MAKING TECHNOLOGY VISIBLE: LIABILITY OF INTERNET SERVICE PROVIDERS FOR PEER-TO-PEER TRAFFIC

Niva Elkin-Koren *

* Professor of Law, University of Haifa School of Law. I am grateful to Stefan Bechtold, Michael Birnhack, Abraham Bell, Assaf Hamdani, Jacob Nussim, and Gideon Parchomovsky for their comments. I also thank Rachel Aridor for her thorough research and insightful comments, and Benny Hadari for providing research assistance. The editorial staff of the *NYU Journal of Legislation and Public Policy* contributed greatly to the final shape of this article.

I.
INTRODUCTION

The interrelationship between law and technology often focuses on one single aspect: emerging technologies are challenging the existing legal regime, creating a need for legal reform. The interrelationship between law and technology is, however, dialectic. The law does not merely respond to new technologies. It also shapes them and may affect their design. A dialectical approach to law and technology would inquire whether some rules may affect the emergence of new technologies and how they are likely to shape design and architecture.

The issue of third party liability for infringing materials distributed by users provides a fascinating example of this dynamic interaction. The liability of Internet Service Providers (ISPs) for injurious content posted by their subscribers was highly controversial during the early days of the Internet.[1] The term ISP refers to a wide range of online intermediaries that facilitate access to the online environment.[2] ISPs were high on the list of copyright owners as potential defendants in online infringement lawsuits. Copyright owners were looking for gatekeepers that would help them keep the Internet clear of infringing materials. ISPs were obvious targets with deep pockets, located

1. *See* JESSICA LITMAN, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET (2001). For further analysis of ISP liability for injurious content posted by subscribers see *infra* Part III.A.

2. During the early 1990s it was common to distinguish between Access Providers and Internet Service Providers. Access Providers simply enable access by offering transmission, routing, and connectivity to digital online networks through dial-up connection, cable, or high-speed DSL circuit. Internet Service Providers offer a wide spectrum of information processing services such as search services, chats, forums, hosting, storage, payments, marketing, and design services. This distinction has been blurred in recent years due to the increasing convergence of communication and content in digital markets. Since the purpose of this Article is to examine the interconnection between various players in the information environment, the term "ISP" is used to describe all sorts of online intermediaries that facilitate Internet communication, such as traditional telephone companies, mobile phone companies, backbone providers, and cable companies.

within national borders and controlling gateways to the online environment. Targeting ISPs for copyright infringements was not just cost effective, but also promised to engage them more actively in the campaign against piracy.

The issue of ISP liability has faded from the public agenda in recent years. This was partly due to the safe harbor regime established by the Digital Millennium Copyright Act (DMCA)[3] in the late 1990's. The safe harbor regime provided ISPs with a shield that mostly kept them out of copyright wars. Under this regime, ISPs were exempted from some liability at a cost. That cost was the implementation of copyright enforcement duties, such as terminating repeat infringers and removing allegedly infringing materials.

Emerging peer-to-peer networks destabilized the equilibrium achieved under the DMCA between copyright owners and ISPs. Peer-to-peer networks facilitate direct exchange of files among individual users. While infringing materials distributed on the web involve identifiable websites, the distribution of infringing materials on peer-to-peer networks is difficult to control. Data is replicated by multiple peers and can be located by peers without relying on a central index server. The distributed architecture of peer-to-peer networks makes it difficult to identify the source of infringing materials and to locate the infringers. These challenges to copyright enforcement policies revived interest in engaging ISPs in copyright enforcement efforts.

Copyright owners are trying to draw ISPs back into the legal scene, seeking to engage them in actively addressing peer-to-peer piracy. The Recording Industry Association of America (RIAA), for instance, requested subpoenas under the DMCA,[4] to identify subscribers who were allegedly infringing copyrights via peer-to-peer systems. In two recent decisions, *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc*.[5] and *In re Charter Communications, Inc*.,[6] the RIAA's requests for subpoenas were denied. The courts held that the DMCA safe harbor regime was tailored to address a different technological infrastructure and did not apply to peer-to-peer technology.[7] Both concluded that peer-to-peer architecture might

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

4. Section 512(h) of the Copyright Act of 1976 permits copyright owners to serve subpoenas on ISPs to obtain personal information of allegedly infringing subscribers. 17 U.S.C. § 512(h) (2000).

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

6. *In re* Charter Commc'ns, Inc., 393 F.3d 771 (8th Cir. 2005).

7. *See Verizon*, 351 F.3d at 1237–38; *Charter*, 393 F.3d at 777.

require a new balance, and that it was the province of Congress to change the law in order to accommodate the relevant competing interests.[8] Both cases were celebrated as great victories for the Internet industry. Nevertheless, the reasoning of the decisions may raise concerns regarding the future of ISP liability, since they suggest that the DMCA can no longer address peer-to-peer challenges. If the safe harbor regime no longer applies to ISPs which carry peer-to-peer traffic, ISPs may be facing extended liability for infringing copies on peer-to-peer networks.

