine as she saw fit. The court viewed Aimster not as such a product but as a service that involved an ongoing relationship between Aimster and its users. *Id.* at 653. Finally, the court read *Sony* as applying only if the defendant did not influence or encourage infringement by the users of its product, and found that Aimster did both. *Id.* at 654.

55. *In re* Aimster Copyright Litig., 334 F.3d 643, 648 (7th Cir. 2003).

> import of the *Sony* decision), because the provider might find it impossible to estimate its potential damages liability to the copyright holders and would anyway face the risk of being enjoined.[56]

The *Aimster* circuit court also expressed disagreement with the Ninth Circuit's position in *Napster*, which it characterized as "suggesting that actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributory infringer."[57]

The court did not, however, merely reaffirm the *Sony* opinion's language that secondary liability would not be imposed on the supplier of a technology that is "capable of substantial noninfringing use." Rather, it held that in order to determine whether the supplier of a dual-use service was liable for users' infringements, "some estimate of the respective magnitudes of [noninfringing and infringing] uses" must be made.[58] The court made clear that it was not enough for Aimster to show that "its file-sharing system could be used in noninfringing ways."[59] The fact that a product or service is *capable* of noninfringing uses would not exempt the supplier from liability if the product or service "in fact is used only to infringe."[60] Because there was evidence that Aimster's system was in fact being used for infringing purposes, the court said that the burden shifted to Aimster, at least at the preliminary injunction stage, "to demonstrate that its service has substantial noninfringing uses."[61] It turned out, however, that the court did not in fact think that it was sufficient that Aimster service *had* noninfringing uses. What the court actually required was that Aimster *quantify* how much of the use of its system was noninfringing. Thus, although the court itself explained several possible noninfringing uses of the Aimster system, it concluded that "[i]t is not enough . . . that a product or service be physically capable, as it were, of a noninfringing use. Aimster has failed to produce any evidence that its service has ever been used for a noninfringing use, let alone evidence concerning the frequency of such uses."[62] This lack of evidence relieved the court from having to decide how frequent noninfringing uses would have to be for the service provider to escape liability for infringing uses of the service, though it quoted the district court's language on Aimster's failure to show that the "primary" use of the system was noninfringing.

The court further suggested that even if a new technology was not only

---

56. *Id*. at 648-49.

57. *Id*. at 649 (citing 2 PAUL GOLDSTEIN, COPYRIGHT § 6.1.2, ¶ 6:12-1 (2d ed. 2003)).

58. *Id*.

59. *Id*. at 651.

60. *Id*. Such an approach would shortchange the importance of potential future noninfringing uses, as the Ninth Circuit recognized in *Napster*. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001) (noting that analyzing only current uses and "ignoring the system's capabilities" undervalues future noninfringing uses).

61. *In re* Aimster Copyright Litig., 334 F.3d at 652.

62. *Id*. at 653.

capable of substantial noninfringing use but was in fact used in noninfringing ways, that would not in itself be enough to avoid secondary liability for actual infringements:

> Even when there are noninfringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.[63]

The requirement, at least in the context of p2p services, that a supplier design her service to prevent or reduce infringement unless it is excessively costly to do so appears to go beyond what *Sony* required: Although the dissenters in *Sony* discussed design alternatives available to Sony that would have reduced infringement, the majority made no mention of those possibilities as relevant to the question of Sony's liability for its users' infringements.[64]

Like the Ninth Circuit's *Napster* opinion, *Aimster*'s interpretation of *Sony* poses significant challenges to innovation. Someone who develops a new dual-use technology must be concerned about whether noninfringing use of that technology will not only be "substantial" but perhaps whether it will be the primary use, as well as whether she will be able to prove that substantial or primary use in court. Perhaps more significantly, even if the innovator is confident as to how the technology will be used, she will have to consider, at least in the case of services, whether she can design the technology to reduce or eliminate the possibility of infringing uses of the technology, what the costs of doing so are, and whether a court will decide that those costs are "disproportionate" and therefore need not be expended.

3. *Grokster*.

One district court has taken a different approach to applying *Sony* to p2p services, in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, involving providers of p2p software.[65] Music and movie copyright owners sued several defendants, alleging that users of their software infringed on the plaintiffs' copyrights and that the defendants, as providers of the software, were secondarily liable for that infringement. In April 2003, the district court granted summary judgment to two of the defendants, Grokster and StreamCast, which disseminate the "Grokster" and "Morpheus" software, respectively.[66] In applying the principles announced in *Napster* to the providers of p2p software,

63. *Id*.

64. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 494 (1984) (Blackmun, J., dissenting).

65. 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

66. *Id*. The decision did not involve a third defendant in the case, Sharman Networks, which disseminates Kazaa p2p software and licenses the "FastTrack" technology on which several p2p software products, including Grokster, are based.

the *Grokster* court appears to have given innovators of dual-use technologies more breathing room.

The court described the operation of the Grokster and Morpheus networks as follows:

> Although novel in important respects, both the Grokster and Morpheus platforms operate in a manner conceptually analogous to the Napster system . . . .
>
> Once [either defendant's software is] installed, a user may elect to "share" certain files located on the user's computer . . . . When launched on the user's computer, the software automatically connects to a peer-to-peer network . . . and makes any shared files available for transfer to any other user currently connected to the same peer-to-peer network.
>
> Both the Morpheus and Grokster software provide a range of means through which a user may search through the respective pool of shared files . . . [Using the search results] [t]he user may . . . initiate a direct transfer from the source computer to the requesting user's computer. When the transfer is complete, the requesting user and source user have identical copies of the file . . . .[67]

Grokster and StreamCast users connect directly with one another's computers in order to transfer files between those computers, as Napster users did. The primary difference in operation between the defendants' software and Napster's software is that in order to search for files, Napster users connected to central servers operated by Napster that identified the files available on the computer of each Napster user when that user was connected to the network. Grokster and StreamCast, by contrast, maintain no such central index.

Finding that at least some users of the defendants' software engaged in direct copyright infringement, the court turned to the question of whether Grokster and StreamCast could be liable as contributory infringers. With respect to the defendants' knowledge of end-user infringement, the court followed the Ninth Circuit's *Napster* decision in reading *Sony* as addressing only the knowledge required for a finding of contributory infringement where a product is capable of substantial noninfringing use. The court found that the defendants' software is capable of such use, including disseminating works with the consent of the copyright owner and disseminating works not protected by copyright, and the defendants offered evidence of such actual use by its customers.[68] As a result, the court applied the standard announced in *Napster*, which it read to create liability for computer system operators only where they had actual knowledge of specific infringement, could have acted to stop such infringement, and failed to do so.

---

67. *Id*. at 1032-33 (citations omitted).

68. The court noted evidence that the software "is regularly used to facilitate and search for public domain materials, government documents, media content for which distribution is authorized, media content as to which rights owners do not object to distribution, and computer software for which distribution is permitted." *Id*. at 1035.

Because the defendants were not operating computer networks, the district court focused on the *timing* of an indirect-liability defendant's knowledge of infringing activity:

> [L]iability for contributory infringement accrues where a defendant has actual—not merely constructive—knowledge of the infringement at a time during which the defendant materially contributes to that infringement. . . .
>
> In other words, as the Ninth Circuit explained, defendants are liable for contributory infringement only if they (1) have specific knowledge of infringement at a time at which they contribute to the infringement, and (2) fail to act upon that information.[69]

The court noted evidence (including internal documents and searches by company executives) which illustrated that Grokster and StreamCast "clearly know that many if not most of those individuals who download their software subsequently use it to infringe copyrights."[70] In addition, the court observed that the plaintiffs had sent defendants thousands of notices of claimed infringements. But in the court's view, the crucial question was whether the defendants had "actual knowledge of infringement at a time when they can use that knowledge to stop the particular infringement"[71]—that is, "whether actual knowledge of specific infringement accrues at a time when either Defendant materially contributes to the alleged infringement, and can therefore do something about it."[72]

With respect to the defendants' material contribution to their users' infringements, the court framed that question as "whether Grokster and StreamCast do anything, aside from distributing software, to actively facilitate—or whether they could do anything to stop—their users' infringing activity."[73] Neither Grokster nor StreamCast operated the network over which the users of their software connected and exchanged files, and the court emphasized the decentralized nature of those networks: When users search for and initiate file transfers, no information is transmitted to or through any computers owned or controlled by the software makers.[74] The court focused on

> a seminal distinction between Grokster/StreamCast and Napster: neither Grokster nor StreamCast provides the "site and facilities" for direct infringement. . . . Users connect to the respective networks, select which files to share, send and receive searches, and download files, all with no material involvement of Defendants. If either Defendant closed their doors and deactivated all computers within their control, users of their products could

69. *Id*. at 1036.

70. *Id*. at 1037.

71. *Id*.

72. *Id*. at 1038.

73. *Id*. at 1039.

74. *Id*. at 1039-40, 1041. Further, the court explained that when a user wishes to connect to the Grokster or Morpheus p2p networks, the user must locate another user to whom to connect, but the court emphasized that neither defendant was involved in the process that allows a user to locate a network connection.

continue sharing files with little or no interruption.

> In contrast, Napster indexed the files contained on each user's computer, and each and every search request passed through Napster's servers. Napster provided the "site and facilities" for the alleged infringement, affording it perfect knowledge and complete control over the infringing activity of its users. If Napster deactivated its computers, users would no longer be able to share files through the Napster network.[75]

The court therefore concluded that Grokster and StreamCast did not provide active and substantial contribution to end-user infringements[76] in a way that justified holding the companies liable as contributors to those infringements:

> Defendants distribute and support software, the users of which can and do choose to employ it for both lawful and unlawful ends. Grokster and StreamCast are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights. While Defendants, like Sony or Xerox, may know that their products will be used illegally by some (or even many) users, and may provide support services and refinements that indirectly support such use, liability for contributory infringement does not lie "merely because peer-to-peer file-sharing technology may be used to infringe plaintiffs' copyrights."[77]

The *Grokster* decision thus offers innovators of dual-use p2p technologies substantially more protection against the danger of secondary liability for their users' acts of copyright infringement than do the *Napster* or *Aimster* opinions, at least where the innovator creates a dual-use product and does not have an ongoing service relationship with the user. Whether this approach will continue, however, will depend on the Ninth Circuit, as the plaintiff copyright owners have appealed the decision. If courts do follow the *Grokster* approach and permit p2p software providers to continue to operate, the focus of the legal debate will necessarily shift from seeking secondary liability for software providers to finding ways for copyright owners to receive compensation from those who actually use p2p networks to infringe copyrights.

---

75. *Id*. at 1041 (citations omitted).

76. The court rejected evidence of "a handful of isolated technical support e-mails from Grokster and StreamCast employees sent in response to users who encountered difficulties playing copyrighted media files." Grokster, 259 F. Supp 2d. at 1042. The court also rejected as irrelevant the defendants' alleged ability to communicate with users and prompt them to upgrade their software. *Id*.

77. *Id*. at 1043 (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020-21 (9th Cir. 2001)).

B. *Expansion of Vicarious Liability and the "Direct" Financial Interest Requirement*[78]

While the *Sony* doctrine's protection of developers of dual-use technologies has been interpreted so as to make it of uncertain use to innovators of p2p technologies, the doctrine may be undermined entirely by recent developments in the law of vicarious liability. Vicarious liability for infringement committed by a third party has expanded in recent years, offering another possible approach for copyright owners to hold p2p developers liable for infringement committed by users of their technologies. The basic rule is that "one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[79] In recent years, courts have substantially expanded what constitutes a sufficiently "direct financial interest" in an infringer's activity to hold a third party liable for that activity. The result is that ever more parties are potentially subject to vicarious liability for others' copyright infringements, including innovators who may be deterred from pursuing innovations because of such potential liability.[80]

Vicarious liability in copyright law can be traced back to the doctrine of respondeat superior and was initially used to hold employers liable for infringements committed by their employees. The doctrine expanded to hold defendants liable for infringements committed by independent contractors as well. The seminal case of *Shapiro, Bernstein & Co. v. H.L. Green Co.*[81] involved a department store whose record departments were operated by an independent concessionaire. Green received ten to twelve percent of the concessionaire's gross receipts from record sales. The concessionaire sold infringing recordings, and Green was held liable. The court found that Green had "an obvious and direct financial interest in the exploitation of copyrighted materials" by the concessionaire—indeed, the court viewed Green as having "a most definite financial interest in the success of [the] concession; ten percent or twelve percent of the sales price of every record sold by [the concessionaire], whether 'bootleg' or legitimate, found its way . . . into the coffers of the Green Company."[82]

78. For a comprehensive general discussion, see Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1843-72 (2000).

79. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

80. As noted above, establishing vicarious liability requires showing both that a defendant has a direct financial interest in the infringing activity *and* that the defendant has the right and ability to control that activity. Our discussion focuses only on the direct financial interest requirement, but in each case a plaintiff would have to establish the control element as well.

81. 316 F.2d 304 (2d Cir. 1963).

82. *Id*. at 307-08.

In recent years, the doctrine has far outgrown the employment and independent contracting contexts, and the financial interest that a defendant must have in a third party's infringing activities in order to be held liable has become more attenuated. The Ninth Circuit's 1996 decision in *Fonovisa, Inc. v. Cherry Auction, Inc.*[83] is generally viewed as a major case in the expansion of vicarious liability. The defendant in that case operated a flea market where it rented space to third-party vendors; Cherry Auction advertised the flea market to the public and charged customers for parking, admission, and food sold at the market.[84] Fonovisa sued, seeking to hold Cherry Auction liable for sales by a flea market vendor of infringing recordings. Under the doctrine of vicarious liability, the Ninth Circuit held that Cherry Auction "reap[ed] substantial financial benefits from admission fees, concession stand sales, and parking fees, all of which flow directly from customers who want to buy the counterfeit recordings at bargain basement prices" and that this was sufficient for the imposition of vicarious liability.[85] The court reasoned that, because the infringing activity "enhance[d] the attractiveness of the venue to potential customers" and served as a "draw" for customers, the venue operator could be held liable for the infringing activity.

Fonovisa's interpretation of the "direct financial interest" standard for vicarious liability allows imposing liability based on what seems to be a somewhat *indirect* financial interest. The flea market earned nothing directly from the sale of infringing recordings by one of its vendors, unlike Greene's percentage cut of its concessionaire's sales. Instead, the court assumes that the vendor's offering of infringing recordings attracted to the flea market customers who otherwise would not have attended, and those additional customers would generate revenues for the flea market not from their purchase of infringing material but from ancillary fees.

The less direct connection between infringement and financial interest had been recognized before *Fonovisa*, but in prior cases the connection between the use of copyrighted works and the financial benefit to the defendant was generally tighter. Thus, the financial connection seems fairly clear in the traditional "dance hall" cases, which hold the operator of a dance hall vicariously liable for infringing public performances of copyrighted musical works committed by a band that the operator hired to play in the dance hall. Most customers pay admission to the dance-hall operator largely because they wish to hear and/or dance to the music performed. Thus, the operator's financial interest in the performance of music, infringing or otherwise, seems sufficiently strong to characterize that interest as "direct" for purposes of vicarious liability. It seems far less clear that most flea market shoppers pay admission to a flea market largely because they wish to purchase copyrighted

83. 76 F.3d 259 (9th Cir. 1996).

84. *Id*. at 261-63.

85. *Id*. at 263.

material such as sound recordings (infringing or otherwise). But in *Fonovisa*, the existence of infringing activity is assumed to draw customers in greater numbers than noninfringing activity, and any money those customers pay to the defendant appears to count as revenue "directly" related to the infringing activity for purposes of vicarious liability.

In *Napster*, the Ninth Circuit in a single paragraph loosened the "direct financial interest" requirement even further.[86] The court followed *Fonovisa* in ruling that the availability of infringing music on the Napster system served as a "draw" for users. But because Napster disseminated its software to users, and permitted them to use its system to list and locate titles, at no charge, it did not, unlike Cherry Auction, make money off of the customers attracted by the infringing material. Indeed, it did not even make money indirectly, by selling advertising to users of the service. The Ninth Circuit concluded, however, that because Napster would likely charge users in the future, and because that "future revenue is directly dependent upon 'increases in userbase,'" Napster had a sufficiently direct financial interest in infringement committed by its users to warrant holding the company vicariously liable for that infringement. Thus, not only can a defendant be held liable if it earns money from providing ancillary services to customers attracted by infringement, it can be held liable if it is likely to earn such money in the future.

Even more significantly, *Napster* concluded that *Sony*'s protection from liability of those who make and supply copying equipment capable of substantial noninfringing use simply did not apply to the question of vicarious liability (as opposed to contributory infringement). The less-direct financial interest that suffices under *Fonovisa* to establish vicarious liability therefore applies to equipment providers under *Napster*, despite strong suggestions in the *Sony* opinion that a provider should not be held vicariously liable if the equipment provided is capable of substantial noninfringing use.[87]

As a result of the loosened requirement for direct financial interest and the elimination of the defense of capability of substantial noninfringing use, innovators are more likely today to be found vicariously liable for copyright infringement committed by users of their innovations, just as they are more likely to be found liable for contributory infringement under the *Napster* and *Aimster* cases than under *Sony*.

86. A&M Records Inc., v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001). The *Napster* court's conclusion that the defendant would likely be held vicariously liable for its end-users' infringements might have been the same even without the loosening of the directness of financial benefit required under *Fonovisa*. The situation in *Napster* seems closer to that of the dance-hall cases, in which users of the service can quite easily be said to be using the service because of the availability of works of authorship. In cases of other innovators facing potential suit as facilitators, however, the innovation may not be so closely tied to works of authorship, such that the innovator might not have a sufficiently direct financial interest under the dance-hall cases but would have such an interest under *Fonovisa*.

87. *See supra* note 41 and accompanying text.

C. *Statutory Safe Harbors for Online Service Providers*

For innovators who are also Internet service providers, the *Sony* doctrine is only one source of limitation on liability for copyright infringement. In 1998, Congress enacted, as part of the Digital Millennium Copyright Act, statutory limitations on the liability of those who provide online services. Essentially, Congress provided "online service providers" (OSPs) with several safe harbors: If an entity qualifies as an OSP[88] and meets two basic eligibility requirements,[89] then it is exempt from all monetary relief and most injunctive relief for copyright infringement with respect to four specified categories of activities if specific conditions (which vary with the type of activity) are met. If an OSP fails to qualify for the safe harbor on any basis, then its liability for copyright infringement is to be determined by the ordinary principles of copyright law.

Congress enacted the safe harbors in response to concerns expressed by online service providers about their potentially overwhelming liability for copyright infringement committed by their users. These statutory safe harbors, however, have not provided significant protection from indirect liability to innovators of dual-use technologies, particularly in the p2p context. The main reason for this is that the safe harbor most relevant to p2p systems (the harbor protecting providers of information location tools) primarily protects service providers against liability for acts of *direct* copyright infringement committed by the provider. This safe harbor largely preserves the availability of relief against service providers on the basis of secondary liability for infringement committed using the service, though the safe harbors may somewhat heighten the requirements for holding the provider secondarily liable.

1. *Eligibility for safe harbors*.

As a threshold matter, the safe harbors apply to any "provider of online services or network access, or the operator of facilities therefor."[90] Some innovators will likely not meet this definition and therefore not be eligible for the safe harbors at all. A company that distributes p2p software, for example, may be disseminating a product that its customers use over an online network, but the company itself may not be providing (or operating any facilities for) online services or network access. Other p2p innovators, however, will likely

88. *See* 17 U.S.C. § 512(k) (2004) (defining "service provider").

89. *See id*. § 512(*i*) (requiring OSPs to adopt and reasonably implement policy of terminating subscribers who are repeat infringers and to accommodate standard technical measures used to identify and protect copyrighted works).

90. *Id*. § 512(k)(1)(B). This includes any "entity offering the transmission, routing, or providing of connections between or among points specified by a user of material of the user's choosing, without modification to the content of the material as sent or received." *Id*. § 512(k)(1)(A).

qualify as service providers eligible for safe harbor protection. Napster and Aimster, for example, seem at least to have offered their users "online services;" a Napster user would connect over the Internet to Napster's own computers in order to identify music files available for copying.

2. *Application to activities of p2p providers*.

The safe harbors protect those that qualify as OSPs from copyright infringement liability for four kinds of activity. The first harbor, in Section 512(a), essentially protects against liability for merely transmitting or retransmitting someone else's material over a computer network—that is, essentially for serving as a mere conduit for Internet transmissions.[91] This harbor protects activities of ordinary Internet access providers, such as Earthlink or AOL, when they transmit a customer's email message over the Internet to its addressee or when they retrieve a webpage from a third-party's computer and transmit it to a customer's computer at that customer's request. The second safe harbor protects a service provider who temporarily caches or stores online material on its own system or network in order to be able to transmit that material at a later time to other of the provider's users who request it.[92] A third safe harbor limits the liability of a service provider that stores information on its own system or network at the direction of a user, such as an OSP that hosts a user's website on the OSP's computers or an online auction website, such as eBay, that hosts a customer's auction information on its computers.[93] Finally, a fourth safe harbor shields service providers who offer "information location tools."[94] These include not only directories, indices, and search engines that direct users to information on the Internet, but also any "reference, pointer, or hypertext link" to such information.[95]

For p2p service providers that meet the statutory definition of "service provider," the Section 512 safe harbors may offer little protection from liability for copyright infringement committed by the service's users. The first court to address this issue in any depth was the district court in the *Napster* case.[96] That court ruled that Napster was not protected from liability for its users' copyright infringements under the Section 512(a) "conduit" safe harbor. It reasoned that the safe harbor only protects a service provider against liability for the

91. *See id*. § 512(a). That section also lists five additional conditions that must be met for the provider's transmission activities to be protected from liability. *Id*.

92. *See id*. § 512(b)(1) (describing the precise parameters of the safe harbor); *id*. § 512(b)(2) (setting forth several detailed conditions that must be met in order for the service provider to qualify for the safe harbor).

93. *See id*. § 512(c).

94. *See id*. § 512(d).

95. *See id*.

96. A&M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 54 U.S.P.Q.2d 1746, 2000 U.S. Dist. LEXIS 6243 (N.D. Cal. May 5, 2000).

provider's "transmitting, routing, or providing connections for, material *through a system or network controlled or operated by or for the service provider*."[97] Because any infringing transfer of files in Napster's system occurred directly between two Napster users over the Internet and not through Napster's own system, the court concluded that the secondary liability claims against Napster were not based on the activity shielded by Section 512(a) and thus were not precluded by the safe harbor. The district court in the *Aimster* case reached the same conclusion about that company's system.[98] Given that p2p services, by their very nature, involve decentralized transmissions directly between users, the Section 512(a) safe harbor, at least as interpreted by the *Napster* court, seems likely to offer little protection against secondary liability claims.

The safe harbors in Sections 512(b) and 512(c) will generally not offer p2p innovators protection against secondary liability claims because those provisions cover infringement claims arising out of the storage of material on the defendant's own computer system or network, and p2p systems, involving as they do transmissions directly between two users of the system, typically do not involve such central storage on a provider's computer.[99]

Section 512(d) governing "information location tools" might cover activities of some p2p providers, since those providers may supply users information regarding where a particular file is available on the p2p network. Indeed, the district court in *Napster* ruled that the defendant "undisputedly performs some information location functions."[100] Nonetheless, Section 512(d) provides little protection to innovators against secondary liability claims, because this safe harbor primarily shields defendants against liability for acts of *direct* copyright infringement while placing essentially no limitation on claims that a service provider is secondarily liable for the direct infringements of its users. As a result, under Section 512(d), someone who refers users to infringing online material or activity remains subject to liability if that person actually knows that the material or activity is infringing or is aware of facts or circumstances from which the infringing activity is apparent.[101] This

97. 17 U.S.C. § 512(a) (2004) (emphasis added).

98. *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 659-60 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

99. The *Aimster* case did involve allegations of temporary storage of copyrighted material by the defendant, but the plaintiffs in that case did not base any claim of infringement on that temporary storage. In addition, the Section 512(c) safe harbor protects defendants against claims of liability for direct infringement based on their storage on a user's material but essentially preserves claims for secondary liability against providers, as does Section 512(d).

100. *Napster*, 2000 U.S. Dist. LEXIS 6243, at *15. Just as a search engine allows a user to locate particular information on the Web, the Napster search function allowed users to locate particular files on other users' computers.

101. 17 U.S.C. § 512(d)(1)(A)-(B) (2004); *cf. id.* § 512(c)(1)(A)(i)-(ii) (stating same proposition with regard to safe harbor for "[i]nformation residing on systems or networks at

essentially mirrors the basic test for contributory infringement, which allows liability if a defendant knows or has reason to know of infringing activity and materially contributes to that activity.[102] And the safe harbor also does not protect a provider who receives "a financial benefit directly attributable to the infringing activity" if the provider "has the right and ability to control such activity."[103] This, of course, is the basic test for vicarious liability, so if a plaintiff can establish the elements of a claim that the service provider is vicariously liable for its user's infringement, the 512(d) safe harbor will not limit the provider's liability pursuant to that claim.[104] The district court in the *Aimster* case took just this approach, treating the conditions on the 512(d) safe harbor as being identical to the elements of claims for contributory infringement and vicarious liability; because the *Aimster* court ruled that the defendant's conduct came within the scope of these secondary liability doctrines, it therefore concluded that Aimster's conduct was simultaneously outside the scope of protection of the safe harbor.[105]

Thus, to the extent that claims for indirect liability pose a threat to p2p innovations, the safe harbors for online service providers added to copyright law by the DMCA do little to ameliorate that threat. Combined with the uncertain application of the *Sony* doctrine to p2p digital innovations after the *Napster* and *Aimster* decisions and the loosening of the direct financial interest requirement for vicarious liability, suits seeking to hold digital innovators liable for infringements committed by users of their products and services have a substantial likelihood of success.