Holding ISPs liable may affect network architecture and involve long-term ramifications that go far beyond the immediate interests of copyright owners and ISPs. ISP liability for peer-to-peer infringing traffic may induce central management of peer-to-peer traffic to minimize the legal exposure of ISPs. Central management of peer-to-peer networks would turn them into a giant broadcast system provided by ISPs, and centrally managed through their gates. Here, ISPs and copyright holders, or for that matter, any law enforcement agencies, may share similar interests. Peer-to-peer technology, which was first introduced by non-market players, confronted ISPs with a dilemma: it boosted their business, increasing the demand for broadband and upgraded services, but at the same time created a growing burden of limitless bandwidth consumption. No single ISP can eliminate peer-to-peer without the risk of losing its market share. Yet peer-to-peer applications consume ISP bandwidths, and in fact shift the cost of communication from the server level to the ISP network. Peer-to-peer networks allow each user to act as a server. Thus, there is no need to invest in strong servers that can meet the demands of many users for the same file. Consequently, however, ISPs must support high bandwidth capacity for the uploads and downloads of every user.

Liability of ISPs for peer-to-peer traffic may come at the cost of losing out on the economic and political benefits produced by peer-to-peer networks. This Article explores the ramifications of liability rules for design choices, focusing on the implications of ISP liability for network architecture. Part II introduces peer-to-peer technology and discusses its economic and political significance. The main advantage of peer-to-peer networks is their decentralized distribution structure. Decentralization, it is argued, may facilitate economic efficiency and enhance personal freedom. Part III provides an overview of legal rules pertaining to ISP liability. Part III.A addresses ISP liability for infringing materials posted on the web. After describing the

8. *See Verizon*, 351 F.3d at 1238–39; *see also Charter*, 393 F.3d at 777.

rise of secondary liability and the safe harbor regime, I move on to discuss the policy considerations that led to the regime's implementation. Lessons drawn from the implementation of the DMCA safe harbor regime demonstrate some of the risks related to enforcement by private intermediaries. Part III.B addresses some recent initiatives to engage ISPs in copyright enforcement efforts. It further analyzes the potential liability of ISPs for peer-to-peer piracy under the current law, examining the applicability of the DMCA safe harbor provisions to ISPs in their capacity as peer-to-peer facilitators. It concludes that in the absence of the DMCA immunities, ISPs could be held liable for infringing peer-to-peer traffic.

Part IV presents a normative framework for analyzing liability issues related to technology. I discuss the underlying assumptions of current liability rules and argue that the implications of liability for design should be taken into consideration when determining the scope of liability. Part V explores ISP business models and examines the design implications of holding ISPs liable for infringing peer-to-peer traffic. Liability for infringing peer-to-peer traffic may re-shape peer-to-peer architecture in a way that would diminish its inherent socio-economic and political advantages.

II.
Technology and Social Change: The Virtues of Peer-to-Peer Networks

Peer-to-peer networks are often considered a major threat to the interests of the content industry, because they are primarily used for sharing copyrighted materials without authorization. With millions of users around the world, peer-to-peer networks allow individual users to instantly obtain a perfect copy of almost any work they desire, free of charge. The massive distribution of infringing materials is claimed to be causing heavy losses to the recording and film industries.

The availability of free copies is definitely the driving force behind the colossal success of peer-to-peer networks. Yet, their economic and political significance lie in their decentralized architecture. Thus, when viewed independently of copyright interests, peer-to-peer networks appear to take advantage of decentralized design for promoting efficiency and greater freedom.

Peer-to-peer networks allow the sharing of computer resources and services by direct transmission of files between the computers connected to it. This architecture distributes information in a decentralized way, allowing direct exchange of files among users of compatible applications without any central management and control.

Peer-to-peer networks connect individual computers instantly, often using connecting nodes via ad hoc connections. Digital files, which are stored on any user's personal computer, could be made available to other users for downloading over the Internet. While first generation peer-to-peer networks were limited to audio files, current systems allow sharing of any type of content file ranging from video to music, text, and software, including real-time data such as telephone traffic.[9]

The first generation of peer-to-peer systems, introduced by Napster, incorporated a centralized index that listed all the files that were made available for download by Napster's users. The second generation of peer-to-peer networks, based on Gnutella technology, no longer employed any central index. A user searching for a particular file sent a search request which was passed among the community of users of the same peer-to-peer application, until the requested file was located. The searching user was then able to download the file directly from the machine on which the requested file was stored.[10] Some variations of this architecture rely on *supernodes*, namely, computers of individual users which are designated ad hoc to host subindexes for the purpose of speeding up the search. Other applications offer a mixture of peer-to-peer and web distribution. For instance, in BitTorrent, ancillary files ("torrents") which govern the simultaneous downloading of any particular file from multiple hosts, are posted on ordinary websites.[11]

The main advantage offered by peer-to-peer networks is the decentralized distribution structure. Decentralization is a fundamental principle that governs Internet design. It goes back to the origins of the Internet as conceived by U.S. Defense Department military strategists, whose aim was to build a computer network that would be resilient to attacks.[12] Decentralization remained the governing principle of

---

9. *See* Wikipedia, Peer-to-peer, http://en.wikipedia.org/wiki/Peer-to-peer (last visited Nov. 29, 2005).

10. Applications using this architecture include Kazaa as well as Grokster. Both were the subject of litigation. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005); Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd. (2005) FCA 1242, *available at* http://www.austlii.edu.au/au/cases/cth/federal_ct/2005/1242.html (Kazaa). For further discussion of *Grokster*, see *infra* Part III.B.4.