---

direction of users"). If an OSP acts "expeditiously" to stop its activity in connection with the infringing material once it gains such knowledge or awareness, then it retains the safe harbor's protection against liability. *Id.* § 512(d)(1)(C). But presumably in any contributory infringement case, a defendant who ceases her contribution to the infringing activity as soon as she acquires knowledge of or reason to know of the activity would face little or no liability for contributory infringement, since there would be little or no time in which she was both contributing and doing so knowingly, and both elements are required for a successful contributory infringement claim.

For a broader reading of Section 512(d) that would confer immunity even as to contributory and vicarious infringement, see 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT 12B.05[C] (2003).

102. The standard of knowledge that a provider must have to fall outside the protections of the safe harbor may be somewhat higher than the standard required in an ordinary action for contributory infringement, so the safe harbor may offer some incremental protection even against claims of contributory infringement.

103. 17 U.S.C. § 512(d)(2) (2004); *cf. id.* § 512(c)(1)(B) (stating same proposition with regard to safe harbor for "[i]nformation residing on systems or networks at direction of users").

104. Actually, the directness of the financial benefit a defendant must have in order to lose the protection of the safe harbor may be somewhat greater than the somewhat loosened "direct financial benefit" required by courts in ordinary cases to hold a defendant vicariously liable.

105. *In re* Aimster Copyright Litig., 252 F. Supp. 2d at 634, 655 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

II. THE ECONOMICS OF DIGITAL COPYRIGHT INFRINGEMENT

A. *What Has Changed?*

Why have copyright owners shifted from suing infringers to suing facilitators? The answer lies in a fundamental shift in the economics of copyright infringement in the digital environment. Copyright in the United States has always been seen principally as a utilitarian response to a public goods problem.[106] It costs more to create a work than it does to imitate someone else's work, and so, without some sort of control over imitation, creators will not have enough incentive to create.[107] But this public goods problem has always been an incomplete one. It was never the case that imitation was costless, only that it was cheaper than creation. An infringer who wanted to distribute counterfeit copies of a book, record, computer program, or videotape in the twentieth century needed the same sort of production and distribution facilities that the copyright owner did. Counterfeiters had to print books, press records, or record tapes or discs en masse and then find a way to ship those counterfeit copies to their own network of retailers, who had to be paid to sell the illegal copies. The costs of distributing any significant quantity of counterfeit copies might be somewhat less than the cost of legitimate distribution—the copies might be sold on a card table on a street corner rather than in a storefront—but counterfeiting required a substantial business of facilities and employees.

During most of the twentieth century, counterfeiters were also clearly distinct from individual end users. End users might also make copies without authorization from or payment to the copyright owner, and some of those end-user copies might be illegal.[108] But unlike counterfeiting, end-user copies weren't a serious threat to a copyright owner's sales during this period. End-user copies were often made for the copier's own personal use, often did not substitute at all for purchase of a lawful copy,[109] and were at worst only a very

106. *See, e.g.*, ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 10-18 (3d ed. 2003).

107. For an outline of this basic argument, see Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 994-99 (1997).

108. Most were not, however. End users have the right to make single temporary copies of broadcast television programs and movies for personal time-shifting use, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984), and the right to make an unspecified number of copies of CDs and cassettes for noncommercial use. 17 U.S.C. § 1008 (2004). More generally, the fair use doctrine likely protects much private, noncommercial copying of a work that doesn't directly substitute for purchases of the work. *See, e.g.*, JESSICA LITMAN, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET (2001). On the more general question of whether limited private copying by an end user infringes under the 1976 Act, see PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY 105-33 (2d ed. 2003).

109. For example, photocopying to replace damaged books and magazines or taping a

small source of substitution for lawful copies. They were not widely distributed: A college student might tape an album for a few friends but was unlikely to make several thousand tapes and give or sell them to strangers.[110]

Copyright owners in the twentieth century sued counterfeiters but generally did not sue end users even if they were making illegal copies. This made perfect sense given the economics of traditional copyright law. There were relatively few such counterfeiters, and the harm each one caused to copyright owners was large enough to justify spending the money to find them and shut them down. By contrast, a large number of end users were making copies. Many of those users were legitimate customers of the copyright owners. Many of those copies were legal, or at least of debatable legality. And in any event, the injury to copyright owners caused by any single end user was quite small, if not zero. Even if it was legally possible, it simply was not economically rational to stop the end users.[111]

The digital environment is quickly changing this calculus.[112] The great

record to listen to at work or in the car all involve copies made by a bona fide possessor who is merely making the copy in order to get better use of the copy already in her possession. Similarly, taping a television program to watch at a later time merely allows someone who has already been invited to view the program to do so on a different schedule.

110. *See* Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1488 (1995) (noting that copyright owners "traditionally avoided targeting end users of copyrighted works" primarily because end-user reproduction "was insignificant and rarely the subject of widespread further dissemination").

Further, many of these tapes did not in fact represent a lost sale to the content owner. Infringement can fill in for the deadweight loss caused by copyright by, for example, allowing those who are not willing to pay full retail price for a CD to acquire it illegally for less. The only economic cost to copyright owners comes from the subset of those who copy a work who would otherwise have paid full price for it. *See, e.g.*, Yannis Bakos, Erik Brynjolfsson & Douglas Lichtman, *Shared Information Goods*, 42 J.L. & ECON. 117 (1999); Julie E. Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799 (2000) [hereinafter Cohen, *Copyright and the Perfect Curve*]; Michael J. Meurer, *Copyright Law and Price Discrimination*, 23 CARDOZO L. REV. 55 (2001); David McGowan, Copyright Ethics and the DMCA (2003) (unpublished manuscript, on file with authors); Michael J. Meurer, Sharing Copyrighted Works and Patented Technology (2002) (unpublished manuscript, on file with authors), *available at* http://lawweb.usc.edu/cleo/workshops/01-02/meurer.pdf (last visited Apr. 3, 2004). It is for this reason that industry estimates of the cost of piracy tend to be inflated.

111. This is part of a more general point: Given resource constraints, the optimal level of infringement is likely greater than zero. We discuss this point in more detail below. *See infra* notes 192-96 and accompanying text.

112. For a comprehensive look at these changes, see Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2003). Some previous academic work has approached this change from the opposite direction, focusing on how legal rules written with the offline world in mind have not translated well to the digital world. These scholars generally seek to change the law to make it work online as much as possible like it worked offline. *See, e.g.*, Ann Bartow, *Electrifying Copyright Norms and Making Cyberspace More Like a Book*, 48 VILL. L. REV. 13 (2003); *cf.* Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 U. DAYTON L. REV. 547 (1997)

promise of digital dissemination—the virtual elimination of the costs of copy production and distribution[113]—is a mixed blessing for copyright owners. Content owner costs go down as they embrace digital dissemination[114] but so do the costs of counterfeiters. Indeed, as the costs of producing and disseminating copies approach zero, the public goods problem gets worse, because the *ratio* of the cost of creation to the cost of imitation approaches infinity.[115] Further, as the cost of producing and disseminating copies approaches zero, the sharp division between professional counterfeiters and end-user copiers breaks down.[116] Anyone can give copies of software or music to others on the Internet in a variety of ways: Put it on a Web page, email it to friends or to a listserv, swap it on Internet relay chat (IRC) or IM, or make it available for download on a p2p file-sharing service. It costs virtually nothing to do so. And unlike end-user copying in the analog environment, online copying by end users can be quite substantial. If I tape a CD to give to a friend, I have deprived the record company of at most one sale. If I post the CD online, thousands or tens of thousands of people might download the music, and the company might lose a large number of sales (though the actual magnitude of lost CD sales due to the availability of recordings online has been sharply disputed). This problem is exacerbated because it is much easier to make a

(describing ways to mimic the role of the first sale doctrine online). Our point in this Part is that the digital revolution changes the economic characteristics of the copyright industries, so that it may not always make sense simply to try to replicate what came before.

113. *See* Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 MICH. L. REV. 1570 (1995); Robert P. Merges, *Intellectual Property and Digital Content: Notes on a Scorecard*, CYBERSPACE LAW., June 1996, at 15. For skepticism that the Internet will actually reduce the costs of exchange, see J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, *in* INTERNET PUBLISHING AND BEYOND 6, 25 (Brian Kahin & Hal R. Varian eds., 2000).

114. Content owners have been slow to do so. The software industry is perhaps most willing to permit digital downloads. The music industry resisted digital content delivery for a number of years but, in 2002, finally put together joint ventures that made significant content available in easily accessible form. *See, e.g.*, Napster, http://www.napster.com (last visited Apr. 29, 2004); Pressplay, http://www.pressplay.com (last visited Apr. 4, 2004); MusicNet, http://www.musicnet.com (last visited Apr. 4, 2004). The publishing and video content industries have made few large-scale efforts to date to distribute content online.

115. As Dan Farber has pointed out to us, it is this ratio, not the absolute costs, that matters most in calibrating incentives. *Cf.* Dan L. Burk & Mark A. Lemley, *Policy Levers in Patent Law*, 89 VA. L. REV. 1575 (2003) (using a similar measure for patent incentives). At the extreme, the two measures converge.

116. *See* Dogan, *supra* note 21, at 90-92. On the precise nature of the infringement involved in transferring files over p2p networks, see R. Anthony Reese, *Copyright and Internet Music Transmissions: Existing Law, Major Controversies, Possible Solutions*, 55 U. MIAMI L. REV. 237, 258-59 (2001). We note that in many circumstances the division between counterfeiters and end users remains, even in the digital environment. Burning a copy of your own CD for personal use or to give to a friend is an example of digital end-user copying that is quite distinct from, and has far less impact than, professional counterfeiting or large-scale dissemination online. Our concern in this Article is with large-scale digital dissemination.

copy of digital content than it is to photocopy a book or tape a CD and, unlike photocopies or analog recordings, digital copies do not degrade in quality from generation to generation, permitting those who obtain copies to make perfect copies of the copies. The massive decline in the cost of copying has made large-scale end-user copyright infringement a more significant problem in the digital environment.

The economics of digital copyright have also rendered traditional solutions to counterfeiting obsolete.[117] The wide dissemination of copies made by end users over the Internet means that content owners can no longer ignore end-user copies and focus on professional counterfeiters. In order to stop large-scale infringement online, copyright owners must stop the end-user copies as well.[118] But it simply is not cost effective to sue each end user for copyright infringement.[119] Napster had seventy million users at its peak; estimates of usage for the various components of the Morpheus network are even higher.[120] Considering that it may cost as much as $250,000 for a copyright owner to take even a low-stakes copyright case to trial and final judgment,[121] suing even a

117. *See* Dogan, *supra* note 21, at 77.

118. Tim Wu makes essentially the same point, though he phrases it in terms of a shift from specialized copying "intermediaries" (in essence, publishers and distributors) to copying by end users. *See* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 685 (2003). We find it unhelpful to talk of traditional copyright law as a system of suing intermediaries. Copyright owners have long sued direct infringers rather than facilitators; it's just that the most important direct infringers until recently were large companies or other large-scale producers, not individual end users. We think the shift towards suing those who do not themselves directly infringe copyrights is therefore more significant than Wu's description might suggest. In part, Wu's point appears to depend on an unusual view that copyright law targets certain end uses of a work (listening to music and reading books). *Id*. at 711. Copyright law, though, has never controlled most of what a private end user does with a copy of a work; it has always focused attention on the copies that are made and distributed *to the public* or on the *public* performance or display of a work. *See* Ginsburg, *supra* note 110, at 1488; Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 34-39 (1994).

119. *See, e.g.*, Alfred C. Yen, *What Federal Gun Control Can Teach Us About the DMCA's Antitrafficking Provisions*, 2003 WIS. L. REV. 649, 652 (detailing the difficulties with such suits).

120. As of late 2002, the Kazaa software behind the Morpheus network had been downloaded 159 million times. *Direct Connect: The Best File Sharing Service?*, AXISNOVA.COM, Dec. 5, 2002, *at* http://www.axisnova.com/articles/021205_direct_connect.shtml (last visited Apr. 4, 2004). This doesn't necessarily translate into 159 million unique users, however, since users may download the file to more than one computer, and many may download the file without becoming ongoing users of the network.

121. The American Intellectual Property Law Association (AIPLA) survey of members finds the following median numbers of estimates of total costs of copyright infringement suits:

fraction of the end users could bankrupt the content industries.[122] It is also generally considered bad for public relations to sue your customers, and most people engaged in illegal file sharing also buy music legally.[123]

Copyright owners have understandably cast about for an alternative to suing end users. The strategy they have settled on is to sue facilitators. Suing facilitators is cost-effective for the content industries because a single lawsuit can eliminate the dissemination mechanism for a large number of end-user copies.[124] The *Napster* case, for example, shut down what was then the single largest forum for disseminating music online;[125] the music and movie industries now hope to do the same with other p2p networks such as Morpheus.[126] If copyright owners can shut off the distribution channels for

Low-Stakes Case	***(<$1 million)***
Thru Discovery	$101,000
Thru Trial and Appeal	$249,000
Medium-Stakes Case	***($1-$25 million)***
Thru Discovery	$298,000
Thru Trial and Appeal	$499,000
High-Stakes Case	***(>$25 million)***
Thru Discovery	$501,000
Thru Trial and Appeal	$950,000

AM. INTELL. PROP. ASS'N, 2003 REPORT OF ECONOMIC SURVEY 96-97 tbl.22 (2003). We have assumed that these figures represent the total costs of the suit to one side, not to both parties.

122. Based on the AIPLA figures for low-stakes cases, if the content industry were to sue seven million end users and take each case to trial, the cost could be over $1.7 trillion. Even under the much more realistic assumption that most of these cases would be resolved quickly without trial, and that the cost was only ten percent of the cost of going to trial, it would still have to spend nearly $170 billion in litigation costs. The costs to the court system would be similarly astronomical.

123. Yen, *supra* note 119, at 652; *cf*. Peter K. Yu, *The Escalating Copyright Wars*, 32 HOFSTRA L. REV. (forthcoming 2004) (manuscript at 18-19) (arguing that the decision to sue file-sharers was a mistake for the RIAA).

124. *See* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 397 (2003) (noting the "substantial enforcement and administrative savings" associated with suing facilitators). Lichtman and Landes also argue that "a lawsuit brought by one copyright holder against a service like Napster generates positive externalities that benefit all copyright holders," while a suit against an individual user does not. *Id*. at 408. This is not precisely correct, both because most suits against facilitators have been brought by a trade association representing all copyright owners, and because suits against individuals, like suits against services, will likely deter those individuals from sharing any copyright owner's files illegally. We do agree with Lichtman and Landes that suing facilitators is a more efficient way of stopping the harm of illegal file sharing than suing individuals. Unfortunately, as we discuss in the next Part, it is also a more efficient way of eliminating the positive benefits of those services.

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

126. More-attenuated facilitator suits have two analogous goals. One is to prevent access to websites that contain digital content by shutting down search engine or wireline connections to those sites; this is the theory behind the lawsuit against Verizon and threats to

digital content, they do not need to worry nearly as much about the low cost of making any given copy of that content. From their perspective, suing facilitators is a logical response to the changing economics of copyright law. Unfortunately, as the next Part illustrates, it is not a socially optimal response.[127]

ISPs. The other is to make investment in or assistance to new digital distribution companies risky; this is the rationale behind the lawsuits against Hummer Winblad and Cooley Godward, both of whom provide necessary infrastructure for start-up ventures.

127. In an important article, Ray Ku argues that digital dissemination technology has solved the principal public goods problem and eliminated the need for middlemen as disseminators of copyrighted works. *See* Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 266-68 (2002). If Ku is right, there is no justification for copyright protection at all in a digital world. We are skeptical of this position, however. While it may well turn out to be the case that digital dissemination mechanisms such as p2p networks can replace the physical movement of goods, they certainly have not yet done so. Despite massive downloading of music, CD sales have declined only somewhat, and to date DVD and book sales seem even less affected by digital dissemination. *See, e.g.*, Stan Liebowitz, *Policing Pirates in the Networked Age*, POL'Y ANALYSIS, No. 438, May 15, 2002, *available at* http://www.cato.org/pubs/pas/pa438.pdf (last visited Apr. 4, 2004) [hereinafter Liebowitz, *Policing Pirates*] (finding no significant decline in CD sales because of Napster but predicting such a decline in the future) ; Stan J. Liebowitz, Will MP3 Downloads Annihilate the Record Industry? The Evidence So Far (2003) (unpublished manuscript, on file with authors), *available at* http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID414162_code030627500.pdf?abstractid=414162 (last visited Apr. 5, 2004) (finding a decrease in music sales attributable to p2p file sharing, but not the collapse of the industry). There is still a demand for physical copies of works of authorship, and there likely will be for the foreseeable future—particularly for the sizeable minority of Americans who are still not online or do not have high-speed connections.

Even if digital dissemination fulfills the promise that Ku sees for it, we think copyright incentives will remain important. One need not agree with Samuel Johnson's quip that "no man but a blockhead ever wrote, except for money" to think that the incentives provided by copyright encourage a substantial amount of creativity. Ku argues that, at least for music, the ability to control sale of tangible copies is largely irrelevant to the incentive to create works of authorship, both because some people will create for nonmonetary reasons and because authors may be funded in other ways. Ku, *supra*, at 306-311. Ku is surely right to suggest that writers and artists create for a variety of reasons and that many would create without any hope of recompense. But fewer would do so, particularly in industries like Hollywood where production costs are substantial, and that additional creativity is what copyright is designed to encourage. Enabling copyright owners to eliminate large-scale infringement of their works over digital networks will likely remain an important element of that encouragement into the foreseeable future. Ku also proposes a general tax to generate revenue to be paid to artists. *Id*. at 311-15. This system has some similarities to the levy systems we discuss below. *See infra* Part III.B.1. We do not evaluate taxation as an alternative to copyright here, though we note that one significant advantage copyright has over a tax-based system is that it allows the market rather than the government to determine *which* works to encourage. For a parallel discussion of tax-based rewards versus intellectual property rights in patent law, see Michael Abramowicz, *Perfecting Patent Prizes*, 56 VAND. L. REV. 115 (2003) (advocating a reward system to complement existing intellectual property protection); John F. Duffy, *The Marginal Cost Controversy in Intellectual Property*, 71 U. CHI. L. REV. 37 (2004) (criticizing such systems); Netanel, *supra* note 29; Steven Shavell & Tanguy van Ypersele, *Rewards Versus Intellectual Property Rights*, 44 J.L. & ECON. 525 (2001) (concluding that

B. *What's Wrong with Suing Facilitators?*

1. *Lumping legal and illegal conduct together*.

Suing intermediaries and facilitators differs in fundamental ways from suing counterfeiters. A lawsuit against a direct infringer allows the court to make a determination about the accused infringer's conduct. A court holds an accused direct infringer liable only if it determines that she did in fact infringe. Any accused infringer can defend such a suit by arguing that she did not infringe, or that her infringement was justified or excused by a recognized defense. The same is true of certain types of indirect liability for infringement in the traditional copyright system. If I am held liable for inducing another to infringe, it can only be because the court has concluded that I had the required relationship with a party who is found to have infringed. The specific facts of the direct infringer's activities matter.[128]

Suits against third parties in the digital environment do not—indeed generally cannot—address specific conduct by particular end users. Suits against facilitators premised on individual cases of infringement would pose the same economic problem for copyright owners as suits against the individual infringers themselves.[129] Rather, the class of suits we consider in this Article involves efforts to shut down a facilitator entirely[130] or to require modification in the way the facilitator operates.[131]

---

an optimal reward system is more effective than intellectual property rights).

128. Other types of indirect liability, such as contributory infringement by device, lack this feature. Courts have been cautious about finding liability in such cases, however. *See supra* notes 36-41 and accompanying text.

129. In some digital dissemination contexts, suits against facilitators premised on individual cases of infringement may be efficient. For example, a suit against an ISP that is hosting a user's website with infringing content may result in the infringing content being removed, thus denying all other Internet users access to the content. In such cases, of course, the copyright owner is not seeking to eliminate entirely the facilitating service. The costs of such suits, however, suggest that copyright owners would have to bring them selectively, if they would in fact go to trial. In practice, the safe-harbor provisions of Section 512 of the DMCA, in light of the agency cost problem described *infra* Part II.B.4, may make the threat of such suits an efficient enforcement mechanism for copyright owners, though at the cost of having some noninfringing content—perhaps a considerable amount—removed from the Web.

130. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

131. Sometimes this latter set of claims seeks technical modifications in the way a service works. This was what the Ninth Circuit required in *Napster*. 239 F.3d at 1027. Sometimes it seeks to require a facilitator to seek out and block infringing content. This is the theory behind search engine cases such as *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002), and suits against auction sites such as Yahoo!. *See* Kelly Choi, *Big Suits: Yahoo! Copyright Litigation*, AM. LAW., June 2000, at 47. And sometimes the goal is to deter a facilitator from dealing with other facilitators that the content owners do not like. This

The problem with these claims is that they lack the granularity of suits against direct infringers. For example, in the *Grokster* case, the Central District of California had to decide either to ban the distribution of software that permits users to connect to the Morpheus network or not to ban it.[132] That essentially binary choice is ill-suited to the realities of the Morpheus network, over which individual end users trade lots of plaintiffs' content, trade some content that either is in the public domain or for which the copyright owner has given permission, trade some files of a type that tends not to be copyrighted at all, and trade significantly more content that might be copyrighted, but whose owner has neither granted permission for its use nor sought its removal by joining in the lawsuit. Lawsuits against end users can distinguish between those who post infringing content and those who do not. A lawsuit against the software maker cannot draw that distinction. And not surprisingly, lawsuits against facilitators are likely to be even worse at determining whether individual end users have made lawful use of the plaintiff's content, a fact-specific inquiry involving the acts and motivations of millions of people who are not parties or even witnesses in the case.

Thus, courts in the facilitator lawsuits are generally put to an unpleasant choice: They must either ban unquestionably lawful conduct in order to get at the infringing conduct or let the infringing content remain online in order to protect the legal trading of content. Neither alternative is particularly attractive as a general matter. The balance between the two harms will tilt different ways in different cases, however. The closer the facilitator's activities are to direct infringement and the more closely tailored the facilitator's system is to infringing content, the less collateral harm an injunction will cause to legitimate users.[133] At some point, though, as Lichtman and Landes note, "the benefits in terms of increased copyright enforcement come at too high a cost in terms of possible interference with the sale of a legitimate product."[134]

In *Napster*, for instance, the service was limited to the trading of music files by users, and the evidence submitted to the court suggested that at least 87% of the files traded, and perhaps as many as 99% of the files traded, were

explains copyright owner lawsuits against Bertelsmann and the venture capital firm of Hummer Winblad for investing in Napster, and Universal's suit against the law firm of Cooley Godward for advising mp3.com. *See supra* notes 11-12 and accompanying text.

132. A third possibility, that the court could itself supervise redesign of the software, seems infeasible and also an undesirable judicial intrusion into the innovation process. We do not discuss it in detail here. We discuss a fourth possibility, requiring the facilitator to screen content, *infra*, Part II.B.3.

133. Sonia Katyal warns against the dangers of lumping different facilitator business models together, a mistake that she argues plays into the hands of copyright owners who would lump all digital innovators together as pirates. *See* Sonia K. Katyal, *Ending the Revolution*, 80 TEX. L. REV. 1465, 1475-76 (2002). We are sensitive to this concern and emphasize that while we have modeled the impact of enforcement on innovation generally in this Article, actual assessment of the harm to innovation from banning any given technology is very much a function of the particular technology and its actual and potential uses.

134. Lichtman & Landes, *supra* note 124, at 397.

copyrighted by the plaintiffs.[135] Some of those copyrighted files were doubtless downloaded for purposes that the law would allow, but even so it seems reasonable to conclude that shutting down Napster stopped far more illegal conduct than legal conduct, at least under the patterns of Napster use at the time of the decision. As we move further away from services that seem particularly susceptible to infringement, however, the balance shifts. Unlike Napster, the Morpheus network permits the transmission of any type of file. While we have not seen definitive evidence on usage, it appears that the plaintiffs in *Grokster* own copyrights covering rather less than 75% of the content shared on the network.[136] Banning the distribution of software that allows users to connect to the Morpheus network would therefore stop more legal conduct and less illegal conduct than an injunction against Napster stopped. As lawsuits move further and further from the actual infringer in their effort to find a lever to stop infringement, the balance shifts even further against the copyright owner. Suits against ISPs or search engines are likely to target far more legal conduct than illegal conduct, and the net social harm to shutting such a facilitator down is correspondingly greater.

2. *Loss of the p2p dissemination network*.

p2p networks can be a particularly efficient means of disseminating content.[137] They often have several advantages over both the existing distribution networks for CDs and over the "top-down" online dissemination models such as MusicNet and Pressplay that have been implemented by content owners to date.[138] First, p2p networks are distributed, while authorized download sites tend to be more centralized. As a result, functioning p2p networks are less vulnerable to bandwidth constraints and the crash of a central server or servers, for the same reason that the Internet is resilient in avoiding

135. *Napster*, 239 F.3d at 1013 (citing A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 911 (N.D. Cal. 2000)).