11. BitTorrent is a protocol and peer-to-peer file sharing system designed by Bram Cohen. For further discussion see *infra* Part IV.C.

12. The theory was that a distributed network would be more resilient than a centralized network to repeated attacks. A packet switching technology was designed to serve this strategic goal, thus reducing dependency on central control systems and securing continuous service even in case of major damage resulting from nuclear or other strategic attacks. *See* Christopher C. Miller, *For Your Eyes Only? The Real*

Internet transmission. The distributed nature of Internet communication was facilitated by the use of open protocols, primarily the TCP/IP protocol, which enabled interconnection among independent and incompatible computers and information systems.

The introduction of the World Wide Web in 1990 advanced a client-server architecture, in which users (clients) request services from powerful servers that store information and manage network traffic. Any computer can be both a client and a server depending on the software configuration. Nevertheless, servers usually required more powerful computers dedicated to managing files and network traffic. Thus, Internet traffic, however distributed, was still concentrated around large servers providing access to content.

Peer-to-peer architecture took decentralization a step further by enabling all users connected to a peer-to-peer network to share resources. Peer-to-peer applications and client/server applications use the network in different ways. In client-server architecture, users are requesting services from servers with a fixed capacity. Consequently, adding more clients may slow down data transfer for all users and in extreme situations may lead to a denial of service.[13] In peer-to-peer architecture users are not only consuming services but also providing resources, such as bandwidth, storage space, and computing power. Consequently, as "demand on the system increases, the total capacity of the system also increases."[14]

Other important advantages of peer-to-peer networks are stability and intensity. The distributed nature of peer-to-peer networks may enhance the system robustness in case of failures. Distributed systems may reduce the risk that a failure in one server will disable the network entirely.

The superiority of peer-to-peer as an efficient distribution method is self evident when compared with the distribution of physical copies of copyrighted works (such as CDs).[15] It involves no cost of storing, packing and distributing copies to vendors. Files are only downloaded by those interested and therefore there is no need to manage any stock

---

Consequences of Unencrypted E-mail in Attorney-Client Communication, 80 B.U. L. REV. 613, 615 (2000).

13. The familiar error messages posted for such circumstances are: "502 Service Temporarily Overloaded"; "503 Service Unavailable."

14. *See* Wikipedia, Peer-to-peer, http://en.wikipedia.org/wiki/Peer-to-peer (last visited Nov. 29, 2005).

15. *See, e.g.*, Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT. L.J. 1, 30–31 (2004) [hereinafter *Sharing and Stealing*] (arguing that because peer-to-peer is based on sharing, which is more efficient method of distribution than selling copies, it should not be prohibited by law).

and there is no waste. It is less clear, however, whether distributing music files through peer-to-peer systems is more efficient than distribution via an online music store, such as Apple's iTunes.

The view of peer-to-peer networks as being more efficient emphasizes the sharing of computing power and bandwidth by all the participants of the network. Distribution via peer-to-peer networks is changing the structure of distribution and the allocation of these costs. The advantage of systems like BitTorrent, for instance, is that they allow any user who wishes to distribute large video files to lower the cost of distribution in terms of bandwidth. Peer-to-peer networks eliminate the need for costly server space since they rely on the storing capabilities of those who are connected to the network at any given time.[16] A user who wishes to distribute a file on BitTorrent no longer needs a powerful server that can respond to users' requests in a timely manner. Instead, the network takes advantage of the distributed resources of all users who participate in uploading and downloading. This causes an increase in bandwidth consumption at the network level, shifting the cost of distribution from servers to access providers.[17]

As further demonstrated below, however, the design of many versions of peer-to-peer systems was dictated by legal considerations and the attempt to escape liability for copyright infringement. Consequently, some applications turned out to be less efficient, offering slower downloading speed and inferior search capabilities.[18] For instance, searching a central index of files available for downloading at any given time, as in Napster, could be faster than passing a search request among all users running Gnutella-compatible software (as in Morpheus).[19] Decentralized searching, however, may offer a legal advantage by preventing the accumulation of information regarding infringing activities and hence avoiding potential liability.

16. The potential advantages of peer-to-peer networks for efficiency were also acknowledged by the Court in *Grokster*. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2770 (2005).

17. *See infra* Part V.B.

18. CHARLOTTE WAELDE & LILIAN EDWARDS, WIPO SEMINAR ON COPYRIGHT AND INTERNET INTERMEDIARIES: ONLINE INTERMEDIARIES AND LIABILITY FOR COPYRIGHT INFRINGEMENT 9 (Apr. 18, 2005), http://www.wipo.int/meetings/2005/wipo_iis/en/presentations/doc/wipo_iis_05_ledwards_cwaelde.doc.

19. Indeed, to improve the efficiency of the search, some decentralized networks, such as Grokster, were using supernodes, which are designated to route file-sharing requests among a large number of other users. Supernodes are computers selected temporarily based on technical parameters among the logged-in computers at any particular time.

Decentralization is also important for reasons other than economic efficiency. A decentralized architecture, lacking central control mechanisms, could enhance personal freedom. It is therefore arguably superior from a political standpoint. The ability of users to remain anonymous and protect their privacy can be secured more easily when users are not required to register at any particular server, but rather shift between ad hoc networks. Anonymity can be liberating: it opens new venues for asserting various aspects of one's identity. It makes it easier for individuals to express authentic preferences, thereby facilitating a more participatory environment for testing new ideas.[20]

The low cost of making content available on peer-to-peer networks may also enhance diversity. Making works available does not require large financial investment. Users of peer-to-peer networks can make files available for downloading by other users by simply placing files in a designated directory on their personal computers. This allows distribution of works which were marginalized in the entertainment markets since they attracted only a small group of fans.[21]

Moreover, decentralized distribution mechanisms constitute an alternative decision-making process, determining which content will become available. Such decisions are not made by consumers who are voting by their purchases and vendors motivated by profits. Choices regarding the music files or videos shared are made in a non-commercial setting, thus communicating information regarding users' preferences relatively free of market effects. Peer-to-peer distribution may thus reflect the preferences of individual users and non-profit organizations rather than the commercial interests of the content industry.

Users of peer-to-peer networks are not only making informational works available. They also convey their judgment regarding the relative value and relevancy of informational works. Distributed networks incorporate individuals' input in determining what to distribute and when. Peer-to-peer networks thus incorporate the "wisdom of crowds"[22]—the aggregated contribution of diverse independent par-

20. Note, however, that anonymity releases the speaker, the source of information, from any accountability. The source does not have to bear the social cost and economic loss associated with misleading information, *i.e.*, one sort of externality, which could therefore encourage deceitful behavior. For further discussion on the applicability of externalities as an analytical tool for justifying governmental intervention, see NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE 79–107 (2004).

21. *See Sharing and Stealing*, *supra* note 15, at 40.

22. JAMES SUROWIECKI, THE WISDOM OF CROWDS: WHY THE MANY ARE SMARTER THAN THE FEW AND HOW COLLECTIVE WISDOM SHAPES BUSINESS, ECONOMIES, SOCIETIES AND NATIONS (2004).

ticipants, who do not necessarily know each other, in determining what should become available to the public. This dimension of peer-to-peer networks has political significance. By incorporating the preferences of individual users, peer-to-peer networks turn individuals into active participants in the public sphere. Participation in cultural discourse is no longer limited to commercial consumption mediated by content producers. By creating an alternative to centralized distribution methods employed by broadcasters and publishers, peer-to-peer networks destabilize the current business models of the content industry, which are based on mass distribution of copies. Such challenges may push forward the transformation of existing business models, adapting them to the needs of the digital environment.[23]

The decentralized nature of the Internet was considered one of its most significant characteristics, since it promised to make the network an alternative to existing content markets. Decentralized design which allows direct exchange of information among individual users is weakening the role of mass media and equivalent mass distributors. It allows individuals to choose for themselves what content becomes available. Opening up opportunities for creating and distributing informational works on a non-commercial basis may lead to greater individual autonomy.

The economic and political significance of peer-to-peer decentralized architecture is the removal of intermediaries. Maintaining effective outlets for decentralized architectures is particularly important as processes of disintermediation are slowing down. The increasing dependency on search engines for accessing the enormous volume of information available online raises serious concerns regarding freedom in the online environment. Online access is only partly direct and decentralized. There is no useful way to find the "information needle" in the stacks of online "information hay" without the aid of search engines. These new intermediaries may suffer from many of the illnesses associated with the old media.[24]

Since the virtues of peer-to-peer networks lie in their decentralized design, maintaining a decentralized architecture is essential for the purpose of promoting public welfare. As the following discussion

23. Arguably, the introduction of several online music stores, such as Apple's iTunes, in collaboration with recording companies, is the result of pressure created by the colossal success of peer-to-peer networks.

24. *See, e.g.*, Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 185–86. (2001) (describing ability of search engines to shape consumer choices and political opinion).

shows, there is no guarantee that this decentralized design will survive the current legal challenges.

III.
LAW: ISP LIABILITY FOR INFRINGING MATERIALS POSTED BY SUBSCRIBERS

Understanding the interconnection between law and technology requires a closer look at the legal regime and how it evolved in response to new technological challenges. In this Part, I discuss the potential liability of ISPs for infringing peer-to-peer traffic. Subpart A provides background on ISP liability for infringing materials posted on the web, and highlights the legal policies and legislative pressures that shaped the scope of liability in the web environment. Subpart B analyzes the potential liability of ISPs for infringing peer-to-peer traffic. After examining whether ISPs, in their capacity as conduits for peer-to-peer traffic, could benefit from the DMCA safe harbor exemptions, I move on to discuss ISP vulnerability under strict liability and secondary liability standards as developed by the courts in recent cases. The analysis shows that at the same time that the DMCA safe harbor exemptions may no longer shield ISPs from liability, there is also sufficient ground for holding ISPs liable for infringing peer-to-peer traffic under current liability doctrines.