136. The defendants in the *Grokster* litigation submitted abundant evidence of legal uses being made of their software. Some of the remaining content is clearly legal. Other content may be owned by parties who are not plaintiffs to the lawsuit.

137. *See* Matthew Fagin, Frank Pasquale & Kim Weatherall, *Beyond Napster: Using Antitrust Law to Advance and Enhance Online Music Distribution*, 8 B.U. J. SCI. & TECH. L. 451, 501-03 (2002); *see also* Simson Garfinkel, *Pushing Peer-to-Peer*, TECH. REV., Oct. 2003, *available at* http://www.technologyreview.com/articles/printversion/wogarfinkel 100303.asp (last visited Apr. 4, 2004); Reuters, *House Fights P2P Risks*, WIRED.COM, Oct. 8, 2003, *at* http://www.wired.com/news/politics/0,1283,60752,00.html (last visited Apr. 4, 2004) (noting increasing use of p2p networks by U.S. government; "The www.fedstats.gov page, for example, uses peer-to-peer techniques to pull statistics and information from computers in more than 100 different government agencies.").

138. The movie industry is less far along in implementing online distribution than the music industry, but the structure of movie ventures so far suggests that they will share this top-down feature with online music.

such problems.[139] Second, p2p file sharing is inherently responsive to content demands. The fact that consumers are also suppliers means that if a large number of people want to download the latest OutKast song, a large number of people are likely to make that song available for upload too, because uploaders by definition provide only the music they themselves download from others or rip from a CD. The music industry doesn't need to print more CDs or decide which songs have sufficient demand to support giving them server space to make this happen; it happens on its own. Third, p2p networks may affect the creation as well as the dissemination of works of authorship by facilitating what Yochai Benkler has called "peer production."[140] Finally, and most significantly, p2p networks harness volunteers providing essentially free computing resources.[141] Just as millions of users support the Search for Extraterrestrial Intelligence (SETI) by donating idle processing power,[142] p2p file sharers are donating their idle computer resources to the cause of music distribution.

One example of the potential advantages of p2p networks is a proposal for the British Broadcasting Corporation (BBC) Creative Archive. The BBC has announced plans to digitize its television archive and make the material available for private noncommercial use without charge. The BBC is considering using p2p networks in order to reduce its costs for the project:

> Why spend money on racks of hardware and fat pipes when your most popular files will be shared by your viewers, who will burn them onto DVDs themselves and create their own copies to match demand? . . . Even a partial archive would place an impossible burden on the BBC's infrastructure, so open licenses will make the Creative Archive possible.[143]

The efficiency of p2p networks might in this case make it possible for a

139. An empirical study of file sharing networks has found that their optimal size is bounded. At some point the benefits of having additional users supplying content are outweighed by the congestion costs of additional demands on the network. *See* Atip Asvanund, Karen Clay, Ramayya Krishnan & Michael D. Smith, An Empirical Analysis of Network Externalities in Peer-To-Peer Music-Sharing Networks (Sept. 2003) (unpublished manuscript, on file with authors), *available at* http://papers.ssrn.com/sol3/Delivery.cfm/SSRNID433780code030902670.pdf? abstractid=433780 (last visited Apr. 4, 2004). This suggests that the efficiencies described in the text are not automatic, but may be a function of the size of the network.

140. Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369 (2002) (discussing "production by persons who interact and collaborate without being organized on either a market-based or a managerial/hierarchical model" such as the Linux operating system and the Wikipedia online encyclopedia); Fagin et al., *supra* note 137, at 501-04.

141. The resources are not always free, of course. File sharers on college campuses may be using university computing capacity, and uploading will take bandwidth away from other uses.

142. SETI@HOME: THE SEARCH FOR EXTRATERRESTRIAL INTELLIGENCE, http://setiathome.ssl.berkeley.edu/ (last visited Apr. 4, 2004).

143. Danny O'Brien, *Something Completely Different*, WIRED.COM, Nov. 2003, at 30, *at* http://www.wired.com/wired/archive/11.11/start.html?pg=1 (last visited Apr. 4, 2004).

copyright owner who wants to make an enormous amount of copyrighted material available to the public at no charge to do so affordably.[144] Other examples of capitalizing on the efficiency of p2p networks include academic institutions, including MIT, Rice University, and the Berklee College of Music, that have made instructional materials available over such networks,[145] and software companies, including Microsoft, that have disseminated software over such networks.[146]

It is an unfortunate fact of modern life that this efficient dissemination mechanism is used to disseminate illegal rather than legal copies in many cases. But shutting down p2p networks to solve the infringement problem forces us in many cases to rely on a less-efficient mechanism for disseminating digital content.[147] This lost efficiency represents a cost to society, one that could be avoided if there were a way to harness the benefits of p2p networks in the service of legally disseminating content.

3. *Requiring the facilitator to police is not a solution*.

A court might try to get around these problems by enjoining the dissemination of infringing material on a facilitator's network, rather than shutting down the site altogether. The Ninth Circuit took this approach in *Napster*, seeing it as a compromise that preserved the legal uses of the network while stopping copyright infringement.[148] This approach echoes the increasingly common approach of building safeguards against copyright infringement into devices or into the network itself, an approach known as "digital rights management" (DRM).[149] Congress has also considered requiring

144. As another example, the company Red Swoosh offers p2p services to noncommercial filmmakers, game developers, and others interested in distributing large files to many people cheaply; one game developer who used the service reportedly saved $36,000 in one month on the dissemination of 18 terabytes of data. John Borland, *Legal P2P Networks Gaining Ground*, CNET NEWS.COM, Mar. 11, 2004, *available at* http://news.com.com/2100-1027-5172564.html (last visited Apr. 4, 2004).

145. Elizabeth Armstrong, *File-Sharing Goes to School*, CHRISTIAN SCI. MONITOR, Dec. 16, 2003, at 11.

146. Douglas Heingartner, *Software Piracy Is in Resurgence, with New Safeguards Eroded by File Sharing*, N.Y. TIMES, Jan. 19, 2004, at C9 (noting that Microsoft used the Kazaa network to disseminate its Windows Media Player 9 software).

147. Indeed, even the shift from Napster to the more decentralized programs in the Morpheus network involves some efficiency loss, because consumers don't get the benefits of a universal central directory. Ideally, innovation policy would be technology-neutral, rather than channeling innovation into one form or another.

148. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).

149. There is a voluminous literature on DRM and its potential problems. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace,* 28 CONN. L. REV. 981 (1996); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) [hereinafter Cohen, *DRM and Privacy*]; Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998); R.

device manufacturers to build in encryption and other tools to prevent infringement.[150]

Such an intermediate approach is unlikely to work, for several reasons. First, *Napster* itself is a caution. The district court ultimately went further on remand than the Ninth Circuit seemed to authorize, holding that Napster must design its system so that *no* infringing content can get through before being allowed to provide its users with access to noninfringing content.[151] The end result was that the parties fought for months about how to redesign the Napster system, and the system never went back online. The "intermediate" injunction was no different than an outright prohibition on the Napster system. Second, there will always be disputes over what content is infringing. Copyright law is full of gray areas,[152] and copyright owners have a history of trying to enforce the law beyond its bounds.[153] A court that decides to stop infringing content while letting the rest of the service continue either will have to enjoin all infringing content in advance (in which case no rational defendant will operate their system at all, for fear of going to jail for contempt) or will be signing up to resolve an endless series of oversight disputes about particular cases.

Third, and most important, the idea of enjoining only the infringing material presupposes control by the facilitator over the material that is disseminated on the system. Napster could in fact exercise such control, because it ran a central directory service that customers had to use in order to

Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997); Simson Garfinkel, *The Rights Management Trap*, TECH. REV., Nov. 2002, at 37, *available at* http://www.simson.net/clips/2002.TR.10.RightsManagementTrap.htm (last visited Apr. 4, 2004).

150. S. 2048, 107th Cong. (2d Sess. 2002). Congress imposed certain similar requirements in the Audio Home Recording Act of 1992, 17 U.S.C. § 1001-1010 (2004).

151. A&M Records, Inc. v. Napster, Inc., 2001 Copyright L. Decs. ¶28,213 (N.D. Cal. Mar. 5, 2001). The broader injunction was ultimately sustained on appeal. *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

152. *See, e.g.*, Dellar v. Samuel Goldwyn, Inc., 104 F.2d 661 (2d Cir. 1939) (Hand, J.) (lamenting the indeterminacy of the fair use doctrine); Sheldon v. Metro-Goldwyn Pictures Corp., 81 F.2d 49, 56 (2d Cir. 1936) (Hand, J.) (lamenting the indeterminacy of the substantial similarity test); Nichols v. Universal Pictures Corp., 45 F.2d 119, 121 (2d Cir. 1930) (Hand, J.) (lamenting the indeterminacy of the idea-expression dichotomy). As Jamie Boyle has put it, "in copyright law—to a greater extent than in most other fields of legal doctrine—there is a routine *and acknowledged* breakdown of the simplifying assumptions of the discourse, so that mundane issues force lawyers, judges, and policy-makers to return to first principles." JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 19 (1996).

153. *See, e.g.*, Suntrust Bank v. Houghton Mifflin Co., 268 F.3d 1257 (11th Cir. 2001) (plaintiff sought to enjoin parody of *Gone With the Wind*); Litchfield v. Spielberg, 736 F.2d 1352 (9th Cir. 1984) (plaintiff sought to enjoin movie *E.T.* as a derivative work based on script that was not substantially similar); Scholastic, Inc. v. Stouffer, 221 F. Supp. 2d 425 (S.D.N.Y. 2002) (plaintiff sought to enjoin Harry Potter books based on minimal similarities to her books), *aff'd*, 81 Fed. Appx. 396 (2d Cir. 2003).

find music on the system. The same cannot be said of most other facilitators, however. Sony has no control over the uses to which its VCRs are put. Companies such as StreamCast and Grokster sell software written by others and used by individuals who make files available on the Morpheus network; they apparently have no ability to remove certain files (or users) from the network and retain others.[154]

Technology that filtered and blocked unauthorized copying of copyrighted works over p2p networks but that allowed copying of public domain material or where authorized by the rightsholder or the Copyright Act would be a welcome solution to the problem of protecting the interests of copyright owners without stifling the deployment and development of p2p networks. Past efforts to implement such a solution, though, have not been promising, and the various parties to file-sharing controversies remain sharply divided over the feasibility of such filtering solutions.[155]

4. *Agency cost problems*.

Even if it were feasible, the idea of compelling facilitators to stop some but not all content would likely not be socially optimal because facilitators do not have the proper incentives to distinguish lawful from infringing content in their filtering. Assaf Hamdani and others have noted that third parties are too quick to take down material posted on their Internet sites by others when they receive a complaint of copyright infringement.[156] ISPs, auction sites, search engines,

154. Similarly, Jon Johansen cannot somehow make DeCSS available only to those who want to use it to view DVDs on a computer but keep it from those who want to make illegal copies of a DVD. (On DeCSS generally, see Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).) Courts will instead be inclined to preclude all uses of circumvention technology, including legal ones, as they did in the *321 Studios* cases. *See* Paramount Pictures Corp. v. 321 Studios, No. 03-CV-8970, 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004); 321 Studios v. Metro-Goldwyn-Mayer Studios, No. C 02-1955-SI, 2004 WL 415250 (N.D. Cal. Feb. 19, 2004). Indeed, for programs already written and released, like DeCSS or Gnutella, the author may lose all control whatsoever over the distribution and use of the program. An injunction against distributing an already widely distributed computer program is likely to prove futile, as the easy availability of DeCSS despite the court's injunction upheld in *Corley* demonstrates.

155. *See, e.g.*, John Borland, *File-Swap "Killer" Grabs Attention*, CNET NEWS.COM, Mar. 3, 2004, *at* http://news.com.com/2100-1025-5168505.html (last visited Apr. 4, 2004); John Borland, *P2P Companies Say They Can't Filter*, CNET NEWS.COM, Jan. 28, 2004, *at* http://news.com.com/2100-1038-5149720.html (last visited Apr. 4, 2004) (discussing dispute over feasibility of filtering); John Borland & Stefanie Olsen, *Napster's Fanning Has Snocapped Vision*, CNET NEWS.COM, Jan. 23, 2004, *at* http://news.com.com/2100-1025-5146858.html (last visited Apr. 4, 2004) (discussing differing views over likely success of audio fingerprinting software under development by company that employs Napster creator Shawn Fanning); John Schwartz, *A Software Aimed at Taming File-Sharing*, N.Y. TIMES, Mar. 8, 2004, at C7.

156. *See, e.g.*, Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002); Matt Jackson, *The Digital Millennium Copyright Act of 1998: A Proposed Amendment to Accommodate Free Speech*, 5 COMM. L. & POL'Y 61, 63 (2000); Malla

wireline providers, and other intermediaries capture only a tiny part of the value of a third-party posting. If the third party pays a flat rate, the intermediary may not in fact suffer any financial consequence from removing a particular posting or link. Indeed, the problem of automatic takedown is so great that when Congress passed the safe harbor for OSPs in the DMCA, it felt compelled to require OSPs to put back disputed content under certain circumstances if their customers complained about it being taken down.[157] The fact that these intermediaries do not bear the full social cost of taking down challenged content means that enforcing copyright law by requiring them to do so creates negative externalities, tilting the law too far in favor of copyright owners.[158]

5. *Harms to innovation*.

Another, potentially even more corrosive, problem with suing facilitators is the danger such suits pose for technological innovation. Traditional copyright suits against direct infringers do not directly threaten technological innovation, since they target only the infringing user of that innovation.[159] Suits against facilitators, by contrast, seek to outlaw a service entirely or to declare a device or program contraband. Banning the sale of a device or computer program obviously restricts innovation directly, and therefore reduces social welfare by the net social value of that innovation. For example, if the courts declare p2p networks illegal altogether (or indirectly do so by ordering modifications and filtering that result in the networks shutting down), the social cost will not only

Pollack, *The Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment*, 17 CARDOZO ARTS & ENT. L.J. 47, 109 (1999) ("The safe harbor provision is a strong incentive for OSPs and ISPs to censor their users at the mere request of allegedly aggrieved right holders."); Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 243 (2002); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1836, 1886-87 (2000). *But see* Matthew Kane, *Copyright and the Internet: The Balance Between Protection and Encouragement*, 22 T. JEFFERSON L. REV. 183, 197 (2000) (arguing that Section 512 draws a fair balance).

157. 17 U.S.C. § 512(g) (2004). The problem persists in spite of the balance in the statutory language. *See, e.g.*, Amy Tsui, *FatWallet Attorney Wants ISP Community to Take Stand Against Abusive Use of DMCA*, 8 ELEC. COMM. & L. REP. 9, 10 (2003) (quoting Megan Gray).

158. *See* Hamdani, *supra* note 156 (making this point in detail).

159. Traditional copyright suits can restrain innovation in particular works of authorship. Where a defendant has borrowed from or built on a previous copyrighted work without authorization, a plaintiff may obtain an injunction effectively suppressing the defendant's work, though the defendant would be free to continue to use any part of her work that is not infringing. This restraint, though, operates only against particular works of authorship, rather than against a technology that can be used with entire categories of works. The difference is between restraining a particular unauthorized film version of the novel *The Lord of the Rings* and restraining a device on which any film (or perhaps any work in digital format) can be viewed or copied.

be the foregone legal uses of those networks at the time they are enjoined but also the unanticipated future benefits those networks could have brought. Economic evidence strongly suggests that those unanticipated future benefits, or "spillover" effects, often exceed the immediate value of most new technologies.[160] The VCR is an obvious example of a technology that the copyright industries tried to ban[161] but that later developed in unanticipated ways, creating new markets that have provided tremendous benefit to the very copyright owners who would have outlawed it.[162] The early history of radio offers a similar lesson.[163]

The alternative discussed above—requiring programmers to change their products to build in screens against illegal copying—is little better, because it puts the courts or Congress in the untenable position of dictating to programmers how they should design their products. Innovation works best when it is as unfettered by governmental requirements as possible, particularly the kind of detailed oversight that the *Napster* case ultimately entailed. Courts are quite properly reluctant to dictate the design of products, and the law generally does so only where public health or safety is at stake (such as with

160. *See, e.g.*, RICHARD R. NELSON & SIDNEY G. WINTER, AN EVOLUTIONARY THEORY OF ECONOMIC CHANGE 130 (1982); ANNALEE SAXENIAN, REGIONAL ADVANTAGE: CULTURE AND COMPETITION IN SILICON VALLEY AND ROUTE 128 (1994); Carol Haber, *Electronic Breakthroughs: Big Picture Eludes Many*, ELECTRONIC NEWS, June 13, 1994, at 46 (detailing numerous examples of fundamental inventions that the inventor herself did not fully appreciate); Nathan Rosenberg, *Factors Affecting the Diffusion of Technology*, 10 EXPLORATIONS IN ECON. HIST. 3 (1972). Among the inventors who did not recognize the potential of their ideas are Marconi, who expected the radio to be used only for point-to-point communications rather than mass broadcast; the inventors of the transistor, who anticipated its use in hearing aids; and the inventors of the VCR, who anticipated it would only be used by television stations. *Id*.; *cf.* Michael A. Carrier, *Unraveling the Patent-Antitrust Paradox*, 150 U. PA. L. REV. 761 (2002) (arguing that innovation should be the paramount concern in setting intellectual property policy, albeit in a different context).

161. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984). For a discussion of the history of the VCR litigation, see JAMES LARDNER, FAST FORWARD: A MACHINE AND THE COMMOTION IT CAUSED (rev. ed. 2003). Doug Lichtman has argued to us that copyright owners would never have banned the VCR even if they had won, since there was a way to make money from it. We are not as sanguine about what the outcome would have been as he is. The industry fought hard to stop a new method of making copies it considered illegal; there is no reason to believe it would have been foresighted enough to embrace the technology despite its determined efforts to halt it. Further, even if the industry had come out with a "licensed VCR," perhaps with copy protection, we are skeptical that it would have worked as well or been as successful as the unapproved product was. The history of technologies over which copyright owners obtain early control is not promising—ask (if you can find them) owners of digital audio tape decks, dual-deck VCRs, laserdiscs and Divx machines.

162. *See* LARDNER, *supra* note 161. Lardner notes Jack Valenti's now infamous statement to Congress that "the VCR is to the American filmmaker and the American public as the Boston Strangler is to a woman home alone." *Id*. at 1 (quoting Jack Valenti).

163. *See, e.g.*, GOLDSTEIN, *supra* note 108, at 57-60; LITMAN, *supra* note 108, at 42-48 (discussing efforts by copyright owners in the 1920s to control the playing of music over radio).

airbags in cars or pharmaceutical composition) and at a level of generality much higher than that involved in the typical dispute over individual copyrighted works.[164]

Over and above the direct restrictions on innovation, the threat of lawsuits or criminal prosecutions against innovators is likely to deter a significant amount of innovation, some of which would unquestionably have been legal.[165] The anecdotal evidence of such deterrence is quite strong. When programmers started being prosecuted criminally for writing code that violated the DMCA's anticircumvention provisions,[166] and online magazines were sued for writing stories that linked the reader to allegedly unlawful sites,[167] the result was to chill programming, deterring some from working on encryption at all and steering others away from work in certain areas perceived as sensitive.[168] A number of programmers went so far as to file suits against the content industries, seeking declaratory judgments that their conduct was lawful.[169] Litigation is expensive, uncertain, and time-consuming; the fact that computer scientists wanted to go to court to gain the assurance that they wouldn't be prosecuted suggests that they were quite worried about what would happen if they continued to innovate. Lawsuits against direct infringers might deter conduct close to infringement, but they do not deter technological innovation, except to the extent that innovation is funded only or overwhelmingly by infringing activity. But lawsuits against facilitators directly deter innovation that might facilitate legal uses as well as infringement.

164. Courts have recognized their limits in mandating technical design. *See, e.g.*, United States v. Microsoft Corp., 147 F.3d 935, 949-50 (D.C. Cir. 1998).

165. *See, e.g.*, Fagin et al., *supra* note 137, at 500 ("Innovation in the technologies of distribution will decline markedly if potential new innovators are chilled by a threat of legal action."); Randal C. Picker, *Copyright As Entry Policy: The Case of Digital Distribution*, 47 ANTITRUST BULL. 423, 452 (2002) ("There is little reason for an outsider to innovate in distribution if it will be blocked at the moment that it needs content."). Indeed, some of the recent copyright infringement lawsuits filed on a theory of tertiary liability have little other evident purpose than to try to deter third parties such as venture capitalists from funding innovation that threatens copyright owners.

166. *See, e.g.*, United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002); *Norwegian Teenager Jon Johansen Acquitted in DVD Case*, Jan. 7, 2003, *at* http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20030107_eff_pr.html (last visited Apr. 4, 2004) (describing the prosecution and acquittal of Jon Johansen in Norway for writing DeCSS).

167. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); David McGowan, *From Social Friction to Social Meaning: What Expressive Uses of Code Tell Use About Free Speech*, 64 OHIO ST. L.J. 1515 (2003).

168. Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501 (2003).

169. *See, e.g.*, 321 Studios v. Metro-Goldwyn-Mayer Studios, Inc., No. C 02-1955-SI, 2004 WL 415250 (N.D. Cal. Feb. 19, 2004) (complaint *available at* http://www.eff.org/IP/DMCA/20021220_321_studios_complaint.pdf (last visited Apr. 4, 2004)); Edelman v. N2H2, Inc., 263 F. Supp. 2d 137 (D. Mass. 2003) (complaint *available at* http://archive.aclu.org/court/edelman.pdf (last visited Apr. 4, 2004)); Felten v. Recording Indus. Ass'n of Am., No. 01-CV-2669 (D.N.J. filed Nov. 28, 2001).

A final threat to innovation is more systematic. Courts can see the advantages of well-established technologies, even if those technologies also facilitate infringement. No court is likely to ban unlicensed printing presses, photocopiers, or computers, even though doing so might be a much more effective way of dealing with piracy than suing counterfeiters. The social value of printing presses, photocopiers, and computers has become quite clear over time. Further, they have become accepted as a part of the status quo, and banning them would look like a social disruption. The same is likely true of the VCR: While it narrowly escaped being declared contraband in 1984, it is highly unlikely that any Supreme Court justice would vote to outlaw the VCR today.

New technologies, by contrast, are much more vulnerable to legal challenge. In part this is because their ultimate value may not yet be clear; as noted above, the VCR is a good example of a technology that turned out to have substantially more value to society than was originally perceived. It is also because stopping the deployment of a new technology will not cause the disruption of settled expectations that rooting out an existing technology would.[170] When courts shut down new technologies, the world may literally never know what it is missing.[171]

Traditional copyright law dealt with the risk of harm to innovation in the same way patent law still does: by sharply cabining the circumstances in which copyright owners could sue makers of technology. The *Sony* decision set an intentionally tough standard for such suits; even if the seller of a device was otherwise guilty of contributory infringement, the court would ban a technology only if the technology was not even capable of a substantial noninfringing use.[172] Recent developments have significantly undermined this

170. As Niccolo Machiavelli put it, "an innovator has as enemies all the people who were doing well under the old order, and only halfhearted defenders in those who hope to profit from the new." NICCOLO MACHIAVELLI, THE PRINCE 17 (Robert M. Adams trans., W.W. Norton & Co. ed. 1992) (1513).

171. This is why we disagree with Lichtman, Landes, and Picker's argument in favor of a weighing of costs and benefits under which any software that has greater harms than benefits would be illegal. They argue that the *Sony* standard is mistaken because it permits the sale of products that have some benefits but greater harms. *See* Lichtman & Landes, *supra* note 124, at 400-01; Picker, *supra* note 165, at 444-45. The problem with any strict balancing of costs and benefits is that the benefits to innovation are likely to be unanticipated and are likely to benefit others, not just the innovator. All three scholars acknowledge this possibility. Lichtman & Landes, *supra* note 124, at 401; Picker, *supra* note 165, at 445. Thus, any effort to weigh the two at the beginning of the innovation process will unfairly discount the social value of innovation.

Lichtman and Landes also argue that making facilitating technologies illegal will give innovators an incentive to modify the technology in ways that reduce its harm, while *Sony* creates no such incentive. Lichtman & Landes, *supra* note 124. This may or may not be true in any given case; in many cases the features of the technology that benefit society are precisely the ones to which the copyright owner objects. In any event, we are less comfortable than they with putting courts in the position of dictating how innovation should occur.

172. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

rule, however. The DMCA's anticircumvention provisions expressly rejected the "substantial noninfringing use" test in favor of one much more generous to copyright owners.[173] And in *Napster* and *Aimster*, the courts appear to have radically rewritten the *Sony* test in a way that may render it impossible to satisfy in virtually any case, including *Sony* itself.[174] The result is that so far, at least, courts in digital copyright cases have shown little hesitation about banning technologies that clearly have at least some social value.[175]

Suing facilitators reduces technological innovation.[176] By the very nature of innovation, it is hard to quantify this harm.[177] But it surely exists, and it must be added to the social harm caused by banning existing legal uses in evaluating the economic effects of permitting suits against facilitators.