A. Liability for Infringing Materials: Web Distribution

1. The Rise of ISP Secondary Liability

Digital networks are constantly challenging enforcement efforts made by copyright owners. By enabling high quality copying at negligible cost and facilitating mass distribution of copies at the click of a mouse, digital networks elevated piracy to gigantic proportions. The cost of enforcing copyrights increased immensely as mass copying and distribution means became widespread and the volume of infringing materials increased. As many scholars have observed, enforcement of copyright in the digital environment creates an "enforcement failure."[25] The high costs of identifying, gathering evidence on, and

25. *See, e.g.*, Assaf Hamdani, *Who's Liable for Cyberwrongs*, 87 CORNELL L. REV. 901, 910–11 (2002) (arguing that suing only individual infringers will result in underdeterrence); Mark Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1373–79 (2004) (arguing that shift from professional to end-user infringement has made old enforcement techniques obsolete); Alfred Yen, *A Preliminary Economic Analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining*, 26 U. DAYTON L. REV. 247, 252, 260–62 (2001) (considering how copyright external-

suing numerous individual infringers—each engaged in small-scale copying but together causing a large financial loss—have rendered lawsuits against individual infringers inefficient. Individual lawsuits are expensive to prosecute, and the likelihood of recovering damages from individual users is low. An exception could be high profile lawsuits against individual users that aim at increasing deterrence among the public at large. Yet suing one's own customers is not a promising business strategy. Therefore, copyright owners have generally been reluctant to pursue this tactic.

The enforcement crises created by digital networks forced copyright owners to explore alternative paths for enforcing their copyrights.[26] One strategy targeted the manufacturers of devices that were capable of cracking the encryption of copyrighted materials.[27] This strategy resulted in the anti-circumvention portion of the DMCA, which outlawed evasion of technological measures that control access to copyrighted materials and banned the manufacture and distribution of technologies which enable such circumvention.[28] Another strategy involved launching strategic lawsuits against developers and distributors of devices that enable copying and distribution of infringing materials, such as MP3 players[29] or file sharing applications.[30]

A third strategy for copyright enforcement focused on the gateways to information, seeking legal remedies against ISPs. ISPs were high on the list of attractive defendants in the 1990s, during the early days of the Internet. The reasons were obvious: ISPs often had deep pockets, they were easily identified, and their role as *gateways* to the online environment made them attractive as potential *gatekeepers*. ISPs are located within national borders and therefore are likely to be more susceptible to incentives created by liability rules. From the perspective of rights holders, ISPs have an important advantage over other third parties. By providing a gateway to the Internet, ISPs are capable of shaping Internet usage through technical standards and pricing mechanisms.[31] Therefore, targeting ISPs for peer-to-peer in-

---

ities should be allocated, given that individual free-riding Internet users are too difficult to target).

26. *See* Lemley & Reese, *supra* note 25, at 1346–47 (discussing copyright lawsuits brought against third parties).

27. *Id.*

28. *Id.*; *see also* 17 U.S.C. § 1201 (2004).

29. *See, e.g.*, Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999).

30. *See, e.g.*, 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); *see also infra* notes 140–147 and accompanying text.

31. *See infra* Part V.B.

fringing traffic is not simply cost effective. It also promises to engage ISPs as the copyright owners' long arm in implementing their enforcement policies.

For all these reasons ISPs became a favorite target of lawsuits by copyright owners during the mid-1990's. As early as 1993, Playboy Enterprises, Inc., a major publishing and entertainment company, successfully sued a Bulletin Board System (BBS) operator for infringing photographs uploaded and downloaded by users.[32] The court held the BBS operator strictly liable for distributing infringing materials.[33]

Soon after, the strict liability rule was replaced by the courts with the secondary liability standard. ISPs were held liable for infringing materials distributed by their subscribers under the doctrines of contributory infringement and vicarious liability.[34] In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, the court had no doubt that an ISP facilitates online communication and therefore could face liability if it acquired sufficient knowledge regarding the infringing activity.[35] Yet, it was unclear what would count as sufficient knowledge for the purpose of liability and what steps an ISP could undertake to minimize such liability.[36]

2. The DMCA Safe Harbor Regime

The relative success of copyright owners in lawsuits brought against ISPs shook the Internet industry. After the decision in *Netcom*, it was made clear that ISPs would not be able to stay out of copyright enforcement campaigns but would instead remain the target of litigation. The scope of their liability, however, was less clear. Are ISPs required to monitor their systems for copyright infringements? When are they held to knowingly contribute to copyright infringement committed by their users? Would they be forced by law to actively monitor and act against copyright infringers upon notice—and what notice would trigger such a duty? The growing Internet industry, including access providers, search engines, and providers of hosting services and interactive forums, was increasingly at risk of being held liable for the injurious behavior of users. ISPs were faced with two

32. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).
33. *Id.* at 1560–61.
34. The first decision which deviated from the strict liability standard for online services providers was *Sega Enters. Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994).
35. 907 F. Supp. 1361 (N.D. Cal. 1995). For further discussion of *Netcom,* see *infra* notes 112–118 and accompanying text.
36. For further discussion of the standard of knowledge under the contributory liability doctrine, see *infra* Part III.B.4.

expensive options: either implementing costly measures to prevent copyright infringement or risking payment of high damages if they were successfully sued by copyright owners. Faced with judge-made liability for injurious content distributed by users, ISPs sought an explicit immunity under the law. Furthermore, the industry searched for ways to minimize the heavier cost associated with uncertainty regarding the scope of liability. Clear-cut rules that would guide ISPs in managing infringement claims could offer a higher level of certainty.