C. *What's the Alternative?*

The arguments in the preceding subparts seem to create a classic policy tradeoff: Suing facilitators is much more cost-effective than suing direct infringers in the digital world, but it also causes social harm. In order to decide whether suing facilitators made policy sense, the traditional approach would be to try to compare the magnitude of the benefit to the magnitude of the harm.[178]

---

173. Under the DMCA's test, a circumvention device is illegal if it is primarily designed or produced in order to aid infringement, if it is marketed for that purpose, *or* if it has only limited legal purposes. 17 U.S.C. § 1201(a)(2), (b) (2004).

174. *See supra* text accompanying notes 42-64.

175. *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); UMG Recordings, Inc. v. mp3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000). *But see* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

176. In an innovative and insightful article, Neil Netanel has proposed that the current system of suits against facilitators could be replaced with a system of levies—effectively, taxes charged on the sale of devices that can be used to infringe copyright and paid to copyright owners. *See* Netanel, *supra* note 29. We discuss this levy proposal, along with one by Terry Fisher, in Part III.B.1, *infra*.

177. We are sensitive to David McGowan's concern that arguments about promoting or retarding progress are easy to make and hard to quantify, though we are less inclined than he is to throw up our hands and call everything indeterminate. David McGowan, *Copyright Nonconsequentialism*, 69 MO. L. REV. 1 (2004). We agree that efforts such as Joseph Liu's to quantify harms of this sort are a good thing. *See* Liu, *supra* note 168. We caution, though, that the loss of future innovation is something that it may simply not be possible to identify with precision.

178. Jane Ginsburg argues that copyright owners should end up with the power to control Internet innovation because she believes this power will encourage the creation of more works of authorship. Jane C. Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613 (2001). While there may be some positive effect on creativity, as Ginsburg suggests, we think it needs to be weighed against the significant social costs of the control over technological innovation that she proposes. And as Jessica Litman points out, the empirical evidence to date is against Ginsburg's argument—content owners have promised for years to put content online if they got the laws they wanted, but they didn't do so until they started losing online copyright cases. Jessica Litman,

David McGowan may well be right that this is an inquiry that will never have a definitive answer.[179]

We do not have to ask the question, however, if there are alternatives to suing facilitators that are cost-effective but do not create the same social problems. In exploring potential alternatives, it is helpful to start with the basic economics of deterrence. The foundational work in this field is Gary Becker's analysis of the economics of criminal law.[180] Becker's insight is that a rational actor will adjust her behavior in response to the *expected* sanction—that is, the penalty that she will pay if caught multiplied by the probability that she will be caught.[181] If the punishment for a particular bad act (say burglary) is set equal to the defendant's gain from that act, the act will not be deterred unless the chance of being caught is one hundred percent. The intuition is simple: If the only cost to being caught is having to give up what you stole, a rational criminal will commit a burglary if there is any chance she might get away with it.[182] The corollary is that the more the sanction exceeds the defendant's gain from her conduct, the more rational actors will be deterred from engaging in crime, even if they are less likely to be caught. If our burglar must pay a fine that is ten times what she stole, she would be wise not to steal even if there is only a ten percent chance of being caught.[183] Indeed, Kaplow and Shavell extend Becker's analysis by pointing out that from a cost-benefit perspective, the maximum possible sanction is the optimal one because it requires the fewest resources to implement.[184]

Becker's fundamental insight focuses on the chance of detection and the magnitude of the sanction. Because he is working primarily with criminal law, this approach makes sense: Those are the likely variables.[185] To apply his model to digital copyright infringement, where private actors are the most likely enforcers, we need to make a few modifications.

First, detection is not as much of a problem in the online copyright environment. While crimes are normally concealed, online copyright

Sharing and Stealing (Feb. 6, 2004) (unpublished manuscript, on file with authors).

179. *See* McGowan, *supra* note 177. McGowan's conclusion, however—that we should abandon utilitarian analysis in favor of a strong copyright law based on Lockean labor theory—is not one to which we subscribe. And even McGowan acknowledges that at least some p2p file sharing produces net gains in welfare. *Id*. at 11.

180. Becker, *supra* note 28.

181. *Id*. at 176-179.

182. *Id*.; *see also* I. Trotter Hardy, *Criminal Copyright Infringement*, 11 WM. & MARY BILL RTS. J. 305, 312-13 (2002).

183. The deterrence effect of punitive sanctions is magnified to the extent that the targets are risk-averse, as most people are, and reduced to the extent they actually prefer risk.

184. Louis Kaplow & Steven Shavell, *Accuracy in the Determination of Liability*, 37 J. L. & ECON. 1 (1994).

185. Most defendants plead guilty or are convicted, so likelihood of acquittal is not much of a factor relative to likelihood of apprehension. In addition, the government is relatively insensitive to the transactions costs of prosecution. *See infra* note 187.

infringement generally is not. Indeed, one of the overlooked benefits of the Internet for copyright owners is the ability it gives them to find infringers who would otherwise remain hidden. Copyright owners are unlikely ever to catch an end user who makes a photocopy of a book, and it is even hard (though certainly not impossible) to detect traditional counterfeiters. By contrast, a large percentage of the copyright infringement that occurs online is publicly searchable,[186] and copyright owners can more easily identify infringers. In applying the deterrence model to the digital environment, likelihood of enforcement substitutes for likelihood of detection. Copyright owners can find online infringers, but for the reasons we discussed in Part II.A they have generally proven themselves unwilling to sue those infringers. Becker's point applies with equal force to potential defendants who know they will be "caught" but who do not expect to be called to account for their behavior.

Enforcement against infringing end users has been unlikely in the digital copyright environment because copyright owners would have to bear a litigation cost that exceeds the likely return to a lawsuit. Becker's framework largely ignores the transactions costs of litigation, because government enforcement is not sensitive to litigation cost in the same way that private litigants are.[187] The cost of litigation affects the likelihood of private enforcement, though, and so the probability of "detection" in Becker's framework is in fact a function of the costs of enforcement.[188]

The second modification to Becker's model concerns the costs of prevention. Becker takes the background environment—the architecture of a city, for instance—as a given. As Joel Reidenberg and Larry Lessig have made clear, however, that background environment is mutable online.[189] Copyright owners who want to stop digital infringement need not sue more infringers or raise the sanction on infringers if they can change characteristics of the Internet itself in a way that makes copyright infringement more difficult. One way to do this is to build copy controls into the digital media themselves. This sort of digital rights management is increasingly common. Another way to change the

186. Websites and p2p networks are searchable. Emails to friends and infringement over IRC are harder to detect, but they also involve smaller networks of copies and therefore cause less harm than the wider nets of infringement. On the potential for shielding online infringement from public view, see *infra* Part III.D.

187. The cost of enforcement does play a significant role in detection: Police may simply not devote the resources to investigating certain types of crimes. But when suspects are arrested, it is rare for authorities not to prosecute solely because of resource constraints. Those constraints, though, may affect *how* authorities pursue a case, in particular whether to accept a plea bargain or proceed to a full trial.

188. The point is actually a bit more complicated than indicated in the text. Transactions costs affect private enforcement decisions where they dissipate the expected gains from litigation. As the sanction increases, therefore, the likelihood of private litigation may also increase.

189. *See, e.g.*, LESSIG, *supra* note 149; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

Internet environment is to sue facilitators. If copyright owners can shut down p2p networks, or can enlist ISPs and search engines to filter their users' content for copyrightable material, they may not need to enforce their copyrights directly at all. The closest parallel to the traditional theory of crime would be a change in the architecture of a city—say, the creation of a gated community. Efforts to change the Internet itself by suing those who build or run pieces of it offer an alternative way to modify behavior in Becker's model.

Our modified analysis of the economics of deterrence suggests that there are several different legal ways to attack the problem of infringement in the online environment. First, copyright owners can try to limit the ability of users to engage in infringement by changing the characteristics of the Internet itself. This is the approach they have taken so far by suing intermediaries.[190] Second, copyright owners can try to deter infringement by raising the effective cost to the infringers when they are caught, which would require enforcement efforts against some end users and either requiring those infringers to pay significant monetary judgments or imposing a nonmonetary penalty such as jail time. Third, copyright owners can try to stop infringement by increasing the likelihood that infringers will be sued, which would require enforcement efforts against many end users. As we have seen, this means finding a way to reduce the cost of enforcement to the copyright owner. Economic theory suggests that copyright owners should be indifferent among these approaches at some level; the level of sanction or enforcement can in theory be set to achieve any particular level of deterrence. As we have seen, however, social welfare is *not* indifferent between these approaches. Suing facilitators imposes collateral social costs that can be avoided either by raising effective sanctions or by lowering the cost of enforcement.[191]

In Part III, we explore these alternatives in detail. Before we do, it is worth emphasizing that the goal of any approach is not the elimination of infringement. Infringement has always been a feature of the intellectual property landscape.[192] Indeed, the United States started life as a pirate nation,[193] and the content industries have long complained about the billions of dollars in revenues lost to piracy every year.[194] Yet those same industries have

190. A parallel approach is to implement DRM or encryption in an effort to make it technologically more difficult for users to make copies. Because this is a technological rather than a legal option, and because it has been discussed in detail elsewhere, we do not evaluate it here. For discussions of DRM, see *supra* note 149 (citing the relevant sources).

191. Direct enforcement may create its own social costs, of course. We discuss those costs *infra* notes 228-45 and accompanying text.

192. *See, e.g.*, BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT 8-9 (1967).

193. *See, e.g.*, JAMES J. BARNES, AUTHORS, PUBLISHERS AND POLITICIANS: THE QUEST FOR AN ANGLO-AMERICAN COPYRIGHT AGREEMENT, 1815-1854 (1974) (describing this history in detail); ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT: CASES AND MATERIALS 9, 10 (2000) (describing the United States as a "pirate nation" for the first century of its existence).

194. *See, e.g.*, Reuters, *Software Piracy Costs Billions*, June 16, 1998, *at*

survived and even thrived despite significant piracy. The content industries have never had or needed perfect control over infringement. They merely need enough control to give them sufficient incentive to create new works.[195] This is not to condone piracy or say that it should not be minimized to the extent possible. Rather, it is to make the point that weeding out all infringement simply isn't cost-effective. To try to give copyright owners perfect control would impose dramatic social costs to gain dubious benefits.[196] In the context of online copyright infringement, the real policy question is how to bring infringement down to a manageable level akin to the rate of infringement in the traditional copyright environment, particularly if this is done in conjunction with making available attractive and reasonably priced legitimate online dissemination alternatives.

http://www.wired.com/news/business/0,1367,13019,00.html (last visited Apr. 4, 2004) (reporting that the software industry claimed losses of $11.4 billion to piracy in 1997); Finlo Rohrer, *The Record Industry's Thorniest Issue*, BBC NEWS, Aug. 27, 2002, *at* http://news.bbc.co.uk/1/hi/entertainment/music/2220117.stm (last visited Apr. 4, 2004) (reporting that the music industry claimed losses of over $4 billion in 2001). As noted above, *see supra* note 110, these claims are likely to be significantly inflated.

195. *See, e.g.*, Lawrence Lessig, *Intellectual Property and Code*, 11 ST. JOHN'S J. LEGAL COMMENT. 635, 638 (1996) (noting that "sufficient incentive . . . is something less than perfect control"); Lance Rose, *The Emperor's Clothes Still Fit Just Fine*, WIRED, Feb. 1995, at 103 (noting that copyright owners have never needed to eliminate piracy in order to stay in business, just to control it). Even the head of the RIAA has acknowledged publicly that some infringement will always be a part of the Internet, and that their goal is to constrain rather than to eliminate it. Darren Waters, *Illegal Music Sites "Here to Stay"*, BBC NEWS, Jan. 8, 2003, *at* http://news.bbc.co.uk/2/hi/entertainment/2636235.stm (last visited Apr. 4, 2004); *see also* Saul Hansell, *Crackdown on Copyright Abuse May Send Music Traders into Software Underground*, N.Y. TIMES, Sept. 15, 2003, at C1, C3 (reporting that the "stated purpose of the [RIAA's] lawsuits is not to catch every hard-core music pirate, but to show millions of casual file sharers that what they are doing is illegal"); Roger Parloff, *The Real War over Piracy*, FORTUNE, Oct. 27, 2003, at 148, 152 ("'We have no illusion of ever getting rid of piracy entirely,' responds David Kendall, the studios' lead counsel in the [MGM v. Grokster] litigation . . . . The goal, Kendall explains, is to shut down the commercial services, which are more user-friendly than the complicated noncommercial methods employed by techies. . . . 'We're just trying to make file sharing harder for users than legitimate alternatives,' he says, referring to the licensed online music services that are now proliferating and improving.").

196. A detailed explication of this point is beyond the scope of this Article. Here, two points will suffice. First, stopping all copyright infringement would require the effective elimination of privacy, not only in the digital realm but in all aspects of our life. *Cf.* Cohen, *DRM and Privacy, supra* note 149 (discussing the relationship between copyright enforcement and privacy). Second, at least some infringement is engaged in by users who would not purchase the work at the prevailing price, but who are willing to pay more than the marginal cost of making another copy. These users are part of the deadweight loss caused by copyright; infringement by these users actually enhances social welfare. Bakos et al., *supra* note 110; Cohen, *Copyright and the Perfect Curve*, *supra* note 110; McGowan, *supra* note 110.

III. EXPLORING ALTERNATIVES TO SUING FACILITATORS

In this Part, we consider two alternatives to suing facilitators in the particular context of p2p file sharing. These alternatives build on the theoretical options taken from our modified Becker model: (1) raising the sanctions actually imposed on large-scale infringers and (2) lowering the costs of copyright enforcement against those infringers.[197]

A. *Raising Effective Sanctions*

In the traditional economics of deterrence, raising the sanction is a simple matter of increasing the legislated or judicially imposed penalty for a particular offense. With digital copyright infringement, things are a bit different. Copyright law already includes substantial supracompensatory sanctions in both civil and criminal law. Any copyright infringer—even one who acts innocently[198]—can be held liable for statutory damages in lieu of actual damages at the plaintiff's sole election.[199] Those statutory damages normally range from $750 to $30,000 per work copied at the factfinder's discretion.[200] The court has the discretion to lower the amount to $200 per work for innocent infringers and to raise it to $150,000 per work for willful infringers.[201]

These damage amounts reflect recent increases by Congress and dealing with large-scale infringement over p2p networks offers no reason to raise these damage amounts further.[202] Because the most likely targets of a civil lawsuit in the p2p context are the "keystone" uploaders, who often have several hundred

197. Glynn Lunney has briefly offered a similar suggestion for addressing private copying generally: Increasing the penalties for copying in order to deter it or reducing the transaction costs of infringement enforcement in order to "bring more private copiers within the law's reach." Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 851-52 (2001).

198. One who commits copyright infringement is civilly liable regardless of the mental state with which she acts. *See* Lipton v. Nature Co., 71 F.3d 464 (2d Cir. 1995); Dane S. Ciolino & Erin A. Donelon, *Questioning Strict Liability in Copyright*, 54 RUTGERS L. REV. 351 (2002); R. Anthony Reese, Historical Development of Mental State Considerations in Copyright Infringement (2004) (unpublished manuscript, on file with authors).

199. 17 U.S.C. § 504(c) (2004); Feltner v. Columbia Pictures Television, Inc., 523 U.S. 340 (1998). A plaintiff may not elect to pursue statutory damages for infringement of a published work unless the work is registered with the United States Copyright Office before the infringement begins or within three months of the work's publication. 17 U.S.C. § 412(2) (2004). Most works disseminated by the major content industries are likely to be registered, making the copyright owners eligible for statutory damages. Any defendant facing liability for statutory damages would also face liability for the plaintiff's attorney's fees, to be awarded at the court's discretion. *Id*. §§ 412, 505.

200. *Id*. § 504(c)(1).

201. *Id*. § 504(c)(2).

202. *See* The Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Pub. L. No. 106-160, 113 Stat. 1774 (codified as amended at 17 U.S.C. § 504(c) (2004)) (increasing maximum statutory damage amounts by 50% across the board).

different songs on their computer,[203] existing statutory damages can easily run into the tens of millions of dollars per individual.[204] This is likely to be an ample deterrent for the individuals who most often hold keystone positions on p2p networks. Indeed, it's arguably far too high already to do much good. College students do not have tens of millions of dollars to lose, and conversely those who do have that kind of money do not tend to spend their time trading music files on p2p networks. But civil suits with potentially enormous statutory damages may deter uploading because college students (or more likely the parents of teenagers) will fear bankruptcy. Indeed, the RIAA may have been able to eliminate some file sharing merely by threatening to sue some p2p users,[205] and more when it actually filed a few hundred suits.[206] But if so, existing statutory damages will be more than sufficient to achieve that deterrence.

College students are perhaps even more likely to be deterred by the prospect of going to jail.[207] Copyright law includes rather substantial criminal

203. *See, e.g.*, Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 551 (2003).

204. A defendant who has infringed 100 copyrighted songs and who is assessed the maximum statutory damages will owe $15 million; even in the absence of a finding of willfulness, the defendant could owe up to $3 million. This is far from hypothetical—mp3.com was assessed over $100 million in damages. UMG Recordings, Inc. v. mp3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

205. *See, e.g.*, John Schwartz, *Use of File-Sharing Services Drops, Survey Says*, N.Y. TIMES, July 15, 2003, at C8 (noting that RIAA threats to sue file sharers caused a 15% decline in the use of p2p networks, even without any actual suits filed).

206. The Pew Internet study estimates that illegal p2p file sharing dropped by 42% in the months after the RIAA filed its first round of lawsuits. Memorandum from Lee Rainey, Director, Pew Internet Project, Mary Madden, Research Specialist, Dan Hess, comScore Senior Vice President, and Graham Mudd, Analyst, The Impact of Recording Industry Suits Against Music File Swappers (Jan. 2004), *available at* http://www.pewinternet.org/reports/pdfs/PIP_ File_Swapping_Memo_0104.pdf (last visited Apr. 4, 2004); *see, e.g.*, Benny Evangelista, *52 Piracy Suits Settled*, S.F. CHRON., Sept. 30, 2003, at B1. While these numbers may be inflated because they rely on self-reporting in a survey, there is no doubt that the lawsuits had a deterrent effect. *See also* Benny Evangelista, *Millions Deleted Downloads*, S.F. CHRON., Nov. 5, 2003, at B1 (reporting study by NPD Group finding that over two million households deleted all the files they had downloaded because of their fear of legal action by copyright owners). The evidence as to the extent of the deterrent effect of the RIAA lawsuits has been somewhat equivocal and has varied over the period in which suits have been threatened or filed. *See, e.g.*, John Borland, *RIAA Lawsuits Yield Mixed Results*, CNET NEWS.COM, Dec. 4, 2003, *at* http://news.com.com/2100-1027-5113188.html (last visited Apr. 2, 2004); John Borland, *RIAA Steps Up File-trading Suits*, CNET NEWS.COM, Feb. 17, 2004, *at* http://news.com.com/2100-1027-5160262.html (last visited Apr. 2, 2004); Brock Read, *The Downloading Beat Goes On*, CHRON. HIGHER ED., Feb. 6, 2004, at A25; Reuters, *Employees Still Swapping at Work*, CNET NEWS.COM, Mar. 3, 2004, *at* http://news.com.com/2100-1027-5169508.html (last visited Apr. 4, 2004).

207. *See* Hardy, *supra* note 182, at 312 (arguing for imposition of criminal copyright penalties because of its deterrence value).

penalties, including prison time, for willful copyright infringement.[208] Under the 1976 Act as originally enacted, copyright infringement was a criminal offense only if the defendant acted willfully and for purposes of commercial advantage or financial gain.[209] Congress expanded criminal penalties rather substantially in the No Electronic Theft Act of 1997, however. The law now provides that willful infringers are criminally liable either if they act for financial gain, a term now defined to include the expectation that others will reciprocate by providing copies of other works, or if they reproduce or distribute works worth more than $1000 retail value in any six-month period.[210] This latter provision is likely to reach most keystone uploaders on a p2p network, so long as they act willfully.[211] As with civil penalties, it doesn't seem that the existing criminal penalties need to be augmented.[212]

208. 17 U.S.C. § 506(a) (2004). Copyright infringers can face up to ten years in prison. 18 U.S.C. § 2319(b)(2) (2004). The criminal penalties can also include substantial fines, although for the reasons just discussed the prospect of fines alone is no more likely than statutory damages to deter the defendants in question here.

209. Pub. L. No. 94-553, Title 1, § 101, 90 Stat. 2586 (codified as amended at 17 U.S.C. §506 (2004)). Prosecutors could not circumvent this requirement by charging violation of more general statutes, such as wire fraud. *See* Dowling v. United States, 473 U.S. 207 (1985).

210. 17 U.S.C. § 506(a)(1), (2) (2004). The maximum penalties differ somewhat for the two different types of criminal infringement. *Compare* 18 U.S.C. § 2319(b) (2004) (providing for imprisonment for up to 5 years, or 10 years for a second offense, for infringement for commercial advantage or private financial gain), *with id.* § 2319(c) (providing for imprisonment for up to 3 years, or 6 years for a second offense, for infringement of one or more works with a total retail value of over $1000 in a 6-month period). If the infringement does not involve reproduction or distribution, then the maximum prison term is not more than one year. *Id.* § 2319(b)(3). The European Commission recently proposed a similar strengthening of criminal copyright laws. *See* Paul Meller, *Europe Offers Plan to Fight Counterfeit Goods*, N.Y. TIMES, Jan. 31, 2003, at W1.

211. If the average price of a CD is $15 and the average price of a single is $2, anyone who has uploaded 67 full CDs or 500 different songs over a 6-month period meets this requirement. *See* Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L.Q. 835 (1999).

212. This doesn't mean there aren't efforts to do exactly that. One current proposal, H.R. 2752, 108th Cong. (2003), would enhance the criminal penalties available against users of p2p networks. Current law provides that criminal copyright infringement is a misdemeanor punishable by no more than one year imprisonment unless the defendant has reproduced or distributed 10 or more copies of one or more works with a total retail value of $2500 or greater. Section 301 of the bill would treat uploading even one work on a p2p network as meeting the 10-copy, $2500 felony threshold, thus subjecting a defendant to the felony penalties of up to 3 to 5 years imprisonment for a first offense. *See* Jonathan Band & Masanobu Katoh, *Members of Congress Declare War on P2P Networks*, J. INTERNET L., Oct. 2003, 18, 20-21. Another proposal, the Artists' Rights and Theft Prevention Act, S. 1932, 108th Cong. (2003), would establish a conclusive presumption that the felony threshold had been crossed any time someone without authorization made available a copy of a film, music recording, or computer program scheduled for commercial release before that release actually occurs. *See* Declan McCullagh, *Share 'True Crime,' Do the Time*, CNET NEWS.COM, Nov. 12, 2003, *at* http://news.com.com/2100-1026-5106684.html (last

The reason the already substantial civil and criminal penalties have only begun to have a deterrent effect is that for the most part they have not yet seriously been pursued against alleged direct infringers on p2p networks.[213] As Stuart Green put it, "if the state is serious about enforcing intellectual property laws, it cannot simply expect to impose harsh criminal sanctions, stand back, and wait for compliance."[214] Only in September 2003 did sound recording

visited Apr. 2, 2004); *see also* H.R. 2517, 108th Cong. (2003) (proposing various clarifications in criminal copyright enforcement authority). Still another proposal would give the Department of Justice the power to bring civil as well as criminal enforcement actions against p2p file sharers. Protecting Intellectual Rights Against Theft and Expropriation Act of 2004, S. 2337, 108th Cong. (2004).

213. *See, e.g.*, Letter from Rep. Lamar Smith, Sen. Joseph Biden, and seventeen other members of Congress, to John Ashcroft, Attorney General (July 25, 2002) (urging the Department of Justice to bring prosecutions against file sharers under the NET Act), *available at* http://www.techlawjournal.com/cong107/copyright/20020725.asp (last visited Apr. 4, 2004). At least one criminal prosecution has been brought in the United States against a college student who apparently made thousands of MP3 files available on a website. *See* Andy Patrizio, *DOJ Cracks Down on MP3 Pirate*, WIRED.COM, Aug. 23, 1999, *at* http://www.wired.com/news/politics/0,1283,21391,00.html (last visited Apr. 4, 2004). In addition, prosecutions have been brought against those operating smaller, underground "warez" networks trading copyrighted works, and at least one conviction involved making musical recordings available online over IRC. *See, e.g.*, United States v. Rothberg, 222 F. Supp. 2d 1009, 1012 (N.D. Ill. 2002) (sentencing defendant for conspiracy to commit criminal copyright infringement as part of "a highly organized Internet-based software piracy group called 'Pirates With Attitudes' that involved perhaps hundreds of participants and members-only websites that made available $1.4 million worth of computer software for downloading by members"); John Borland, *Net Music Pirate Faces Years in Prison*, CNET NEWS.COM, Aug. 21, 2003, *at* http://news.com.com/2100-1027-5066894.html (last visited Apr. 26, 2004); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, INTELLECTUAL PROPERTY CASES, *available at* http://www.cybercrime.gov/ipcases.htm (last visited Apr. 4, 2004); Brock Read, *2 SUNY Employees Plead Guilty to Online-Piracy Charges After a Federal Investigation*, CHRON. HIGHER EDUC., Oct. 9, 2003, *at* http://chronicle.com/prm/daily/2003/10/2003100901t.htm (last visited Apr. 4, 2004). And Japan has arrested two file-sharers. *See Japanese Police Make First File-Sharing Arrests*, MAINICHI DAILY NEWS INTERACTIVE, *at* http://www12.mainichi.co.jp/news/mdn/search-news/899563/file20sharing-0-2.html (last visited Apr. 26, 2004). Copyright owners and district attorneys talked for almost two years about suing direct infringers using public p2p networks, eventually making more and more frequent threats. *See, e.g.*, *DOJ Vows Prosecution of Internet Piracy*, 64 PAT. TRADEMARK & COPYRIGHT J. (BNA) 391 (2002) (citing statement of Deputy Assistant Attorney General John Malcolm); N.Y. TIMES, June 26, 2003, at A19 (full-page ad threatening to sue file-sharers); Reuters, *Piracy Warning Targets 300 Companies*, Mar. 17, 2003, *at* http://news.com.com/2100-1027-992992.html (last visited Apr. 4, 2004). But the first such civil suits were not filed until September 2003. *See, e.g.*, Declan McCullagh, *Perspective: The New Jailbird Jingle*, CNET NEWS.COM, Jan. 27, 2003, *at* http://news.com.com/2010-1071-982121.html (last visited Apr. 26, 2004). What was commonly reported as a group of suits against individual file sharers during early 2003, see Amy Harmon, *Recording Industry Goes After Students over Music Sharing*, N.Y. TIMES, Apr. 23, 2003, at A1, were in fact suits filed against college students who were facilitators running their own networks. *See, e.g.*, Amy Harmon, *Suit Settled for Students Downloading Music Online*, N.Y. TIMES, May 2, 2003, at A22.