The DMCA safe harbor regime,[37] adopted by Congress in 1998, reflects a compromise between the demands of copyright owners, on the one hand, and the concerns of the Internet industry, on the other hand.[38] The Internet industry sought immunity but managed only to achieve a regime that enhances "certainty . . . with respect to copyright infringement liability online."[39] For copyright owners the DMCA offered a more effective mechanism for enforcing their rights.

The DMCA was drafted based on the recommendations of the Clinton Administration's Working Group on Intellectual Property Rights ("Working Group") which explored, among other things, the standard of liability for ISPs.[40] The Working Group took a strong position in favor of ISP liability, stressing the ongoing business relationship between ISPs and their subscribers[41] and concluding that ISPs

---

37. 17 U.S.C. § 512 (2000).

38. This view of the legal history of the DMCA is expressed by the Court of Appeals for the Eighth Circuit, which described the DMCA as reflecting:

> "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights." H. Rep. No. 105-551(II) at 23 (1998). . . . It was designed to strike a balance between the interests of ISPs in avoiding liability for infringing use of their services and the interest of copyright owners in protecting their intellectual property and minimizing online piracy.

In re Charter Commc'ns, 393 F.3d 771, 774 (8th Cir. 2005).

39. S. REP. No. 105-190, at 2 (1998). Thus, for the Internet industry, the DMCA was only a partial victory, or even a failure to obtain the absolute immunity achieved two years earlier under section 230 of the Telecommunications Act of 1996. *See* 47 U.S.C. § 230 (2000).

40. WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114–24 (1995).

41. "[O]n-line service providers can certainly investigate and take appropriate action when notified of the existence of infringing material on their systems and thus limit their liability for damages to those for innocent infringement." *Id.* at 116–17. "The risk of infringement liability is a legitimate cost of engaging in a business that causes harm to others, and that risk apparently has not outweighed the benefits for the more than 60,000 bulletin board operators currently in business." *Id.* at 118.

are in the best "position to know the identity and activities of their subscribers and to stop unlawful activities."[42]

The Working Group, however, recognized the need to reduce liability in special circumstances given the diversity of services offered by ISPs, as well as the numerous types and different size of ISPs. Therefore, the Working Group recommended that the final exemptions be determined through negotiations among the government, copyright owners, and industry representatives.[43] The final language adopted by Congress reflected intensive negotiation among the affected players.[44]

Section 512, as added by the DMCA, immunizes ISPs from liability for monetary damages and limits the availability of injunctive relief, with certain limitations and in exchange for help with copyright enforcement. The DMCA immunity covers four strictly defined categories: "transitory digital network communications,"[45] "system caching,"[46] hosting and storage,[47] and "information location tools."[48] To be eligible for any exemption, an ISP must adopt and implement policies that facilitate the enforcement of copyright on its system.

The safe harbor regime introduced several mechanisms for enforcing copyright. First, there is the *notice and take-down* procedure, which requires ISPs to remove infringing materials residing on their systems upon notice from the copyright owner, or to block access to sites where the infringing material resides on an online location outside the United States.[49] The notice and take-down procedure strictly defines the notice requirements and the procedures to be followed upon notice, thus providing ISPs with guidelines regarding the management of infringement claims. A second enforcement mechanism requires ISPs to terminate the accounts of repeat infringers.[50] Third, section 512(h) requires disclosure of the identities of infringers upon subpoena,[51] but ISPs are not required to identify those infringers

42. *Id.* at 117.
43. *Id.* at 123.
44. The DMCA "represents many months of negotiations among interested parties, including software companies, computer manufacturers, and the copyright community. This bill is a compromise; it does not represent any group's 'wish list' for WIPO implementing legislation." 143 CONG. REC. S8582–83 (1997) (statement of Sen. Hatch).
45. 17 U.S.C. § 512(a) (2000).
46. *Id.* § 512(b).
47. *Id.* § 512(c).
48. *Id.* § 512(d).
49. *Id.* § 512(j)(1)(B).
50. *Id.* § 512(i)(1).
51. *Id.* § 512(h).

absent a subpoena.[52] Finally, ISPs are required not to interfere with standard technical measures employed by copyright holders.[53]

3. Policy Considerations

The liability of ISPs for copyright infringements committed by their users reflects an enforcement strategy that engages private gatekeepers in copyright enforcement. When ISPs are at risk of being held liable for infringing materials, they are likely to try to minimize their legal exposure, thereby internalizing the interests of copyright holders in copyright enforcement. Although this strategy certainly serves the interests of copyright owners, the desirability of such a regime would depend on whether enforcement by private parties is likely to coincide with the public interest.

Policies governing injurious content are also necessary in other contexts. The interactive online environment allows all users to make their content available. Some content, however, is harmful. From defamatory statements posted in chat rooms, to consumer fraud and the disclosure of individual users' private information, content distributed online may threaten interests that deserve protection. Consequently, policymakers are seeking practical solutions for governing the increasing volume of injurious content that is distributed online. Enforcement by private gatekeepers becomes attractive as the global nature of the Internet challenges existing law enforcement authorities and legal institutions. The cross-border nature of the Internet weakens the effectiveness of regulation by making it more difficult to identify injurers and bring them to justice.[54] The global nature of the Internet further weakens the legitimacy of regulation that would be justifiable within territorial borders.[55] Since copyright infringements take place across national borders, regulating such activity by one country may affect citizens of another country.[56]

Private enforcement by ISPs, however, has raised serious concerns since the early days of Internet regulation. One concern is that

52. *Id.* § 512(i)(1)(B).
53. *Id.*
54. *See* David R. Johnson & David G. Post, *The New 'Civic Virtue' of the Internet*, 1998 ANN. REV. INST. FOR INFO. STUD. 23.
55. For the perception of the Internet as a global enterprise that lies beyond the reach of laws of any particular government, see *id*. at 26–31. For criticism of that viewpoint, see Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395 (2000).
56. *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367 (1996); Joel Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS 261 (2002).

holding ISPs liable for potentially injurious content would encourage them to screen postings, filter out potentially controversial postings, and restrict access to controversial content. Risk-averse ISPs might seek to minimize their potential liability by limiting access to any risky content, or disabling any interactive services that could increase their potential liability—as long as the utility they derive from allowing the distribution of infringing materials remains low.[57] There is a serious concern that turning decisions regarding access to information to private parties, motivated by profits, would compromise free speech.

The potential chilling effect of enforcement by private gatekeepers on freedom of speech was the dominant rationale underlying the Telecommunications Act of 1996.[58] Enacted in 1996, section 230 exempted interactive computer service providers from strict liability for publishing injurious content that originated with their subscribers.[59] This provision explicitly excludes any liability arising from intellectual property infringement.[60] Pursuant to section 230, no provider of an "interactive computer service"[61] shall be "treated as the publisher or speaker of information provided by another information content provider."[62] This provision has been interpreted by courts as defining a broad exemption from liability, even when an ISP receives a notice regarding injurious content posted on its system.[63] The courts assumed that, unless exempted, ISPs would be forced to decide whether to publish, edit, or withdraw a posting every time a notice is served by

57. *See* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability for Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 363 (1995) [hereinafter *BBS Liability*].

58. Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.).

59. 47 U.S.C. § 230 (2000); *see also* Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (holding that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entering claims that would place a computer service provider in a publisher's role."); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998); Jane Doe v. America Online, Inc., 783 So.2d 1010 (Fla. 2001).

60. 47 U.S.C. § 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.").

61. An "interactive computer service" is defined in section 230(f)(2) as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(2).

62. *Id*. § 230(c)(1).

63. *Zeran*, 129 F.3d at 333; *Blumenthal*, 992 F. Supp. at 52.

a party claiming injury.[64] This costly decision-making process would induce ISPs to remove every controversial message upon notice, and would therefore lead to the chilling effect the law sought to avoid.[65]

Similar considerations would apply in the case of web distribution of infringing content, where the potential gains for ISPs in providing access to infringing materials are very low.[66] ISPs derive very little utility from providing access to any particular infringing work, and would therefore tend to block access to potentially infringing materials. ISPs rarely bear any risk for blocking access or disconnecting a user. Users whose content was removed can protest or threaten to move to another provider. Nevertheless, if their content is controversial, other ISPs are likely to treat the matter similarly. Therefore, in the case of web distribution, when the expected utility of a single infringing posting is relatively low, and the expected liability is high, ISPs would tend to remove access to any controversial content, thereby denying public access to potentially significant materials.

The purpose of section 230, as reflected in its legislative history and interpreted by courts, was to exempt ISPs from potential liability, in order to prevent potential chilling effects on freedom of speech.[67] At the same time, however, section 230 was intended to eliminate disincentives to implementing self-help means against harmful content.[68] Thus, section 230 reflects two conflicting strategies pulling in oppo-

64. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.

Zeran, 129 F.3d at 331.

65. *Id.* at 333.

66. *See BBS Liability*, *supra* note 57; *see also* Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261, 2282 (2003) (arguing that if ISPs were held liable for criminal acts of their subscribers, they would be likely to purge even only slightly suspicious users from network, "because the marginal benefits to the ISP of having an additional subscriber are outweighed by the risk of an adverse judgment against it").

67. *See Zeran*, 129 F.3d at 333; *Blumenthal*, 992 F. Supp. at 52; 141 CONG. REC. S15,153 (daily ed. Oct. 13, 1995) (statement of Sen. Feingold); 141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) (statement of Rep. Lofgren).

68. Section 230 followed the decision in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.,* 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), in which the defendant ISP was held strictly liable for a defamatory statement carried by its network, since it practiced self-help means of screening and filtering family unfriendly content, which in the court's opinion turned it into a publisher. *See Zeran*, 129 F.3d 327, 331; S. REP. NO. 104-230, at 194 (1996) (Conf. Rep.) ("One of the specific purposes of this section is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have

site directions.[69] The immediate result of the immunity provided under section 230 is that ISPs have absolutely no incentives to undertake self-regulatory measures and filter injurious content.