214. Stuart P. Green, *Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights*, 54

copyright owners begin to pursue civil infringement suits against individual p2p uploaders.[215] In this subpart, therefore, we consider whether a small number of high-profile civil suits against, or criminal prosecutions of, file traders could substantially reduce widespread online infringement.[216]

The prospect of spending several years in prison or owing millions of dollars in damages is likely to serve as a substantial deterrent to digital copyright infringement by end users.[217] The more difficult empirical question is how many people the government must prosecute, or copyright owners must sue, in order to create a credible deterrent to illegal activity. We think the number of cases may actually be relatively small, and indeed the empirical evidence to date offers some support for that view.[218] There are several reasons for this.

First, while the number of users of p2p networks such as Morpheus and (before the injunction) Napster is massive, the overwhelming majority of those users engage only in downloading. Indeed, by one estimate, 3% of the users of a p2p network upload 97% of the files on that network.[219] These high-volume uploaders also seem to be the users most likely engaged in uploading illegal content, rather than providing access to legal files.[220] They are easy to identify, both because they will repeatedly appear in content searches and because many run so-called "supernodes" that facilitate fast downloads.[221] Reducing infringement on a p2p network doesn't require targeting downloaders, who may in any event have a legitimate reason for downloading some copyrighted

---

HASTINGS L.J. 167, 239 (2002).

215. Michael Warnecke, *Record Labels Sue 261 'Major Offenders' for Alleged Unlawful Online File-Swapping*, 66 PAT., TRADEMARK & COPYRIGHT J. (BNA) 545 (2003). The RIAA filed a second wave of suits in January 2004, see *RIAA Files 'John Doe' Complaints Against Alleged P2P Copyright Infringers*, 9 ELEC. COMM. & L. RPT. (BNA) 85 (Jan. 28, 2004), and a third wave in February, see Ted Bridis, *RIAA Sues Another 531 Downloaders in 4 Eastern States*, S.F. CHRON., Feb. 18, 2004, at B3.

216. For further discussion of criminal sanctions and p2p file sharing, see FISHER, *supra* note 29, at ch. 4; Geraldine Szott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. REV. 731 (2003).

217. *Accord* Dogan, *supra* note 21, at 80 ("[T]his renewed focus on primary infringers . . . may well deter enough unauthorized file-sharing to stanch the current flood of infringement.").

218. See *supra* text accompanying notes 205-06 on the deterrent effects of the lawsuits filed so far by the RIAA against p2p users.

219. *See, e.g.*, Matt Bai, *Hating Hilary*, WIRED, Feb. 2003, at 95, 97 (quoting Hillary Rosen of the RIAA), *available at* http://www.wired.com/wired/archive/11.02/hating.html (last visited Apr. 4, 2004); *see also* Dogan, *supra* note 21, at 102 (suggesting that 90% of content is provided by 10% of users).

220. Indeed, the recording industry's lawsuits have focused on such high-volume uploaders—those "who on average have allegedly distributed over 1000 copyrighted music files unlawfully." Warnecke, *supra* note 215, at 545. The record companies estimated that "10 percent of users are responsible for 90 percent of the infringement." *Id*.

221. *See* KAZAA, THE GUIDE: SUPERNODES, *at* http://www.kazaa.com/us/help/faq/supernodes.htm#whatis (last visited Apr. 4, 2004) (describing supernodes).

content.[222] It just requires targeting uploaders, and in particular the much smaller number of high-volume uploaders.[223] If there are 3 million users logged onto Morpheus at any one time,[224] perhaps 90,000 of them are high-volume uploaders.

Second, many high-volume uploaders are likely to be easily deterred. They are not paid for uploading files and indeed contribute substantial bandwidth and perhaps time on a voluntary basis in order to make files available to others. They are persuaded to do so in part because the p2p community inculcates a "norm" of sharing,[225] though the fact that most people do not upload indicates that that norm is not a particularly strong one in the community at large. But it is possible to participate in the p2p system without uploading, and the threat of bankrupting civil suits or criminal prosecution may induce a substantial number of high-volume uploaders to become passive downloaders instead. This is particularly true with criminal prosecution because the sort of individuals who tend to be high-volume uploaders seem likely to fear jail more than the average criminal. Willful digital copyright infringement over p2p networks is a crime apparently committed in significantly higher proportion than many other crimes by college students: young, educated members of society with a bright future ahead of them. The prospect of going to prison—and the attendant consequences, such as being kicked out of school—may worry a college student more than it would those inclined to commit other kinds of crime, such as burglary. The college student may feel she has more to lose and less to gain from this particular criminal activity than does the burglar. And since she has no strong stake in being an uploader, she may simply decide to quit. While it is

222. 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, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), 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.*, 180 F.3d 1072 (9th Cir. 1999), but that occurred in the context of a device that permitted personal space shifting without making files accessible to others.

223. "By targeting the [high-volume] uploaders, RIAA's strategy appears to be to choke off the supply of unlawful copies upstream and save the hassle of chasing after every downloader . . . ." Warnecke, *supra* note 215, at 545.

224. *See* Charles C. Mann, *The Year the Music Dies*, WIRED, Feb. 2003, at 90, 92, *available at* http://www.wired.com/wired/archive/11.02/dirge.html (last visited Apr. 4, 2004) (noting that 3.1 million users were logged on using Kazaa at one time).

225. Strahilevitz, *supra* note 203. The norm is phrased in the form of parity—it is unfair to take from the network if you will not also give to the network. Most people do in fact take without giving back, something the p2p systems conceal in a design element Strahilevitz calls "charismatic code." *Id*. One new system—BitTorrent—takes the reciprocity norm to an extreme, preventing users from downloading unless they also upload. *See* Dustin Goot, *Has Hollywood Met Its Napster?*, WIRED, Aug. 2003, at 38, *available at* http://www.wired.com/wired/archive/11.08/start.html?pg=9 (last visited Apr. 4, 2004).

only a guess, it might be reasonable to say that a five percent chance of criminal prosecution and punishment for uploading files in any given year would be enough to deter the majority of uploaders. Similarly, the parents of teenagers—another significant group of uploaders—may fear the prospect of a bankrupting multimillion dollar damage award more than other potential defendants in other types of unlawful activity, such that the same five percent chance of owing such an award might be enough to deter most uploaders. This means that if we must deter 90,000 people, we need only successfully prosecute or sue, and impose severe sanctions on, 4500. These numbers are only the roughest of estimates, but they suggest that the numbers involved may be more realistic than would otherwise seem the case from the large absolute numbers of people who participate in p2p networks.

Even this number might overstate the number of suits or prosecutions needed to significantly reduce widespread p2p infringement. While it is possible that deterrence occurs only after a threshold—that is, that no one will be deterred by the threat of legal action until the chance of prosecution reaches five percent—we think it more likely that deterrence is at least partially linear, because some high-volume uploaders are more risk-averse than others.[226] Prosecuting fewer than 4500 people—say, 1500—might deter some but not all uploading of illegal content.[227] Partial deterrence will not only reduce the infringement on p2p networks by eliminating the deterred users as sources of infringing files, but will also increase the burden on the remaining high-volume uploaders, as the mass of downloaders in a network shifts to the remaining uploaders. The result may be a cascade effect, in which causing some uploaders to stop providing illegal content (and deterring others from starting to provide such content) imposes technical burdens that in turn cause more uploaders to drop off the network, further increasing the technical burden (and the percentage risk of prosecution) for the remaining uploaders.

We can foresee at least four main objections to the use of criminal or severe civil sanctions to enforce the law against large-scale infringement in the p2p context.[228] First, imposing such liability, especially criminal liability, on a few individuals in order to deter thousands of others may seem unfair to those who are singled out for prosecution.[229] This unfairness may have no formal

226. Partial deterrence is also possible because of discontinuities in the patterns of prosecution. If U.S. Attorneys in California are more likely to prosecute than in other states, for example, uploaders might be deterred in California even though their peers in Kentucky are not.

227. While we wrote this statement in April 2003, subsequent events have provided support for it. Estimates suggest that a few hundred lawsuits may have deterred a substantial number of illegal file sharers. *See supra* text accompanying notes 205-06.

228. We distinguish objections to the successful use of prosecution from claims that prosecution will likely be ineffective because of the characteristics of the Internet. The latter claims apply both to criminal and civil liability and to an administrative remedy, and we consider them below. *See infra* Part III.D.

229. *Cf.* David Strauss, Must Like Cases Be Treated Alike? (2003) (unpublished

legal consequence; selective prosecution occurs in a variety of fields and courts have consistently rejected constitutional challenges to the arbitrariness of making examples of a few defendants, at least where racial animus is not at issue.[230] But it does put the burden of reducing infringement squarely on the backs of a few uploaders, rather than distributing it more evenly among the population of infringers, and many people might find that morally objectionable.[231] And the level of sanction imposed on those select few against whom enforcement is vigorously pursued may well seem "radically disproportionate to the wrong they committed."[232]

Second, the downside of effective deterrence is the risk of overdeterrence. Criminal penalties are particularly likely in white collar cases to deter legal conduct that is near the borderline of illegality and may be wrongly perceived as illegal.[233] In this case, however, we think the risk of overdeterrence is minimal. We are describing criminal prosecution or civil suits for significant monetary damages focused entirely on high-volume uploaders—say, those who upload more than 500 copyrighted songs. It is highly unlikely that these high-volume uploaders are in fact engaged in legal conduct.[234] If virtually all high-

manuscript, on file with authors).

230. *See, e.g.*, Gary v. City of Warner Robins, 311 F.3d 1334, 1339 n.12 (11th Cir. 2002) ("'[T]o state a claim for selective prosecution, [Gary] must demonstrate that she was prosecuted while others similarly situated were not, and furthermore that the government prosecuted her invidiously or in bad faith.'") (quoting Lanier v. City of Newton, 842 F.2d 253, 256 (11th Cir. 1988)); United States v. Berrigan, 482 F.2d 171, 174 (3d Cir. 1973) ("[A]lthough the government is permitted 'the conscious exercise of some selectivity' in the enforcement of its criminal laws, any 'systematic discrimination' in enforcement, or 'unjust and illegal discrimination between persons in similar circumstances,' violates the equal protection clause.") (citations omitted).

231. *See, e.g.*, Frank I. Michelman, *Property, Utility, and Fairness: Comments on the Ethical Foundations of "Just Compensation" Law*, 80 HARV. L. REV. 1165, 1214-15 (1967) (discussing the "demoralization costs" that result when people perceive themselves as having been treated unfairly). A more general moral objection is offered by Geraldine Moohr, who argues that personal use of copyrighted materials is not morally wrong and therefore should not be criminalized. *See* Moohr, *supra* note 216, at 734. Our argument in the text proceeds from the assumption that criminal copyright law, like its civil counterpart, has utilitarian rather than moral purposes.

232. Lunney, *supra* note 197, at 851-52 (suggesting that copyright law may already have reached the point at which "the level of punishment required to deter private copying generally [has] simply become unjust").

233. *See, e.g.*, Michael K. Block & Joseph Gregory Sidak, *The Cost of Antitrust Deterrence: Why Not Hang a Price Fixer Now and Then?*, 68 GEO. L.J. 1131, 1133-38 (1980) (discussing the cost of overdeterrence); Mark A. Lemley, *The Economic Irrationality of the Patent Misuse Doctrine*, 78 CAL. L. REV. 1599, 1620 n.130 (1990) (noting the risks of overdeterrence of speeding).

234. High-volume uploaders could conceivably be engaged in space-shifting their entire music library so they can access it from another location, but it seems unlikely either that this is what most high-volume uploaders are doing or that a court would find such space-shifting to be fair use in this context. *See also* Band & Katoh, *supra* note 212, at 21 (noting that "[e]very court to consider file trading has concluded that the typical file trader is a direct infringer" and that any fair use defense is more plausible for a downloader than for an

volume uploaders are acting illegally, and if it is clear how to avoid being in that category, overdeterrence doesn't seem a significant problem.

Third, as with any criminal law, mistaken prosecutions will impose significant costs on those wrongfully targeted.[235] Similarly, mistaken civil suits will impose significant litigation expenses and related costs. Mistakes will certainly be made, though the straightforward nature of the case and the detailed electronic trails that file transfers create may actually make the risk of mistaken prosecution rather small.[236] It is somewhat more likely that courts will err by punishing high-volume uploaders who are not in fact willfully infringing copyright, but who instead genuinely believe that their conduct is legal.[237] This would be a miscarriage of justice, since willfulness is an element of criminal copyright infringement and of enhanced statutory damages,[238] and the danger of such mistaken verdicts, given the potentially severe sanctions, may be a significant cost of pursuing criminal penalties or enhanced statutory damages against high-volume uploaders.

Finally, criminal prosecution requires the initiative of U.S. Attorneys, and they may find the prospect of prosecuting college students for uploading music politically unpalatable.[239] And imposing criminal penalties is likely to cause

uploader).

A somewhat more plausible defense could be offered by a high-volume uploader who uploads only obscure, out-of-print works. Such a defendant might have an argument that the dissemination of these out-of-print works was a fair use, though the success of that argument is far from clear. While it is possible such high-volume uploaders exist, we doubt that most high-volume uploaders focus on obscure works of this sort. *See infra* text accompanying note 282.

235. This seems to animate David Rice's concern about the "public-private partnership" in criminal copyright enforcement. *See* David A. Rice, *Copyright As Talisman: Expanding 'Property' in Digital Works*, 16 INT'L REV. L. COMPUTERS & TECH. 113, 125 (2002). Rice foresees the potential for abuse by copyright owners who refer for criminal prosecution charges that do not in fact constitute copyright infringement.

236. At least 2 of the RIAA's first 261 suits filed in September 2003 have led to claims of mistake and, in one case, dismissal of the complaint. *See, e.g.*, Katie Dean, *Fan to RIAA: It Ain't Me, Babe*, WIRED.COM, Oct. 15, 2003, *at* http://www.wired.com/news/digiwood/0,1412,60814,00.html?tw=wn_culthead_6 (last visited Apr. 16, 2004); John Schwartz, *She Says She's No Music Pirate. No Snoop Fan, Either.*, N. Y. TIMES, Sept. 25, 2003, at C1 (reporting RIAA dismissal of suit against 66-year-old Sarah Ward and noting that Ms. Ward's computer is a Macintosh, while the Kazaa software she was alleged to have used does not run on that platform).

237. *See* Loren, *supra* note 211, at 854 (making this point).

238. United States v. Moran, 757 F. Supp. 1046 (D. Neb. 1991); Loren, *supra* note 211, at 854. This assumes that these individuals do not know they are violating the law. One way to minimize this risk would be for criminal or civil suits to be brought only against individuals who had previously been warned by copyright owners to cease their conduct and who nonetheless persisted. In addition, with respect to civil enforcement, it is not clear that the enhanced statutory damages dependent on willfulness are necessary for deterrence. A defendant who had uploaded 1000 different works would face a maximum statutory damage award of $30 million, even in the absence of willfulness. 17 U.S.C. § 504 (2004) (permitting maximum statutory damage award of $30,000 per work infringed in ordinary case).

239. *See, e.g.*, Band & Katoh, *supra* note 212, at 22 ("Enforcement of the criminal

defendants to fight back harder. To date, many file sharers sued civilly have settled for relatively low sums of money. Threaten to put them in jail, though, and many will plead not guilty and go to court. This raises the costs, both financial and political, of any given prosecution, though it may be a good rather than a bad thing for society to have these issues vetted in open court. Similarly, while the RIAA has proven willing to file civil suits, none have yet gone to trial, and it may be that jurors will prove sympathetic to file-sharing defendants regardless of what the law provides.[240] This isn't really an objection to liability as much as skepticism that severe civil or criminal sanctions will really be enforced. It is true that a large number of people participate in p2p file sharing, and it is possible that they would protest criminal prosecutions, making the person who brought those prosecutions unpopular, or that they would serve on juries and return nullifying verdicts.[241] On the other hand, some of the most powerful lobbying groups in the world are behind stronger criminal copyright enforcement. They managed to persuade Congress to pass the NET Act, strengthening criminal penalties and expanding the definition of criminal copyright infringement. More recently, a number of Congressional representatives have on two different occasions taken the Justice Department to task for not enforcing the NET Act,[242] suggesting that there might be substantial political will in favor of criminal prosecution.

Still other objections to criminal prosecution or severe civil penalties stem from broader objections to the enforcement of copyright law in the digital environment. If you believe copyright law in the digital environment in general is a bad idea,[243] or that p2p file sharing should be legal,[244] it follows that you

copyright provisions against non-commercial infringers simply has not been a priority for the Justice Department. The Justice Department correctly perceives that the public has little interest in seeing college students sent to prison merely because they traded songs on the Internet."); Liebowitz, *Policing Pirates*, *supra* note 127, at 15 ("It is painful to imagine the authorities . . . prosecuting copyright infringers, often teenagers, for downloading music and other files."). Copyright owners apparently long hesitated to bring civil suits against p2p end users because of fears about how such suits would be perceived by the public. *See, e.g.*, John Borland, *Why File Swapping Tide Is Turning*, CNET NEWS.COM, Sept. 18, 2003, *at* http://news.com.com/2008-1082-5078418.html (last visited Apr. 4, 2004).

240. *See, e.g.*, Brock Read, *Nobody Likes a Snitch*, CHRON. HIGHER EDUC., Mar. 12, 2004, *at* http://chronicle.com/prm/weekly/v50/i27/27a03101.htm (last visited Apr. 4, 2004) (detailing harassment against college students identified as having alerted college officials to p2p networks on campus).

241. Even forcing jury nullification might have social value. *Cf.* Lunney, *supra* note 197, at 821 (noting in connection with the effect of the DMCA's anticircumvention provisions on private copying, that "in the face of unjust laws, individual citizens have no choice but to disobey and thereby force society to enforce the law in a way that makes its injustice palpable").

242. *See, e.g.*, Smith et. al., *supra* note 213.

243. *See, e.g.*, John Perry Barlow, *The Economy of Ideas: A Framework for Patents and Copyrights in the Digital Age. (Everything You Know About Intellectual Property Is Wrong.)*, WIRED, Mar. 1994, at 84, *available at* http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html (last visited Apr. 4, 2004).

wouldn't want to see criminal prosecutions of, or substantial monetary penalties for, uploaders. From the perspective of those who both believe in the copyright system and believe that large-scale file sharing is illegal, however, criminal prosecutions or very large statutory damage awards offer the advantage of dealing with infringement without unduly hampering technological innovation.

They have disadvantages too, however, as noted above. Most notably, it seems unfair and disproportionate to impose the burden of enforcing copyright so heavily on a few unlucky defendants. This is particularly true if the sanction is severe—we put up with random enforcement of traffic offenses because the sanction is so minor, but we might feel differently if speeders had to spend a year in jail. A perception of unfairness and disproportionality may be particularly likely in regard to p2p users, since the unlucky defendants may be particularly sympathetic: high school or college students who aren't engaged in more obviously antisocial types of conduct. Because of these shortcomings, in the Part that follows we examine alternative methods of targeting enforcement at direct infringers rather than at intermediaries.

B. *Lowering Enforcement Costs*

A more palatable alternative to raising sanctions by putting a small number of college students in jail (or bankrupting them) in order to deter their peers is to lower the cost of enforcement. Suing most or all direct infringers currently isn't attractive because litigation is so expensive and time-consuming. If enforcement is quick, cheap, and certain enough, the sanction for infringement doesn't need to be very high in order to achieve the same deterrent effect. In this Part we discuss two possible systems for lowering enforcement costs: an

244. *See, e.g.*, Ku, *supra* note 127.

Jessica Litman argues that it is not clear under current law whether individual users are liable for copyright infringement for personal copying. *See* Jessica Litman, *War Stories*, 20 CARDOZO ARTS & ENT. L.J. 337, 341-42 (2002). We think there is a fair policy question as to whether individual noncommercial use *should* be illegal, though the case law seems fairly clear that such reproduction by individuals may infringe. *See also* Ho, *supra* note 25, at 1568-70 (describing the legality of noncommercial use as a myth of modern copyright law). Litman relies in part on 17 U.S.C. § 1008 (2004), a part of the Audio Home Recording Act, *see* Litman, *supra*, at 346, 356-60. That statute has so far been interpreted largely not to apply to copies made by computer. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999). On the other hand, in the latter decision, the court strongly endorsed application of Section 1008's policy of not penalizing consumer noncommercial copying of musical recordings even to activity outside the section's literal scope. *Diamond Multimedia Sys.*, 180 F.3d at 1079. In any event, the activities engaged in by keystone uploaders on p2p networks seem quite distinct from the kinds of private, personal, noncommercial acts of reproduction or distribution that might not be infringing under current law and that should not, in our view, attract the kind of enforcement efforts we describe in the text. *See supra* notes 108 & 116.

automated compulsory license system implemented through a levy, and a streamlined online arbitration system for resolving copyright disputes.

By any count there are a lot of infringers online. The task any widespread enforcement approach must confront, therefore, is to permit copyright owners to pursue enough of these infringers to reduce infringement to manageable proportions[245] without imposing extraordinary costs on the copyright owners. If we are not to raise the sanction for enforcement to harshly punitive levels,[246] this means lowering the cost of enforcement against individuals to such a degree that copyright owners can cost-effectively pursue tens or even hundreds of thousands of them.

1. *Levies*.

One possibility is to do away with lawsuits altogether in favor of an ex ante mechanism for compensating copyright owners. In important new works, both Neil Netanel and Terry Fisher have proposed that copyright be "enforced" online in this context through a system of levies—or rather, that levies be used to compensate copyright owners for the online activities against which traditional enforcement has proven difficult.[247] A levy is a form of blanket compulsory license, authorizing copying in exchange for a set fee. Rather than requiring each individual who wants a license to affirmatively apply for one or requiring copyright owners to identify and sue those who owe the license fee, however, the levy would be automatically collected on the sale of software, services or hardware that are likely to be used in infringement. Similar systems exist or are being implemented in Canada,[248] Germany, and elsewhere in the European Union,[249] where purchasers of computers pay a set fee (currently

245. Recall that the law has never stopped, and need not stop, all infringement. *See supra* notes 192-96 and accompanying text.

246. On that approach, see *infra* Part III.A.

247. FISHER, *supra* note 29, at ch. 6; Netanel, *supra* note 29. For other suggestions along these lines, see Aric Jacover, *I Want My MP3! Creating a Legal and Practical Scheme to Combat Copyright Infringement on Peer-to-Peer Internet Applications*, 90 GEO. L.J. 2207, 2250-54 (2002); Ku, *supra* note 127.

248. *See* John Borland, *Canada Deems P2P Downloading Legal*, CNET NEWS.COM, Dec. 12, 2003, *at* http://news.com.com/2100-10205-5121479.html (last visited Apr. 4, 2004) (reporting ruling by Copyright Board of Canada applying levy on recording media to hard-drive-based music players, ranging from $2 for players with less than 1 GB of memory to $25 for players with 10 GB of memory or more).

249. *See* P. BERNT HUGENHOLTZ, LUCIE GUIBAULT & SJOERD VAN GEFFEN, THE FUTURE OF LEVIES IN A DIGITAL ENVIRONMENT: FINAL REPORT (2003), *at* http://www.ivir.nl/publications/other/DRM&levies-report.pdf (last visited Apr. 26, 2004); Bernt Hugenholtz, Remarks delivered at the Berkeley Center For Law & Technology, Symposium on The Law and Technology of Digital Rights Management (Mar. 1, 2003), *in* 18 BERKELEY TECH. L.J. 697, 768-70 (2003). Levies designed to provide equitable remuneration to copyright owners for private copying of their works have been part of the law in many European nations since before the digital age, often covering photocopying and "home taping" of music. *See* PAUL GOLDSTEIN, INTERNATIONAL COPYRIGHT: PRINCIPLES,

twelve euros in Germany) into a fund designed to compensate copyright owners for infringement.[250] And there is precedent in U.S. law: The Audio Home Recording Act of 1992 (AHRA) provides for a levy to be charged on all blank digital audio media and digital audio recorders, with the revenue to be allocated among music copyright owners.[251] The AHRA hasn't seen much use, but that is because the digital audio recording systems covered by the Act never caught on.

Levies of the type Netanel and Fisher have proposed offer substantial advantages over the existing regime of secondary and tertiary liability.[252] They are likely to force virtually all copyright infringers to pay what amounts to a relatively modest license fee. Because they operate automatically, they can be enforced at a minimum of cost.[253] And because they replace the existing scheme of legal enforcement, they permit society to make use of the existing, efficient p2p networks to disseminate digital content online. In essence, a levy

LAW, AND PRACTICE 312-13 (2001). Professor Hugenholtz notes that a recent European enactment on digital copyright "effectively sets out a track for the gradually phasing out of levies" in favor of systems of digital rights management. Hugenholtz, *supra*, at 769.

250. *See* Press Release, Campaign for Digital Rights, UK Campaign for Digital Rights Condemns German PC Levy (Mar. 13, 2003), *available at* http://lwn.net/Articles/25409/ (last visited Apr. 4. 2004) (discussing a German levy on the sale of PCs designed to compensate copyright owners for infringement by computer users); *see also* Associated Press, *Apple Faces Claim in France for Royalties Levy on iPod*, Mar. 10, 2004, *at* http://www.fortwayne.com/mld/newssentinel/business/8151296.htm (last visited Apr. 4, 2004).

251. 17 U.S.C. §1004-07 (2004) (setting the royalty and providing for its allocation among copyright owners).

252. *But see* Dogan, *supra* note 21, at 78-80, 101-10 (arguing that common law secondary liability rules can address digital copyright problems without the need for levies). We should be clear that we are speaking here of levies that would substitute for rather than supplement normal copyright enforcement. Under the substitution approach, an individual who has paid the levy fee would in effect have purchased a paid-up license to download copyrighted content. Thus, the levy would replace existing copyright enforcement efforts. *See* Netanel, *supra* note 29. By contrast, a levy that is added to the existing legal rules would not accrue the advantages discussed in the text, though it would still suffer from the disadvantages we describe.

253. There would be some administrative cost, of course. Someone—perhaps the Copyright Office—would have to set the fees, determine the devices or services to which they apply, and periodically adjust both determinations. The resulting revenue would have to be distributed equitably among copyright owners. Existing precedent suggests both costs are not necessarily overwhelming, however. The Copyright Office already sets a large number of compulsory license fees by rulemaking and distributes the proceeds among copyright owners in some cases. *See, e.g.*, 17 U.S.C. §§ 111, 114, 115, 118, 119 (2004); Bonneville Int'l Corp. v. Peters, 153 F. Supp. 2d 763 (E.D. Pa. 2001); Reese, *supra* note 116, at 242-44, 248-49; Raffi Zerounian, Bonneville International v. Peters, 17 BERKELEY TECH. L.J. 47 (2002). And private organizations such as ASCAP have developed ways of dividing collective licensing revenue based on statistical analyses of use. *See, e.g.*, Stanley M. Besen, Sheila N. Kirby & Steven C. Salop, *An Economic Analysis of Copyright Collectives*, 78 VA. L. REV. 383 (1992); Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293 (1996).

coopts illegal file-sharing by charging a fee and then declaring it legal.[254]

A hybrid levy approach would not impose the levy by law on all devices but would permit facilitators who might otherwise fear indirect liability to buy immunity by paying a levy for their users. If Grokster paid a levy for each copy of Morpheus software that it disseminates, for example, the company could avoid being sued for facilitating infringement by users of its software. Companies that specialized in facilitating music downloads would want to pay the fee, since they would face liability under traditional principles of contributory or vicarious infringement. By contrast, companies with rather less connection to infringing activity could opt not to pay the levy, gambling that they are not infringing.[255]

One problem with levies is that, like suing facilitators, they target upstream technologies rather than the people doing the infringing. Indeed, imposing a levy is economically quite similar to suing facilitators—the levy just substitutes a liability rule and a collection mechanism for copyright law's existing property rule. To make the levy small, it has to be imposed on a wide range of devices (say, all computers or all modems or all ISP service agreements). But a levy charged on a range of devices with multiple uses is a tax on those devices, paid by both those who download music and those who do not. This is akin to a tax on innovation in the Internet environment. This tax seems better than suing innovators under a property rule, because copyright owners will not have the power to ban innovation outright, but taxing innovation will naturally

254. One advantage of such legalization of p2p networks over using criminal or civil enforcement against infringing p2p uploaders is that such enforcement would—if it works—over time effectively shut down p2p networks all or almost all of whose content is illegal, since without uploaders there can be no downloaders. Only those networks that were put to a sufficiently large number of legal as well as illegal uses would be likely to survive. Relative to proposals to render file-sharing legal, therefore, enforcing the copyright law against direct infringers may have the effect of eliminating the efficiencies associated with the p2p distribution system, at least where the system is used overwhelmingly for disseminating works without permission. Criminal or civil enforcement against p2p users is still preferrable to suing the p2p network provider itself, however, because the former approach would permit the uploading of legitimate content.

255. Still other proposals that seem to have little in common with levies operate on the same basic principle. One such approach seeks to have facilitators internalize the harm their technology causes. Lichtman and Landes argue for a hybrid property-negligence standard, under which Internet service providers that facilitated copyright infringement by failing to design their system to avoid it would have to pay the damages caused by that infringement but under which they might also be subject to property-like relief such as injunctions and supracompensatory damages. *See* Lichtman & Landes, *supra* note 124. Thus, Lichtman and Landes would create a rule with some of the characteristics of a tort regime but also some characteristics of a property regime. Unlike current copyright law, a true liability rule would permit neither injunctive relief shutting down the facilitators nor supracompensatory remedies like statutory damages. Such a liability rule, like a levy, is a tax imposed on facilitators to pay for the harm they cause to the incentives of copyright owners. And a liability rule, like a levy, is in effect a compulsory license, with all the problems those entail. The difference is that the tax is calculated ex post by a court, rather than ex ante by an administrative agency.

discourage it somewhat.[256]

Levies will likely have other consequences as well. If a levy is charged on a single device or service (say a computer or an ISP account) and if paying the levy makes downloading content legal, the levy will create moral hazard problems.[257] There is every incentive to download as much music as possible if you are paying a flat rate.[258] One might question whether this is a bad thing, however, given that the goods in question are nonrivalrous. Copyright owners, though, may want to compensate for this effect by having the rate set relatively high, and if they persuade the rate-setting body to do so, that will do further damage to innovation and discourage casual users from buying the device or service at all. Further, this flat rate charge would likely sharply limit the role of authorized musical services provided by the content owners. This may not be a problem—as noted above, there are reasons to think that p2p networks disseminate content more efficiently than the copyright owners would—but if you think top-down networks are preferable, or that copyright owners should have the ability to choose to use them over other methods, then the fact that p2p networks will replace them is an additional cost. Third, someone—either the government or a private group mediating between copyright owners and device manufacturers—will have to set the levy, and because they do not face the discipline of the market it is reasonable to worry that they will not do so at a market-clearing price.[259] Finally, a levy generally requires money to be paid by a facilitator, which will often mean that the facilitator will collect a fee from the user at the point the device, program or service is provided, restricting the use of anonymous computer networks.[260]

To reduce some of these problems, a levy could be closely tailored to acts of infringement. A partial step in this direction would be to charge a per-use

256. It may also distort the nature of that innovation. If a levy is charged on each device that can be used to download digital content, there will be a strong incentive to use a single device that serves just that purpose—and therefore pay only one levy—rather than to combine general-purpose devices that serve other purposes as well but would require the payment of multiple levies. While it may be possible to avoid this problem by tailoring the levy for each device closely to how it is used, doing so raises the administrative cost of the proposal substantially and makes it more dependent on getting a complex system of levy amounts correct.

257. Stacey Dogan phrases the point a bit differently, saying that levies constitute a subsidy from technology users generally to those who are high-volume downloaders, but the basic point is the same. *See* Dogan, *supra* note 21, at 101.

258. On the other hand, one possible distortion suggested to us by Glynn Lunney is that to the extent people think of devices and entertainment in separate budget categories they may overpay for entertainment if we charge them an entertainment tax that gets mentally filed in the device budget.

259. *See, e.g.*, Dogan, *supra* note 21, at 78 (describing a levy as "replac[ing] the current market-based approach to intellectual property licensing with a government-imposed royalty system").

260. The facilitator might not collect a fee from the user but instead pay the fee on the user's behalf and recoup the cost by other means, such as advertising.

rather than a flat-rate fee.[261] Charging a levy on every megabyte downloaded, for example, might correlate reasonably well with copyright infringement, and it would solve the moral hazard problem described above (to the extent that it is viewed as a problem). Such a bandwidth tax would still affect certain types of innovation, however, notably those that involve high-bandwidth uses of the Internet. And discouraging the fledgling broadband Internet market seems a bad idea, given the lengths policy makers are willing to go in other circumstances to encourage broadband rollout.[262] An additional cost of tailoring is that it may tend to channel innovation in the relevant market into pay form and centralized software distribution and also to discourage anonymity, so that the levy can be effectively collected.[263]

Charging a levy only on acts that would otherwise be infringing—say, a fee per mp3 file downloaded without authorization from the copyright owner—would be ideal from an innovation standpoint, since it would distinguish between legal and illegal uses of a device or service. But such an approach would obviously create serious monitoring problems. Indeed, it doesn't make sense to talk about such a finely targeted levy as a "levy" at all. Instead it would be a compulsory license dependent on identifying and collecting from infringers.[264] As such, it would replicate many of the problems discussed above for copyright owners who must enforce their rights against a large number of individual infringers.

2. *A streamlined dispute resolution system*.

Besides a levy system, another possible alternative for lowering enforcement costs for copyright owners would be to make dispute resolution by

261. Lon Sobel has offered just such a proposal. *See* Lionel S. Sobel, *DRM As an Enabler of Business Models: ISPs As Digital Retailers*, 18 BERKELEY TECH. L.J. 667, 680-81 (2003) (proposing that ISPs be immune from liability only if they meter and charge for the use of copyrighted works over p2p networks).

262. Much of the debate over modern telecommunications policy is about how to encourage broadband deployment. *See, e.g.*, Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001); Howard A. Shelanski, *The Speed Gap: Broadband Infrastructure and Electronic Commerce*, 14 BERKELEY TECH. L.J. 721 (1999); James B. Speta, *Handicapping the Race for the Last Mile?: A Critique of Open Access Rules for Broadband Platforms*, 17 YALE J. ON REG. 39 (2000); Phil Weiser, *Paradigm Changes in Telecommunications Regulation*, 71 U. COLO. L. REV. 819 (2000).

263. While in theory there are ways of paying bills anonymously online, they have not taken off. *See, e.g.*, Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 353 (2001). For more detailed discussion of anonymous electronic cash, see, for example, A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases,* 15 J.L. & COM. 395 (1996); Kerry Lynn Macintosh, *The New Money*, 14 BERKELEY TECH. L.J. 659 (1999).

264. This is how we view Sobel's proposal to have ISPs monitor the usage of their customers and charge for the use of copyrighted works.

those owners against large-scale direct infringers quick and cheap, so that owners would be more inclined to pursue such direct infringers instead of suing facilitators. While enforcement costs are likely always to be too great to allow pursuit of every infringer, lower costs would allow for enforcement against *more* infringers, increasing any given infringer's chance of being sued.[265]

Is it possible to make such dispute resolution quick and cheap? Traditional arbitration is neither. There is, however, an online model in the Uniform Dispute Resolution Policy (UDRP) for Internet domain name trademark disputes implemented by the Internet Corporation for Assigned Names and Numbers (ICANN).[266] This policy has resolved about 7500 such disputes involving over 13,000 domain names in four years, at a cost of $1200-$1500 each and an average resolution time of little more than a month.[267] The UDRP is an alternative dispute resolution system that allows trademark owners to bring complaints that a domain name registrant has in bad faith registered and used a domain name identical or confusingly similar to the owner's trademark. These complaints are considered by expert panelists through accredited private providers of dispute resolution services. The system is designed to resolve only straightforward cases of bad-faith cybersquatting, and to reserve for the courts difficult factual and legal disputes between parties with competing and arguably legitimate claims to the same domain name.[268] For those straightforward cases of cybersquatting, there are unlikely to be significant factual or legal disputes that need resolving. A panelist given the basic facts can make a decision fairly quickly. Like the UDRP, a copyright dispute resolution system, if properly conceived, could target straightforward conduct that is unlikely to have legitimate justifications, such as high-volume uploading of copyrighted works to p2p networks. Assertion of a plausible factual or legal dispute—evidence suggesting that the works in question weren't copyrighted, or weren't copied, or that the use is fair—should result in denial of the

265. *See* Lunney, *supra* note 197, at 852 ("Even if suing every private copier remained impractical, an increase in the number of enforcement actions would increase the risk of a lawsuit for each private copier.").

266. On the UDRP as a model for institutional design, see Lawrence R. Helfer & Graeme B. Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141 (2001); Andrew F. Christie, The ICANN Domain Name Dispute Resolution System as a Model for Resolving Other Intellectual Property Disputes on the Internet (2002) (unpublished manuscript, on file with authors).

267. For a list of decisions, see ICANN, Search Index of Proceedings Under the Uniform Domain-Name Dispute-Resolution Policy, *at* http://www.icann.org/cgi-bin/udrp/udrp.cgi (last visited Apr. 4, 2004). The cost figure is for the price charged by the dispute resolution provider.

268. It has been abused in some instances, however, by trademark owners using it in dubious cases, and panels have sometimes granted relief to complaining trademark owners on claims that arguably fall outside the limited scope of the UDRP. *See* Michael Geist, *Fair.com?: An Examination of the Allegations of Systematic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903 (2002) (collecting examples).

copyright owner's claim without prejudice to her ability to bring a lawsuit where such legal and factual issues can be fully explored.

Our analogy to the UDRP will raise some people's hackles. The UDRP has some serious structural problems. It lacks some important procedural due process protections, such as an administrative appeal, a fair system for assigning panelists, and a penalty for overreaching by complainants.[269] But these problems can be solved in the copyright context by learning from the UDRP experience. A digital copyright dispute resolution process could select judges in a fair and balanced® way. It could permit an administrative appeal. And it could impose some sanction on frivolous or bad-faith claims made by copyright owners.[270]

There are, however, two fundamental differences between the factual settings of the UDRP and of the digital copyright cases a dispute resolution panel would likely be called upon to resolve. First, the domain name at stake in the UDRP is ultimately under the control of ICANN. As a result, a successful UDRP complainant does not have to collect money or property from a losing domain name registrant; the UDRP panel merely needs to instruct ICANN to transfer ownership of the domain name to the trademark owner. There is no similar control over digital copyright infringers. A copyright system therefore needs a substitute sanction and enforcement mechanism, such as an award of money damages or a reliable way to remove infringing material or the infringer herself from the network.

Second, the UDRP is imposed by ICANN on all registrars, who impose it by contract on all registrants. It requires contracts with and reliable identification of users. There is no central authority that contracts with Internet users generally. Binding Internet users to a p2p copyright dispute resolution system by contract would require them to contract with their ISPs or with providers of specific services, and there is no entity akin to ICANN that has contracts with all the ISPs and could impose this contracting requirement on them. As a result, the dispute resolution system we propose would be imposed by statute as part of copyright law.

269. We consider these to be important due process protections, whether or not they would be required by the Constitution's due process clause. For detailed discussion of these problems in the UDRP, see A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy": Causes and (Partial) Cures*, 67 BROOK. L. REV. 605 (2002); Geist, *supra* note 268; Kenneth L. Port, *Intellectual Property in an Information Economy: Trademark Monopolies in the Blue Nowhere*, 28 WM. MITCHELL L. REV. 1091 (2002); Elizabeth G. Thornburg, *Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process*, 6 J. SMALL & EMERGING BUS. L. 191 (2002).

270. For suggestions of these and similar changes to the UDRP itself, see Orion Armon, *Is This As Good As It Gets? An Appraisal of ICANN's Uniform Dispute Resolution Policy (UDRP) Three Years After Implementation*, 22 REV. LITIG. 99, 138 (2002) (proposing that complainants should be required to post a small bond to be forfeited to the defendant if they are found to have acted in bad faith in filing the complaint); Froomkin, *supra* note 269, at 688-92; Port, *supra* note 269, at 1117-22.

We suggest that Congress amend the copyright statute to provide that in a certain category of cases of copyright infringement over p2p networks, a copyright owner would have the option to choose to enforce her copyrights *either* by pursuing a civil copyright infringement claim in federal court *or* by pursuing a claim in an administrative dispute resolution proceeding before an administrative law judge in the Copyright Office.[271]

Consistent with the original intent of the UDRP, the administrative proceeding would be available only for relatively straightforward claims of copyright infringement. To start, the process should be available only against those alleged to have uploaded copyrighted works to a p2p network and thus made them available for downloading by others.[272] Making a copyrighted work available for any other person to copy is much more likely to constitute copyright infringement than is any individual instance of downloading, where the downloader's act of reproduction might well be excused as fair use or by some other defense. The potential for justifiable instances of downloading means that keeping the dispute resolution procedure streamlined would require a focus on much less defensible acts of uploading.[273]

Even with respect to uploading, the potential that an uploader's conduct might be noninfringing is likely to be inversely proportional to the number of works uploaded and made available. Someone who has uploaded only one or even 10 copyrighted works may well be engaged in copyright infringement, but she is less clearly infringing than someone who has uploaded 1000 or even 100 works. In order to restrict the dispute resolution process to conduct that is fairly clearly infringing, the process should be available only in cases where evidence shows that the person targeted has uploaded to a p2p network at least one copy of at least 50 copyrighted works during any 30-day period.[274]

A copyright owner whose claim comes within the scope of the administrative procedure would have to put forth a prima facie case of copyright infringement. The copyright owner would need to show that it has

271. Legislation that would create administrative law judge positions in the Copyright Office for another purpose passed the House in early 2004 and seems likely to pass in the Senate as well. *See House Passes Bill On Copyright Royalty Distribution Reform*, 67 PAT., TRADEMARK & COPYRIGHT J. (BNA) 392 (March 5, 2004).

272. While we anticipate that administrative infringement claims will primarily involve the uploading of musical recordings, the procedure would also be available in cases involving other types of copyrighted works, and we suspect that owners of copyright in motion pictures and software might be particularly likely to use the system. *See* Heingartner, *supra* note 146 (reporting that 88% of files on p2p networks are music and video, with the remaining 12% including "software and 'everything else'").

273. *See supra* note 116.

274. Admittedly, any threshold can be gamed, and it may be that everyone will upload only 49 songs in order to avoid liability under our administrative regime. But even stopping high-volume uploading would be a partial victory for copyright owners, and if it was not enough they could always bring lawsuits, with potential ordinary statutory damage awards ranging from $36,750 to $1.47 million for uploading 49 works.

registered claims of copyrights in the works in question.[275] In addition, the copyright owner would need to provide a sworn statement that it owns the copyright (or the relevant exclusive right) in the works identified. Next, the complainant would have to provide evidence that the works complained of were available for downloading from a particular IP address at a particular date and time. Such evidence could consist of, for example, screen shots showing the availability of files and a sworn statement that the copyright owner determined that the titles listed were actually available and were actually copies of the copyrighted works.

Finally, the copyright owner would need to provide evidence showing that the particular IP address in question was, at the time in question, assigned to the person against whom the dispute is brought. This would normally be shown through evidence obtained from the ISP that controls the address. In the civil suits brought initially by the RIAA, the information identifying the alleged uploader was generally obtained by using a subpoena process provided for under the OSP safe-harbor provisions added to the Copyright Act by the DMCA.[276] Section 512(h) allows any copyright owner to request any U.S. district court clerk to issue a subpoena to any online service provider to identify an alleged infringer. The use of that provision has been quite controversial. As a matter of statutory interpretation, the text is ambiguous as to whether its provisions apply to every online service provider or only to providers engaged in certain kinds of activities. The D.C. Circuit recently rejected efforts by the RIAA to apply the DMCA subpoena provisions to OSPs that provide mere conduit services.[277] Constitutional concerns have also been raised over the fact that copyright owners can obtain subpoenas from the court clerk when no actual litigation under the supervision of a judge is pending in that court (or, indeed, in any court).[278] And the concerns are heightened by the fact that the real target of the subpoena—the alleged infringer who is to be identified by the OSP—may not even be aware of the subpoena in order to attempt to challenge the copyright owner's right to the information before her identity is disclosed.

Regardless of what ultimately happens in the current challenges to the DMCA's subpoena provisions,[279] the dispute resolution process we propose

275. Or at least has complied with the registration requirement for suit, which technically requires only an attempt to register and a negative response from the Copyright Office. 17 U.S.C. § 411(a) (2004). For works whose registrations are available in the online database of the U.S. Copyright Office, the copyright owner might only be required to provide the title of the work, the name of the author, the name of the copyright claimant, and the date and number of registration, rather than a copy of the actual certificate.

276. *Id*. § 512(h). On the OSP safe harbors generally, see *supra* Part I.C.

277. RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003).

278. *See, e.g.*, Pac. Bell Internet Servs. v. RIAA, No. C03-3560 SI, slip op. (N.D. Cal. Nov. 26, 2003) (procedural ruling on a suit challenging the constitutionality of the Section 512(h) subpoena provision).

279. The ruling by the D.C. Circuit has not prevented the RIAA from continuing to pursue lawsuits against high-volume uploaders. In January and February 2004, several

depends on copyright owners being able to identify the individuals engaged in high-volume uploading. The process might well allow this to occur under somewhat greater supervision than currently provided for in Section 512. The process could allow copyright owners to file a claim against a particular unidentified alleged uploader. Once the copyright owner provided evidence of the registration of its copyright claims, and of the availability of its works at a particular IP address at a specific time, the administrative judge could authorize the issuance of a subpoena, in aid of the existing proceeding, ordering the ISP to identify the customer who was using that address at that time.[280] This would provide at least some supervision to ensure, before an ISP is ordered to disclose the identity of its customers, that the party seeking the identification is a copyright owner with a prima facie claim of copyright infringement by the customer. In addition, it may be advisable to require the ISP to notify the customer whose identity is sought and give that person a short time period in which to challenge the subpoena if she wishes to do so.

Once the copyright owner has established this prima facie claim of infringement and identified the uploader, the uploader would have the opportunity to rebut or defend against the claim. In order to keep the process streamlined and focused on straightforward cases of infringement, an administrative judge should reject, without prejudice, any claim by a copyright owner that presents plausible legal or factual issues as to the uploader's liability. For example, a plausible claim of mistaken identification of the assignment of an IP address might be shown where the copyright owner alleges that a person uploaded works at a particular IP address using Windows-based software, but where the person accused of uploading can show that she only uses an Apple computer incapable of running the software she is alleged to have used.[281] Resolution of such disputes is better handled in an ordinary court

consolidated "John Doe" lawsuits were filed alleging copyright infringement occurring at particular IP addresses. After filing the suits, the plaintiffs have sought subpoenas against the ISPs controlling those IP addresses, in order to identify the particular person using those addresses. *See* John Borland, *RIAA Steps Up File-Trading Suits*, CNET NEWS.COM, Feb. 17, 2004, *available at* http://news.com.com/2100-1027-5160262.html (last visited Apr. 4, 2004); John Schwartz, *Music Industry Returns to Court, Altering Tactics on File Sharing*, N.Y. TIMES, Jan. 22, 2004, at C1, C8. At least one court has ruled that a consolidated suit naming a couple hundred "John Does" is improper and that copyright owners must file a separate suit against each individual "John Doe" alleged to infringe, thus raising the cost of court enforcement efforts even more, given the $150 filing fees required for each case in at least one district court. Katie Dean, *One File Swapper, One Lawsuit*, WIRED.COM, Mar. 8, 2004, *available at* http://www.wired.com/news/digiwood/0,1412,62576,00.html (last visited Apr. 4, 2004).

280. This would essentially replicate in the administrative process the procedures being used by the RIAA in identifying infringers after the D.C. Circuit limited the availability of subpoenas under Section 512(h).

281. *See supra* note 236. *But see* John Borland, *Macintosh Users Join Kazaa Network*, CNET NEWS.COM, Nov. 19, 2003, *available at* http://news.com.com/2100-1027-5109645.html (last visited Apr. 4, 2004) (noting release of new software enabling Macintosh users to download from, and in some cases upload to, p2p networks originally available

proceeding, and the administrative judge should have the power simply to dismiss such claims without prejudice to a civil suit on the same grounds.

In addition to this general authority for the administrative judge to reject claims that do not involve fairly clear cases of infringement, it may be useful for the statute to specify certain cases that the judge *must* reject. A prime example would be a claim involving the uploading only of works that are out of "print" and unavailable from the copyright owner. Those circumstances may present the strongest argument in favor of finding that uploading works to a p2p network constitutes fair use.[282] While this fair use argument is not clearly correct, it is at least sufficiently plausible that it should be considered and resolved in the first instance by a court, rather than by the administrative dispute resolution process. Similarly, if the person accused of uploading can show that the works were made available simultaneously with substantial comment or criticism, the potential for the accused to make out a viable fair use claim would counsel for court resolution of the case and mandatory rejection of the administrative claim.[283]

For the process to work, however, it must be able actually to resolve clear cases of infringement by uploaders. If every uploader against whom a claim was filed could simply assert a defense and have the claim dismissed, the system would never succeed.[284] Thus, an uploader must provide evidence to support a claim of, for example, mistaken identity or uploading only out-of-print works. In addition, there may be certain legal defenses that should not be

primarily to users of Windows computers). To reduce the risk that a defendant would falsely assert such a claim, factual statements by parties to the administrative process should be made under penalty of perjury.

282. *Cf.* Michael J. Madison, A Pattern-Oriented Approach to Fair Use 4 (2003) (unpublished manuscript, on file with authors) (suggesting that courts have erroneously concluded that p2p file sharing can never be fair use).

283. Another type of claim that should be rejected from the administrative procedure would be one involving the uploading of unpublished and confidential documents for reasons of public discussion or commentary. In late 2003, copies of internal memoranda by employees of Diebold, a company that produces electronic voting equipment, began circulating on the Internet. Those who had found and circulated the memos did so because they believed the memos showed problems with the company's voting systems that raised questions about whether those systems should be adopted. Diebold responded by claiming infringement of its copyright in the memos and threatening action against, among others, ISPs who provided connection and storage services to those posting the memos. *See* John Schwartz, *File Sharing Pits Copyright Against Free Speech*, N.Y. TIMES, Nov. 3, 2003, at C1. While it is not clear that the dispute involved any postings to p2p networks, it is quite easy to imagine the documents finding their way onto such a network, raising the possibility of a claim under our proposed dispute resolution system. The streamlined process we propose is not the place to resolve the difficult questions involved in these types of cases involving unpublished confidential copyrighted material, which may often involve privacy and free speech issues.

284. One defendant in such a suit has counterclaimed under RICO, claiming that a pattern of suing people and then agreeing to settle with them was an act of racketeering. *See Recording Industry Countersued*, N.Y. TIMES, Feb. 19, 2004, at C9. Such far-fetched claims should not gum up the works of the administrative dispute resolution system.

resolved by the dispute resolution procedure but that also should not result in the claim simply being dismissed and the copyright owner relegated to a civil infringement suit. For example, an uploader might claim that the copyright owner is engaged in copyright misuse and is therefore not entitled to enforce the copyrights until the misuse has been purged. Or the uploader might claim that the copyrights are unenforceable because of alleged fraud in registering the works as works made for hire; with respect to sound recordings, the question of whether those recordings can qualify as works made for hire has been controversial.[285] Because these are complicated issues that should be resolved in court rather than in the dispute resolution process, and because allowing the mere assertion of such a defense to take a claim outside the dispute resolution process would threaten to make it impossible to hear any claims in the process, an alternative is required. We propose that if such defenses are raised in the dispute resolution process, the administrative judge should decline to decide the defenses, proceed to consider all other aspects of the case, and if she awards a decision against the uploader, stay her decision for thirty days to allow the uploader time to bring a declaratory judgment suit in court asserting the defenses. An uploader who seriously wishes to pursue these defenses would be able to do so in the proper forum for considering them, but mere assertion of the defense in the administrative forum would not prevent that forum's consideration of the dispute.

In order to make the results of the administrative proceeding as consistent and fair as possible, initial decisions should be subject to an administrative appeal to a panel of administrative judges. This would allow for an additional layer of review but in a somewhat streamlined format. Any party that was dissatisfied with the outcome of a complaint on appeal would then have the option of bringing the dispute to a district court for review. In order to discourage groundless appeals, a party that brings an unsuccessful appeal could be required to pay the costs of the appeal.

The administrative dispute resolution procedure we propose would provide a quicker, lower-cost alternative for copyright owners to enforce their rights against individual large-scale infringers on p2p networks. To be effective, the process must be streamlined. Both parties should have an opportunity to present evidence and argument online, but there should not be face-to-face argument or

285. Many sound recording copyright owners have represented the works they registered as works made for hire. Congress changed the statute to make specially commissioned sound recordings expressly eligible to be works for hire in 1999, but reversed the change in 2000, leaving open the question of whether commissioned sound recordings qualify as works made for hire under some other category of work. 17 U.S.C. § 101 (2004); Pub. L. No. 106-113, § 1000(a)(9), 113 Stat. 1501 (1999); Pub. L. No. 106-379, § 2(a)(1), 114 Stat. 1444 (2000). For a detailed discussion of these issues, see David Nimmer & Peter S. Menell, *Sound Recordings, Works for Hire, and the Termination-of-Transfers Time Bomb*, 49 J. COPYRIGHT SOC'Y 387 (2001); David Nimmer, Peter S. Menell & Diane McGimsey, *Preexisting Confusion in Copyright's Work-for-Hire Doctrine*, 50 J. COPYRIGHT SOC'Y 399 (2003).

discovery of the sort that exists in civil litigation. The decisionmaker's job should be relatively straightforward: rejecting claims that do not fit within the system's requirements or with plausible disputes of law or fact that are better resolved in court, and determining whether the plaintiff has proved its charges of infringement. The judges should be obligated to issue a short written decision within two months after the case is submitted. While this may sound like an unrealistic goal to those whose experience is with the expensive, drawn-out system of civil litigation in the United States, the success of the UDRP in resolving over 7500 domain name disputes in the last four years suggests that the goal of quick and cheap resolution is workable. Provided the copyright dispute resolution system avoids the obvious mistakes of the UDRP—systematic bias of judges, lack of an administrative appeal, and a tendency to resolve difficult questions best left for the courts[286]—it should prove an attractive alternative to litigation for copyright owners and not unfair to accused infringers.

Making the procedure attractive to copyright owners as an alternative to criminal or civil infringement suits and to suits against facilitators will also require that the procedure provide an adequate remedy. We suggest that the process provide two types of remedies: monetary relief and the official designation of an unsuccessful defendant as an infringer.

Monetary penalties should be sufficiently large that the possibility of having uploading challenged in the administrative procedure serves to deter others from engaging in large-scale uploading. As noted above, the existing maximum penalties available in civil actions under the statutory damage regime seem likely to provide far in excess of the penalties needed to have a deterrent effect. It seems likely that in cases involving the uploading of 50 or more works, a penalty on the magnitude of $250 per work infringed would have a strong deterrent effect.[287] Someone who uploaded 1000 songs—the threshold used by the RIAA in its initial lawsuits—would face $250,000 in liability. While statutory damages could provide an award that is 120 times greater, even the $250,000 award from the administrative process would likely be beyond the ability of most uploaders to pay, suggesting that the higher award is not needed. Even someone who just met the administrative threshold of uploading fifty works would face $12,500 in liability. The potentially lesser deterrent effect of the lower penalty would be offset by the increased likelihood that any particular uploader would face enforcement action, since the administrative procedure would make enforcement quicker, cheaper, and easier and would allow

286. On these shortcomings, see, for example, Froomkin, *supra* note 269; Geist, *supra* note 268.

287. The Copyright Act's statutory damage provisions have generated some uncertainty as to whether the song or the CD is the appropriate "work" to use as the basis for calculating damages per work infringed. *See* 17 U.S.C. § 504(c) (2004). In the administrative procedure, each particular song (in the case of music infringement) seems to be the appropriate unit on which to assess the penalty.

copyright owners to bring claims against greater numbers of uploaders. The fact that when the RIAA did in fact begin to sue uploaders in court, it settled with many of them for only a few thousand dollars despite the higher cost of litigation suggests that the RIAA was satisfied with the deterrent effect of even these low penalties.[288] Making enforcement more likely but the penalties less draconian may also blunt criticism that the RIAA is unfairly singling out particular individuals for doing what countless others have gotten away with.

While an uploader must have uploaded at least fifty works in order to be subject to the dispute resolution procedure, any actual monetary award imposed on the uploader would of course include only those works owned by the complaining copyright owner or owners. Still, copyright owners have an incentive to cooperate in bringing a single complaint, sharing the costs of each administrative adjudication, and receiving an award for their particular works.[289] This should decrease the likelihood that an uploader would have to face repeated claims from multiple copyright owners based on the same course of conduct. Indeed, the recording industry's first wave of lawsuits against uploaders appears to have operated this way, with all of the affected major record labels joining in a single action against particular downloaders. To the extent that the possibility of multiple claims against a single uploader based on the same course of conduct remains a concern, the procedure could be available only if the uploader has made available on a p2p network fifty copyrighted works *of the complaining copyright owners*. This would provide an incentive for copyright owners to cooperate in bringing a single suit, since in many cases an uploader may well have made available too few works owned by any one copyright owner to allow an individual copyright owner to pursue a claim but will still have uploaded enough works so that a claim can be brought if

288. *See* John Borland, *New RIAA File-Swapping Suits Filed*, CNET NEWS.COM, Mar. 23, 2004, *available at* http://news.com.com/2100-1027-5177933.html (last visited Apr. 4, 2004) (reporting more than 400 settlements of RIAA lawsuits, with payments averaging $3000); Cynthia L. Webb, *Settling in with the RIAA*, WASHINGTONPOST.COM, Sept. 30, 2003, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A21601-2003Sep30?language =printer (last visited Apr. 4, 2004) (reporting settlements in 52 of 261 initial RIAA lawsuits against p2p users, with payments ranging from $2500 to $10,000).

289. A related issue arises when more than one person owns overlapping rights in the same copyright. For a description of how this often occurs, see Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet,* 22 U. DAYTON L. REV. 547 (1997); Lydia Pallas Loren, *Untangling the Web of Music Copyrights*, 53 CASE W. RES. L. REV. 673 (2003). This situation is particularly common with respect to music recordings, which typically involve separate copyrights in a musical composition and a sound recording, generally owned by different parties. *See* Reese, *supra* note 116, at 240-41. We would address this problem by permitting any copyright owner whose rights are infringed to file a complaint but permitting only one such complaint per defendant per work. In other words, just as joint owners of copyright each have the right to exploit the work subject to an accounting to their coowners for profits, any of the owners can bring an administrative claim. But once a claim has been brought regarding an act of infringement, other owners can't file a new complaint against the same uploader for the same acts, and they would have to seek a share of their compensation from the recovering copyright owner.

copyright owners act jointly.

Copyright owners would, of course, have to enforce administrative awards against uploaders. In some cases, no doubt, the losing uploader would voluntarily comply with the award to the extent she is able to do so. In other cases, the copyright owner might need to go to court in order to execute on the administrative award. While this might entail some expense, enforcing a judgment is usually simpler and cheaper than litigating a civil case to judgment in the first place. And the copyright owner's burden of executing on a judgment against an infringer should not be significantly different in the case of an administrative award than in that of a court judgment of infringement. The formal procedures for enforcing judgments (as well as the costs of doing so) vary by state and range from ineffectual to fairly draconian. Enforcement can involve measures such as garnishing the defendant's wages and placing liens on her property, though many high-volume uploaders may be college students or young people with limited wages and property available to satisfy a judgment through such measures. But even where executing on an administrative infringement judgment proves difficult or expensive, copyright owners can notify credit reporting agencies of the unpaid judgment. This relatively inexpensive step may make it more difficult or costly for the infringer to obtain a credit card, an auto loan, or a home mortgage—giving even an uncollectible infringement award some deterrent effect among high-volume uploaders who enjoy or look forward to a middle-class lifestyle.

The dispute resolution process would also offer an important form of nonmonetary relief. An uploader against whom a copyright owner brings a successful claim would also be officially designated by the administrative decision as a copyright infringer. This designation is important because it has consequences for the safe harbors for OSPs provided for under the DMCA. The DMCA grants safe harbors to OSPs only if they have in place and reasonably implement a policy for terminating the accounts of "repeat infringers" in appropriate circumstances.[290] No one seems to know what makes one a "repeat infringer," however.[291] Copyright owners have read the term broadly, to include anyone who is the subject of two allegations of infringement made by a copyright owner to an OSP under the DMCA, and possibly even anyone who has posted two or more allegedly infringing works at one time.[292] It seems

290. 17 U.S.C. § 512(i)(1)(A) (2004).

291. On the ambiguities in the meaning of the DMCA, see David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909 (2002).

292. On these interpretations, see Ian C. Ballon & Keith M. Kupferschmid, Third Party Liability Under the Digital Millennium Copyright Act: New Liability Limitations and More Litigation for ISPs 6-7 (2004) (unpublished manuscript, on file with authors). The district court in *Napster* held that there was a genuine issue of fact as to whether Napster had in fact adopted an effective policy for terminating repeat infringers but did not itself decide what the term meant. A&M Records Inc., v. Napster, Inc., No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, at *28 (N.D. Cal. May 5, 2000). For criticism of this broad interpretation of the

wrong, though, to say that one is an infringer merely by virtue of receiving a cease and desist letter, which some content owners have been sending with reckless abandon and which need not even meet the standards of Rule 11.[293] The other extreme—that one is not an infringer until adjudicated so by a court, and so repeat infringers must be sued to final judgment and lose twice—seems equally unworkable. The administrative procedure provides a middle ground, by allowing a relatively quick determination by a neutral third party that an individual is in fact an infringer. Keying the termination obligation to an administrative finding would protect the due process rights of those wrongfully accused of infringement without rendering the repeat infringer provision virtually ineffective.

If an uploader was twice the subject of a successful complaint in the administrative process, then the uploader would qualify as a "repeat infringer." As a result, an OSP that wanted to remain eligible for the benefits of the safe harbors would need to stop providing service to that uploader. The most obvious application of this provision in the p2p context would be to centralized p2p service providers, such as the original Napster, who can exclude individual users from participation in their networks.[294] This ability to exclude could provide an effective sanction against a user found to be a repeat infringer. Of course, most p2p networks today are more decentralized than Napster was (though it is unclear to what extent that is because decentralization is a technologically superior alternative and to what extent it is because of court decisions on the indirect copyright liability of centralized systems).[295] But

term "repeat infringer," see MELVILLE NIMMER, NIMMER ON COPYRIGHT § 12B.02[B][2] & n.54 (1978); David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC'Y 401, 452 n.244 (1999).

293. For example, copyright owners have sent cease and desist letters to students posting book reports about copyrighted books and to people who have the misfortune to share the last name of a musician. *See* Dave Farber*, RIAA Apologizes to Penn State for Confusing Usher with Prof. Usher*, *at* http://www.interesting-people.org/archives/interesting-people/200305/msg00117.html (last visited Apr. 26, 2004); *Music Industry Sues for Names of Copyright Violators*, *at* http://www.foxnews.com/story/0,2933,64771,00.html (last visited Apr. 26, 2004) (documenting cease and desist letter sent to a child who wrote a book report about Harry Potter). Surely a recidivist writer of Harry Potter book reports is not a "repeat infringer" merely because Scholastic sends two mistaken cease and desist letters. *See also* Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 62-67 (2003) (discussing the obligation to terminate repeat infringers and the Catch-22 imposed if doing so is used as evidence of the right and ability to control a network).

294. In the case of Napster, for example, because the system operated by maintaining a centralized directory of files available on users' computers, users had to connect to Napster's centralized directory in order to locate other users and their files. As a result, Napster was in a position to screen users when they attempted to connect and to select which users could or could not access the directory.

295. *See, e.g.*, Wu, *supra* note 118 (arguing that distributed p2p networks evolved as a reaction to the success of legal challenges to centralized p2p networks). The popularity of Napster during its heyday suggests that centralized p2p networks may well be viable technological and business models in the absence of the prospect of liability for all infringing

being designated a repeat infringer would have serious consequences for participants in decentralized p2p networks as well. Because the requirement to terminate repeat infringers applies to all of the safe harbors, even an OSP that does nothing more than provide Internet connectivity would not be able to keep the repeat-infringing uploader as a customer and enjoy the safe harbor. While the uploader might simply switch to another service provider, that provider would be similarly obligated to terminate the uploader's service. As a consequence, the uploader might not be able to obtain Internet access (or other Internet services covered by the safe harbors).

Given the increasing importance of online activity in our society, the possibility of losing Internet access should provide an additional deterrent to potential high-volume uploaders. At the same time, we should be concerned about the possibility that some substantial number of people might be denied online access entirely.[296] It is possible that ISPs will arise that are willing to forego the benefits of the safe harbors and face potential copyright infringement liability in order to provide service to repeat infringers; presumably those ISPs will charge higher costs to compensate them for the risk that their repeat-infringing subscribers will again engage in infringement and the ISP will be held liable for that infringement. It also seems possible, however, that those designated as repeat infringers by the administrative process would simply be unable to obtain any Internet service at all; it is by no means clear that some ISPs would choose to take the risk of foregoing the safe harbor. We are not certain that even someone who has twice engaged in egregious uploading should be permanently barred from the Internet. It may well be that the designation as a repeat infringer, or the requirement for ISPs to terminate repeat infringers' accounts, should carry some time limitation, so that after, for example, five years, a repeat infringer could again become a customer of Internet services without the provider of those services losing the benefit of the safe harbor.

A final consideration is the cost of the administrative dispute resolution proceedings. While these costs should be significantly lower than those of litigation because of the streamlined and largely online nature of the proceedings, there will still be costs to be paid. In order to encourage copyright owners to pursue this process rather than court actions, and to enhance the deterrent value of successful claims against high-volume uploaders, the costs of a successful infringement claim could be assessed against the infringing

use by network users.

296. This concern might be alleviated somewhat by the fact that the termination obligation only applies to *repeat* infringers, so that denial of online access would occur where an individual was determined by the administrative process to have engaged in large-scale infringement and then subsequently determined to have engaged in such conduct a second time. We might further require that any second determination be based on conduct that occurs after the date of the first administrative decision declaring the uploader to be an infringer.

uploader. In many cases, perhaps, the uploader will be unable to pay the full amount of the award against her even before costs are added, so there may be many cases in which copyright owners will not be able to recover costs from the infringer. Nonetheless, the possibility of recovering the costs of the claim (as well as the fact that in such a situation, those costs, where not practically recoverable, are likely to be lower than the equally unrecoverable costs of a civil suit) should help encourage copyright owners to pursue claims in the administrative process. By the same token, unsuccessful copyright owners should in appropriate circumstances be obligated to pay the accused infringer's costs. Awards of costs are routine in civil litigation; the fact that the UDRP imposed no penalty whatsoever on unsuccessful and even bad-faith allegations of infringement is one of its shortcomings.[297]

We believe that the dispute resolution procedure we have proposed would make it possible for copyright owners to obtain effective relief against individuals engaged in relatively egregious acts of copyright infringement without the costs and delay of litigation, while at the same time reducing the potentially enormous penalties facing the few high-volume uploaders targeted by lawsuits or criminal prosecutions seeking to generate deterrence. Some people may still have concerns about the harshness of the penalties—both in dollar amounts and in "exile" from the Internet—possible under the system we propose. One way to alleviate that concern would be to make the system prospective—to apply it only to acts that occur after a date specified in the legislation establishing the system.[298] The publicity that has accompanied the controversies over music on p2p networks, and that would no doubt accompany

297. *See* Froomkin, *supra* note 269. Appropriate circumstances would include complaints that are rejected because the works involved are not available from the copyright owner or are disseminated by the uploader for purposes of commentary or criticism.

298. This might relieve one specific concern about the harshness of the penalties: The concern that some high-volume uploaders may have acted unknowingly, since some p2p software automatically makes every file downloaded by a user available for uploading by other users. In some instances, this automatic sharing appears to be a default setting when the software is installed. As a result, a user might do nothing more than install p2p software and download numerous files and yet be engaged without her knowledge in high-volume uploading. (Of course, such an uploader would still be liable for copyright infringement, since the statute penalizes both knowing and unknowing infringement, *see supra* note 198, though the amount of statutory damages awarded against the unknowing uploader might be smaller.) Given the widespread publicity over suits against individuals for uploading, making harsh penalties for high-volume uploading in an administrative system prospective rather than retrospective should provide sufficient notice to encourage most people to check their system settings so that those who upload large numbers of works are likely to be doing so knowingly. Indeed, in the wake of the RIAA's first lawsuits, P2P United, a group representing several major p2p software providers, announced a code of conduct that would involve providers modifying their software to include warnings against copyright infringement, to make uninstalling the software easier, and to help enable parents to prevent children from sharing files. David McGuire, *Song-Swap Networks Unveil Code of Conduct*, WASH. POST, Sept. 29, 2003, at D1. Alternatively, the administrative process might be limited to instances in which the complaining copyright owner notified an individual of her p2p uploading activities and those activities continued after the notification.

the enactment of the dispute resolution system we propose, would serve to put most people on notice that moderate- to high-volume uploading is infringing activity and could result in severe penalties. Because copyright owners have seemed more concerned about trying to cut off infringing activity on p2p networks than about actually collecting monies for all or most acts of past infringement, a system that operates prospectively may sufficiently address their most significant concern.[299]

The administrative dispute resolution system that we propose is flexible enough to be part of a number of different approaches to the problem of copyright infringement on p2p networks. The system could serve, as we have suggested, as a substitute for holding p2p providers liable for infringement committed by their users; indeed, Congress could provide, in enacting such a system, that providers would not be liable for user infringements if the network is capable of substantial noninfringing use. The system would also serve, in most cases, as a substitute for civil or criminal enforcement against infringers on p2p networks, not because civil or criminal suits would be unavailable but because administrative proceedings would be less costly and more efficient. Even if the existing legal rules governing secondary liability in the p2p context are not changed, the administrative system may be important. Under the caselaw at the moment, centralized systems such as those in *Napster* and *Aimster* would have a high burden to police infringement on their networks to avoid liability, while producers of software for decentralized systems, such as those at issue in *Grokster*, would not face liability for their products. While these rules are likely to make centralized systems infeasible, decentralized systems are likely to flourish, and copyright owners will need to target their enforcement efforts at direct infringers. Our proposed administrative system would reduce the cost of those efforts for copyright owners and would substantially reduce the potential penalty for the direct infringers who are pursued.

The system could also be part of an approach that imposed levies to compensate copyright owners. If a levy is mandated, it would authorize all uses of p2p networks in return for the levy payments, and there would be no need for the system we propose. But if a levy were adopted on an opt-in basis, only levy-paying users, or customers of ISPs or other providers that had paid the levy, would be immune from suit, and our administrative remedy could be used for disputes outside the levy system. Along these lines, Jessica Litman has proposed an "opt out" levy system in which copyright owners could affirmatively choose to make their works ineligible for dissemination pursuant to the levy and could pursue enforcement actions against those who uploaded

299. Of course, so long as the statute of limitations has not expired, litigation would be available to those copyright owners who do wish to try to recover monetarily for previous infringements on p2p networks.

their works;[300] our administrative procedure could reduce enforcement costs in those circumstances.

Similarly, the administrative system could be part of a filtering approach. Despite our skepticism about the potential for filtering,[301] a viable technology might emerge for filtering unauthorized uses of copyrighted material on p2p networks. Given concerns about technological mandates, particularly mandates of any particular firm's technology, Congress might prefer not to require that every p2p software developer or every ISP adopt specific filtering technology. Congress might instead strongly encourage the use of filters by granting immunity from copyright infringement actions to those using p2p software or networks that incorporate the filters. To make the incentive effective, the threat of enforcement against those committing copyright infringement on unfiltered networks would need to be realistic, and far more enforcement actions could likely be pursued under a streamlined administrative system than in court.

A final approach in which our proposed administrative system might also be useful is voluntary collective licensing for using music in p2p networks. The Electronic Frontier Foundation (EFF) has proposed such a system.[302] The proposal envisions virtually all music copyright owners voluntarily forming a licensing collective that would offer a blanket license for p2p dissemination of their works on a per-person, per-month basis and that would distribute the license fees to copyright owners. The proposal envisions that users would have an incentive to take the license in order to avoid the legal threat of otherwise being sued for infringement[303] and that copyright owners would continue to be able to bring enforcement actions against p2p users who do not take a license. Our proposed administrative system would offer copyright owners a realistic possibility of enforcing against large numbers of unlicensed p2p users, thus increasing the incentive for individuals to buy a blanket p2p license.[304]

C. *Providing Legitimate Alternatives*

Any approach for dealing with large-scale infringement over p2p networks by targeting enforcement efforts at individuals who commit such infringement

300. Litman, *supra* note 178, at 31-35.

301. *See supra* text accompanying note 155.

302. ELEC. FRONTIER FOUND., A BETTER WAY FORWARD: VOLUNTARY COLLECTIVE LICENSING OF MUSIC FILE SHARING (Feb. 2004), *available at* http://www.eff.org/share/collective_lic_wp.pdf (last visited Apr. 4, 2004).

303. *Id*. at 2 ("[T]hose who today are under legal threat will have ample incentive to opt for a simple $5 per month fee.").

304. The major performance rights collective licensing societies, ASCAP and BMI, use civil infringement actions to stop public performances of their works by those who refuse to buy a license and thus deter others from unlicensed public performances. The number of potentially unlicensed public performers, though, is much smaller than the number of potentially unlicensed p2p music users, suggesting that a streamlined administrative proceeding would be more useful than court actions in sanctioning the latter.

will be more effective if the deterrent impact of enforcement actions is combined with the availability of legitimate alternatives for online music dissemination.[305] The rational actor deciding whether or not to engage in p2p infringement should be less likely to do so, given the risks of enforcement and the potential sanction, if a legal alternative provides a reasonable substitute for obtaining online access to music. As Ann Bartow has suggested, most Americans are law abiding most of the time and "[a]s long as it is reasonably convenient, efficient, and economical to gain access to [copyrighted content by legal means], then few people are likely to invest a lot of time and energy in obtaining [the content illegally]."[306]

Efforts at developing attractive and affordable online music dissemination services have really only begun in earnest in the last year or so.[307] These efforts have enjoyed some initial success, though they have also earned criticism on grounds such as the selection of music available, limitations imposed on customers' use of that music, pricing, and usability.[308] The potential business models for legitimate online music services are numerous and several different such models might simultaneously prove viable in the marketplace.[309] Our point here is not to canvass or evaluate those models and their chances for success, but only to emphasize that reducing infringement on p2p networks through enforcement efforts against those who actually infringe will be more successful if those who are given pause by the potential sanctions for infringement have somewhere else to turn for reliable, affordable online access to a wide variety of high-quality digitally formatted music. As the head of a p2p monitoring firm has said, "[t]he only way to really marginalize online piracy is to make online retail so transparent, so convenient and so appealing that when you're faced with two icons—one that's an unknown, perhaps virus-infested crack on Kazaa, and the other that's double-click to download the legitimate version," users will choose the latter.[310]

D. *Can Enforcement Work on the Internet?*

A policy of targeting direct infringers is workable only if enough of those

305. Music is not the only copyrighted content disseminated on p2p networks, but it is the primary content. *See supra* note 272.

306. Ann Bartow, *Arresting Technology*, 1 BUFF. INTELL. PROP. L.J. 95, 118-19 (2001).

307. *See supra* note 32.

308. *See, e.g.*, Neil Strauss, *Online Music Business, Neither Quick Nor Sure*, N.Y. TIMES, Oct. 29, 2003, at B1, B5.

309. These models might include dissemination over p2p networks that is authorized, either because the files disseminated are copy-protected and require permission or payment to use, *see* John Borland, *Kazaa to Launch P2P Print Ads*, CNET NEWS.COM, Nov. 12, 2003, *available at* http://news.com.com/2100-1025-5106581.html (last visited Apr. 4, 2004) (discussing efforts of owner of Kazaa software to promote dissemination of protected files), or because the operator of the p2p network has obtained licenses from copyright owners.

310. Heingartner, *supra* note 146 (quoting Eric Garland, CEO of BigChampagne).

direct infringers can be found and brought to justice to substantially deter others. Surely, one might object, the Internet makes this infeasible. After all, among the most celebrated characteristics of the Internet are its international character and the potential for anonymity.[311] On the Internet, the saying goes, no one knows you're a dog.[312] A common argument against enforcement of intellectual property law online has been that infringers will simply move offshore[313] or conceal their identity using unbreakable encryption.[314] If enough p2p uploaders do so, enforcement targeted at those uploaders will fail.

Infringement abroad and anonymity will undoubtedly limit the efficacy of efforts to target large-scale direct infringers on p2p networks to some extent. We are skeptical that these effects will be substantial enough to prevent effective enforcement, however, for three reasons. First, the same objections can be made to efforts to sue facilitators. If individual uploaders can move offshore or conceal their identity, so too can at least some facilitators. Specifically, facilitators whose primary business is making software can easily relocate, and if the software will be provided for free they can release the program anonymously.[315] Indeed, these challenges to enforcement may be more daunting when suing facilitators than when targeting direct infringers. A company that expects to be sued has significant incentives to incorporate in a foreign jurisdiction and to keep all assets and personnel outside the United States and perhaps also has the resources to do so. A college student is unlikely to move overseas in order to be able to continue to upload music. If facilitators

311. *See, e.g.*, Froomkin, *supra* note 263; A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, U. CHI. LEGAL F. 139 (1996).

312. *See* Peter Steiner, *69:20*, NEW YORKER, July 5, 1993, at 61.

313. *See, e.g.*, Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 162 (1999); Matthew V. Pietsch, *International Copyright Infringement and the Internet: An Analysis of the Existing Means of Enforcement*, 24 HASTINGS COMM. & ENT. L.J. 273 (2002); *cf.* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 94 (2001) (making the same argument for criminal conduct online).

314. U.S. DEP'T OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (Mar. 2000) (report of the President's Working Group on Unlawful Conduct on the Internet), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last visited Apr. 4, 2004); David Friedman, *A World of Strong Privacy: Promises and Perils of Encryption*, 13 SOC. PHIL. & POL'Y 212 (1996) [hereinafter Friedman, *Strong Privacy*]; David Friedman, *Does Technology Require New Law?*, 25 HARV. J.L. & PUB. POL'Y 71 (2001).

315. Other facilitators, such as ISPs and others who charge their customers, will obviously find it difficult to conceal their identity from those customers. And some large facilitators will be unwilling to relocate in order to avoid liability. *See, e.g.*, http://www.earthstation5.org (last visited Apr. 4, 2004) (a new p2p network based in the Jenin refugee camp in Palestine).

are as likely or more likely than individuals to escape justice in these ways, these concerns do not justify a policy of suing facilitators rather than individual uploaders.

Second, neither anonymity nor moving offshore is nearly as easy to implement as first-generation Internet scholars have predicted.[316] To take the more obvious case first, physical relocation to another country imposes huge burdens.[317] Existing individual uploaders are unlikely to view the "benefits" of providing digital music for free to strangers as worth the major economic, social, and cultural costs of a move. This leaves the possibility that new uploaders will spring up in those countries to take the place of those who are deterred. This is a potential risk: Traditional (nononline) piracy is much more common in some countries than in others, and the Internet may permit infringement that occurs at that higher rate to be transmitted internationally. But even this risk seems overstated, because many of the countries that lack modern copyright laws (or effective enforcement of them) also lack the wealth and Internet infrastructure to support a large number of large-scale uploaders. Nor will geographic indeterminacy necessarily permit uploaders to evade local laws; most IP addresses can ultimately be traced via the ISP or network owner to a user who has provided a geographic address, and in any event a wealth of new technologies permit geolocation of Internet addresses.[318]

Anonymity doesn't require physical relocation, but it does have social costs. True anonymity precludes building reputation or establishing repeat play (which may be important aspects of p2p networks), because if you are truly anonymous you cannot prove you are the same person who logged on yesterday.[319] It is difficult (though as Michael Froomkin has shown not impossible)[320] to maintain a consistent pseudonymous persona that can build reputation and be found repeatedly online by others, but that cannot be traced to an individual who might be held legally accountable. Such untraceable pseudonymity[321] requires both the faithful use of unbreakable encryption and the presence of intermediaries willing to provide anonymous remailing services to parties unknown to them. Unbreakable (generally public-key) encryption is currently available, but it is not widely used, though less powerful forms of

316. Friedman, *Strong Privacy*, *supra* note 314; A. Michael Froomkin, *Anonymity and Its Enmities*, J. ONLINE L. art. 4 (1995); Johnson & Post, *supra* note 311.

317. These burdens are heightened because, as noted below, there are only a few, mostly small, countries that might be safe havens from copyright enforcement.

318. Among the companies providing geolocation services are CyberSource, http://www.cybersource.com (last visited Apr. 29, 2004); Digital Envoy, http://www.digitalenvoy.net (last visited Apr. 29, 2004); and Quova, http://www.quova.com (last visited Apr. 29, 2004). *But see* ITAA, ECOMMERCE TAXATION AND THE LIMITS OF GEOLOCATION RULES (2001), *available at* http://www.itaa.org/taxfinance/docs/geolocation paper.pdf (last visited Apr. 4, 2004) (discussing the shortcomings of these technologies).

319. *See* Froomkin, *supra* note 316, at 72.

320. *Id*. at 71-72.

321. *Id*. at 71.

encryption such as Secure Sockets Layer are a common feature of ecommerce.[322] Such remailing services do exist, but they are hardly common.[323] In part this is because the only way such an entity could get paid is through anonymous, untraceable digital cash, and digital cash never took off.[324] It is certainly true that high-volume uploaders today aren't anonymous. We think it unlikely that the infrastructure exists today to support a widespread shift to anonymity in response to a new copyright enforcement initiative.[325] Further, while there are some efforts to develop anonymous file-sharing in response to industry lawsuits, those efforts may be self-limiting. By eliminating any trusted intermediary, most truly anonymous approaches to file-sharing will emphasize sharing among small groups of friends, rather than open sharing with strangers.[326] This may produce true anonymity, but at the cost of creating mini-networks that do not scale. From the perspective of copyright enforcers, this would be a major victory.

Networks designed to protect users' anonymity may also be more vulnerable to interference by copyright owners who sabotage the network by offering fake files[327] or who create their own apparently anonymous proxy servers "to serve as decoys and gather information on users."[328] In addition, p2p software designed to protect anonymity has, to date, been slower and less efficient, and less user-friendly, than ordinary p2p networks.[329]

Third, even if a significant number of high-volume uploaders seek to escape legal accountability by moving offshore or distributing files anonymously, it is not at all clear that those strategies of evasion will prove entirely effective. At the outset, it is worth noting that as of April 2003, 146

322. *See, e.g.*, JRH WEB DESIGN & HOSTING, FREQUENTLY ASKED QUESTIONS (1999) *available at* http://www.jrhwebdesign.com/faq.shtml (last visited Apr. 4, 2004).

323. *See, e.g.*, Winn, *supra* note 263.

324. *See* Mark A. Lemley, *Standardizing Government Standard-Setting Policy for Electronic Commerce*, 14 BERKELEY TECH. L.J. 745 (1999); Winn, *supra* note 263.

325. Even such a shift would protect only new entrants into the high-volume uploader business; those who have already been identified as uploaders could be sued or prosecuted for their past offenses (though such enforcement would need to be in the courts if our proposed administrative system operates only prospectively, as suggested *supra* note 298).

326. *See, e.g.*, Hansell, *supra* note 195, at C1, C3 (describing efforts to develop such systems and their limitations). As Tim Wu notes, "trust systems are difficult, if not impossible, to create without some centralized system of verification." Wu, *supra* note 118, at 722.

327. *See* Wu, *supra* note 118, at 722; Doug Lichtman, *Anonymity: A Double-Edged Sword for Pirates Online,* CHI. TRIB., Apr. 13, 2000, *available at* http://www.law.uchicago.edu/news/lichtman-pirates.html (last visited Apr. 4, 2004).

328. Hansell, *supra* note 195.

329. *See, e.g.*, John Borland, *Covering Tracks: New Privacy Hope for P2P*, CNET NEWS.COM, Feb. 24, 2004, *available at* http://news.com.com/2100-1027-5164413.html (last visited Apr. 4, 2004) ("At the very least, adding anonymity to peer-to-peer systems involves a trade-off in efficiency, creating performance headaches that bring a network to its knees."); Hansell, *supra* note 195 (noting that first major anonymous p2p system, Freenet, "is slow and hard to use, and it requires knowing a specific file name").

countries have adhered to the WTO's Agreement on Trade Related Aspects of Intellectual Property (the TRIPs Agreement) and 154 have adhered to the Berne Convention as of March 2004. Fleeing to these countries (which include nearly every major nation in the world) will not ensure escape from legal consequences; the law in those countries should permit domestic enforcement against high-volume uploaders, though actual enforcement can be spotty.[330] Proposed international conventions would also permit the enforcement of national copyright judgments in any member country.[331] And going abroad may not even be necessary to pursue foreign infringers—the recent history of digital copyright enforcement suggests that the reach of U.S. law is long indeed.[332] U.S.-based content industries have managed to obtain civil jurisdiction over companies based in Spain, Nevis, the Netherlands, Australia, and Vanuatu[333] and pushed the U.S. government to bring criminal prosecutions

330. Enforcement efforts against file-sharing individuals have been initiated or successful in Japan, *see supra* note 213; Taiwan, *see* Bill Heaney, *Music Industry Rejoices over File-Sharing Victory*, TAIPEI TIMES, Nov. 27, 2003, at 10, *available at* http://www.taipeitimes.com/News/biz/archives/2003/11/27/2003077458 (last visited Apr. 4, 2004); Canada, *see* Angela Pacienza, *Music Uploading Case Back in Court Friday; New Ways to Hide from Law*, CANADA.COM NEWS, Mar. 22, 2004 (discussing Canadian recording industry suit seeking identities of p2p users from ISPs in preparation for suits against users); and Australia, see *Students Get Suspended Terms in Music Piracy Case*, SMH.COM.AU, Nov. 18, 2003, *available at* http://www.smh.com.au/articles/2003/11/18/1069027100496.html (last visited Apr. 4, 2004). Suits against individual uploaders in Europe are reportedly on the horizon, though predictions about the likely success of those suits and likely reaction to them, have varied. *See, e.g.*, Kevin J. Delaney & Charles Goldsmith, *Music Industry Targets Piracy by Europeans*, WALL ST. J. ONLINE, Jan. 20, 2004, *at* http://www.wsj.com (last visited Apr. 4, 2004); Mark Landler, *For Music Industry, U.S. Is Only the Tip of a Piracy Iceberg*, N.Y. TIMES, Sept. 26, 2003, at A1, C4.

331. *See* Rochelle Cooper Dreyfuss, *An Alert to the Intellectual Property Bar: The Hague Judgments Convention*, 2001 U. ILL. L. REV. 421; Hague Conference on Private International Law, Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters (Oct. 30, 1999) (unpublished manuscript, on file with authors), *available at* http://www.hcch.net/e/conventions/draft36e.html (last visited Apr. 4, 2004); *see also* Graeme B. Dinwoodie, *The Architecture of the International Intellectual Property System,* 77 CHI.-KENT L. REV. 993 (2002) (describing the increasing role national courts will play in deciding international intellectual property disputes); Rochelle C. Dreyfuss & Jane C. Ginsburg, *Draft Convention on Jurisdiction and Recognition of Judgments in Intellectual Property Matters*, 77 CHI.-KENT L. REV. 1065 (2002) (criticizing the Hague convention and proposing an alternative). Whether a judgment from an administrative system such as the one we propose would be enforceable under such a convention would depend on the specific language ultimately adopted.

332. Among the myriad discussions of international jurisdiction on the Internet, see Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311 (2002); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001).

333. Arista Records, Inc. v. Sakfield Holding Co. S.L., No. Civ. 03-1474 (RCL), 2004 U.S. Dist. LEXIS 7023 (D.D.C. Apr. 22, 2004) (finding jurisdiction over Spanish music site based on transactions with residents of District of Columbia); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 243 F. Supp. 2d 1073 (C.D. Cal. 2003) (holding that Kazaa was subject to the jurisdiction of U.S. courts); *see also* Graduate Mgmt. Admission Council

of a Russian company and software engineer.[334] Courts in France and Australia have also subjected U.S. citizens to jurisdiction for complaints involving content available on the Internet.[335] And even if an uploader resides in a jurisdiction that will not enforce copyright, that uploader needs to worry about criminal as well as civil liability every time she travels to one of the many countries that do enforce copyright.[336] Dmitry Sklyarov found this out to his detriment when he came to the United States to present a paper and was arrested for violating the DMCA.[337]

Nor is anonymity of the kind commonly used necessarily a barrier to prosecution. The most famous "anonymous remailer" of the 1990s, anon.penet.fi, disclosed the name of one of its users and folded its service in

v. Raju, 241 F. Supp. 2d 589 (E.D. Va. 2003) (finding jurisdiction in Virginia over accused infringer in India who operated a website there designed to reach U.S. customers, even though only two Virginia customers had obtained infringing products from the website, because accused's contact with the U.S. as a whole sufficed to make jurisdiction consistent with due process).

334. United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002); *see also* Press Release, Elec. Frontier Found., Norwegian Teenager Jon Johansen Acquitted in DVD Case: Legal to Descramble his DVDs on Linux Computer in Norway (Jan. 7, 2003), *available at* http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20030107_eff_pr.html (last visited Apr. 4, 2004) (describing the prosecution and acquittal of Jon Johansen in Norway for writing DeCSS).

335. *See, e.g.*, Tribunal de Grande Instance [T.G.I.] [trial court of original jurisdiction] Paris, Nov. 20, 2000, Ordonnance de Référé, UEJF et Licra v. Yahoo!, Inc., *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm (last visited Apr. 4, 2004); T.G.I. Paris, May 22, 2000, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm (last visited Apr. 4, 2004) (both holding Yahoo! and its employees subject to criminal jurisdiction in France for conduct on their website); Dow Jones & Co. Inc. v. Gutnick (2003) 194 A.L.R. 433 (Australian High Court decision that Dow Jones & Co. was subject to Australian jurisdiction in a defamation suit based on Internet publications in the United States). Neither case involves copyright infringement, and U.S. courts will not necessarily enforce those judgments. *See* Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

336. *See, e.g.*, Jonathan A. Franklin & Roberta J. Morris, *International Jurisdiction and Enforcement of Judgments in the Era of Global Networks: Irrelevance of, Goals for, and Comments on the Current Proposals*, 77 CHI.-KENT L. REV. 1213, 1230 (2002) ("If a website is accessible to hundreds of jurisdictions, it could become subject to hundreds of criminal laws."). Indeed, even staying at home may not be enough to avoid criminal liability; the United States recently indicted an Australian citizen for copyright infringement and has sought (so far unsuccessfully) to have him extradited to the United States. Jennifer Lee, *U.S. Charges Australian with Copyright Infringement*, N.Y. TIMES, Mar. 13, 2003, at C2; John Borland, *Attempt To Extradite Online 'Pirate' Blocked,* CNET NEWS.COM, Mar. 15, 2004, *at* http://news.com.com/2100-1027-5179588.html (last visited Apr. 29, 2004); *see also Thailand to Send Ukrainian Hacker to U.S.*, CNETASIA, Dec. 19, 2003, *available at* http://asia.cnet.com/newstech/security/0,39001150,39161888,00.htm (last visited Apr. 4, 2004). Extradition of individuals engaged in large-scale uploading to p2p networks does not seem particularly likely, however.

337. The charges were ultimately dropped but not until months later and in return for his testimony in the criminal prosecution of his employer. *See* United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002). The employer in turn was acquitted at trial.

response to a search warrant issued by the Finnish government.[338] "Anonymous" posts in chat rooms or on ISP bulletin boards also have proved thin protection, as companies file John Doe lawsuits and then compel the ISP to disclose the identity of the "anonymous" poster. Truly untraceable anonymity will permit uploaders to avoid prosecution, but what often passes for anonymity on the Internet today will not.

None of this is to suggest that Internet enforcement will be perfect. Indeed, it is reasonable to assume that some high-volume uploaders will live in countries where copyright enforcement is impractical and that some uploaders will be able to maintain true anonymity. Further, we must consider not just how file-sharers behave now but how they might respond to more aggressive enforcement.[339] If file-sharers really care about uploading rather than just downloading digital music—something about which we are skeptical—they may make a significant investment in anonymity to preserve their ability to do so.[340] For example, Freenet and Earthstation5 both offer anonymous file sharing,[341] though they are much less popular than Kazaa, and a new product called AnonX permits masking of the IP addresses of p2p file sharers.[342] As noted above, though, users seeking such anonymity may face tradeoffs as to usability, efficiency, and reliability.

But as we noted above, perfect enforcement isn't the goal. Antipiracy enforcement has never been perfect. The real question is whether the characteristics of the Internet prevent enforcement in the p2p context from being "good enough" to allow copyright owners to reap a reasonable profit by exploiting their works. We think the answer is "no"—or at least likely enough to be "no" as to make enforcement against direct infringers worth a try, particularly if the alternative is shutting down p2p networks entirely.

Indeed, imperfect enforcement may have affirmative social benefits. First, digital dissemination by consumers of some classes of works over p2p networks may well turn out to be legal. The obvious example concerns sharing

338. For a report of the incident from the owner of the remailer, see Posting of Kurt Fuchs, Kurt.Fuchs@aut.alcatel.at, to an0@anon.penet.Fi (Mar. 23, 1995) *available at* http://www.dbai.tuwien.ac.at/marchives/ece/0135.html (last visited Apr. 4, 2004).

339. *See* Wu, *supra* note 118, at 3.

340. Interestingly, however, true anonymity may undermine the culture of sharing that Strahilevitz identifies as being at the heart of the success of the p2p system. Strahilevitz, *supra* note 203.

341. *See* John Alan Farmer, *The Specter of Crypto-Anarchy: Regulationg Anonymity-Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 726 (2003) (pointing to Freenet as a means for circumventing legal regulation).

342. Associated Press, *Angry with RIAA Tactics, Programmer Creates Mask for File Sharers*, Feb. 11, 2004, *available at* http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7927993.htm (last visited Apr. 4, 2004). Anon-X charges $5.95 per month and apparently maintains records of its customers' IP addresses, though the program's creator reportedly has taken steps to try to put that information out of the legal reach of copyright owners. *Id*. The creator also reportedly intends to "cut off service for egregious downloaders of copyrighted material." *Id*.

authorized by the copyright owners.[343] Another example involves out-of-print works not made available for authorized dissemination. Because of the extraordinary length of the copyright term, a large number of such works languish in the clutches of apathetic copyright owners.[344] A court may well conclude that some reproduction and transmission of such works is fair use because it causes no economic harm to the copyright owner, who after all is not exploiting the work, and permits dissemination of a work that would otherwise be lost.[345] p2p networks may serve a useful function in disseminating this copyrighted content.[346] A second argument is broader. A number of scholars have argued that as digital dissemination takes hold, more and more content owners will voluntarily disseminate their works for free online[347] or alternatively that digital dissemination companies will come up with ways to compensate authors at least as well as the rather inefficient existing system of middlemen.[348] If this is true, a service that starts out as a haven for large-scale infringement could over time turn into a legitimate means of disseminating content as artists voluntarily embrace it. This may or may not happen.[349] But shutting down p2p networks outright will terminate this experiment before it has a real chance to unfold. By contrast, targeting direct infringers may actually facilitate the shift from illegal to legal uses precisely *because* it does not shut the network down all at once; rather it removes illegal content one bit at a time. The resulting demand for legally distributed content (from independent bands and filmmakers, of out-of-print works, and the like) may or may not be enough

343. An increasing number of content owners are making their files available on p2p networks. *See* Chris Nelson, *Upstart Labels See File Sharing As Ally, Not Foe*, N.Y. TIMES, Sept. 22, 2003, at C1; *supra* text accompanying notes 143-46.

344. *See, e.g.*, Deirdre K. Mulligan & Jason M. Schultz, *Neglecting the National Memory: How Copyright Term Extensions Compromise the Development of Digital Archives*, 4 J. APP. PRAC. & PROCESS 451, 472 (2002) ("According to the Internet Movie Database, 36,386 motion picture titles were released from 1927 to 1946. Of those, only 2480 are currently available on videotape; only 871 are available on DVD; only 114 are available on Pay-Per-View/TV; and only thirteen are available in theaters."). By contrast, just one archive—Prelinger—has put 28,800 public domain films online.

345. The argument for fair use is even stronger if the work itself is deteriorating, as is the case with many movies still protected by copyright but not exploited by their owners.

346. Matt Jackson makes a related argument that suing facilitators will interfere with legitimate speech interests of users and that the law would do better to require copyright owners to sue users. *See* Jackson, *supra* note 156, at 63.

347. *See, e.g.*, Amy K. Jensen, *Copy Protection of CDs: The Recording Industry's Latest Attempt at Preventing the Unauthorized Digital Distribution of Music*, 21 J. MARSHALL J. COMP. & INFO. L. 243, 265 (2003); L. Kevin Levine, *Digital Music Distribution Via the Internet: Is It a 'Platinum' Idea or a 'One Hit Wonder'?*, 104 W. VA. L. REV. 209, 224 n.104 (2001).

348. *See* Ku, *supra* note 172, at 263 (arguing that the current system provides little incentive to musicians and that they could do better in the digital environment without copyright).

349. For skepticism from a content provider, see James Gleick, *I'll Take the Money, Thanks*, N.Y. TIMES, Aug. 4, 1996, § 6 (Magazine), at 16.

to support a robust online dissemination network. But we will at least get a chance to find out.

CONCLUSION

Copyright owners sue facilitators online because it is cheaper and easier for them than suing direct infringers. Cheaper and easier does not necessarily mean more efficient, however. The shift toward suing facilitators who are further and further removed from the act of direct infringement imposes substantial social costs on both legitimate users and on innovation, costs that the copyright owners do not have to bear. A better approach is to change the economics of targeting direct infringers. One way to do this is to enforce civil and criminal copyright statutes against high-volume uploaders. Such enforcement would likely have a substantial deterrent effect on uploading illegal files, though it may have undesirable social or moral consequences. Alternatively, we could reduce the cost of targeting direct infringers by imposing a levy on the technology they use or by subjecting them to a relatively low-cost, quick administrative enforcement system. As to the latter option, recent experience with such a system in the Internet domain name context suggests both that it is workable and that careful attention must be paid to process concerns in its design.

None of these approaches is perfect. Further, none will stop the demand for digital content, and so none will work unless accompanied by a serious, sustained effort by copyright owners to offer digital content online in legal form.[350] But the approaches we discuss are better than the alternatives: quashing innovation by expanding the scope of indirect liability or doing nothing in the face of rampant digital copyright infringement. The Internet has changed the economics of copyright enforcement irretrievably. Policymakers must set legal rules with these economic developments in mind.

350. That effort in turn may require redesign of other aspects of the copyright system, which may have granted too many different rights to too many different parties to permit efficient licensing of music online. *See* Loren, *supra* note 289; Reese, *supra* note 116. But that is a subject beyond the scope of this Article.