While perfect immunity creates no incentives to intervene in injurious content originated by subscribers, immunity that is contingent upon undertaking enforcement measures may lead to over-enforcement. The DMCA safe harbor regime provides a test case in self-regulation and privatized enforcement. The safe harbor regime established an expedited procedure for blocking access to infringing materials.[70] ISPs were making the first cut for copyright owners, which often turned out to be the final stroke against alleged copyright offenders. The safe harbors were also successful from the ISP perspective, since they removed the immediate threat of copyright lawsuits.[71]

Nevertheless, enforcement of copyright by private parties may disrupt the necessary balance between copyright and free speech. The most significant lesson to be drawn from the implementation of the DMCA safe harbor provisions is that enforcement by gateways reflects their self interest, which is not necessarily the same as the public interest, and which can lead to over- or under-enforcement, as the case may be. Data collected on the implementation of the DMCA notice and take down procedures suggest that ISPs have strong incentives to comply with any notice regarding copyright infringement, and often lack sufficient interest in challenging such notices. Self-regulation then, has led to over-compliance by ISPs and provided strong protection to copyright holders.[72]

The implementation of the safe harbor provisions demonstrates the risks of private enforcement. It shows that assigning ISPs the task of copyright enforcement could lead to over-enforcement, causing a chilling effect on speech. The gap between the incentives of ISPs and

---

treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

69. Judges have begun to question whether it is possible to accomplish the two conflicting goals of section 230. *See, e.g.*, John Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2003).

70. 17 U.S.C. § 512(g)(1) (2000).

71. ISPs could also have ancillary gains from such cooperation, such as business partnership and licensed content.

72. For instance, Chilling Effects Clearinghouse, a joint project of the Electronic Frontier Foundation and several academic institutions, monitors the misuse of intellectual property laws to chill legitimate online activities, maintaining a database of notices served by copyright owners to online service providers under the DMCA. *See* Chilling Effects Clearinghouse, Database of Cease and Desist Notices, http://www.chillingeffects.org/notice.cgi; *see also* Michael Davis-Wilson, Google DMCA Takedowns: A Three-Month View (June 2, 2005), http://www.chillingeffects.org/weather.cgi?WeatherID=498 (analyzing Chilling Effects data).

the public interest could become even more apparent when ISPs are called to address the challenges posed by peer-to-peer networks.

Another consideration to be taken into account when entrusting ISPs with copyright enforcement tasks is cost. ISP liability for copyright infringements committed by their users involves a high cost of monitoring online usage, screening, filtering, and editing online materials, and managing conflicting claims.[73] Such liability rules shift the cost of copyright enforcement to ISPs, which will tend to spread the cost among their subscribers, thus increasing the price of online access.

The most intriguing consequences of private gatekeeper liability, however, are the ramifications for design. While the consequences of liability for design were recognized by courts addressing the potential liability of device manufacturers,[74] they have been overlooked when addressing the liability of other online players.

B. ISP Liability for Infringing Materials on Peer-to-Peer Networks

1. ISPs Are Drawn Back to the Liability Scene

The recent challenges to copyright enforcement posed by peer-to-peer networks revived efforts to engage ISPs in copyright enforcement. As described above, peer-to-peer networks facilitate direct exchange of files among individual users. Subscribers who use peer-to-peer interoperable applications constitute networks in which files can be located and downloaded by users. Typically, the networks themselves do not host or transmit any infringing materials. The applications merely facilitate the process of locating the files that are available for download. The files themselves are made available by any individual user who possesses copies of the requested files; once located, files are downloaded directly by the users who searched for them. In sharp contrast to web distribution, which involves trackable websites, peer-to-peer networks are difficult to control. Data is replicated by multiple peers, and is located by peers without reliance on any central index server. The distributed architecture of peer-to-peer

73. *See BBS Liability*, *supra* note 57, at 404–07.

74. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984). In *Grokster*, the Court acquiescently cited *Sony* and the purpose of the *Sony* rule, which is to "leave[ ] breathing room for innovation and a vigorous commerce." Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2778 (2005). The major point of departure from *Sony*, however, was in stressing that secondary liability is one of a whole set of theories, of which contributory infringement by "design or distribution of a product capable of substantial lawful use" is only a subset. *Id.* at 2777–78.

networks makes it more difficult, and more expensive, to identify the source of infringing materials and to locate infringers. Furthermore, the absence of intermediaries requires rights holders to focus their enforcement efforts against end users.

One could offer several explanations for the revival of ISP liability. One reason for the growing legal attention to ISPs is rights holders' concern that their current legal strategies are ineffective. The focus on the makers of software may not be as robust as copyright holders had hoped. The entertainment industry did win a great victory in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,[75] which was brought directly against distributors of peer-to-peer software. On the other hand, the content industry is concerned that new software companies will nonetheless continue to emerge, facilitating new infringing capabilities.[76] In an effort to cash in on its success in *Grokster*, the content industry is likely to further pressure ISPs to take active steps to control peer-to-peer.[77]

The growing interest in ISPs is a predictable outcome of a particular technological change. The relatively new architecture of peer-to-peer is already challenging the safe harbor regime adopted eight years ago in the DMCA. This legal regime, which provides partial immunity to ISPs in exchange for their assistance in enforcing copyright, seems to be inapplicable to the peer-to-peer environment. Indeed, as further discussed in the next section, the DMCA safe harbor and notice and take-down regimes have recently been held inapplicable to ISPs in their capacity as carriers of peer-to-peer traffic. There is therefore a high degree of uncertainty regarding the duties of ISPs in managing infringing peer-to-peer traffic and the scope of their liability.

Consequently, ISPs are being drawn back to the legal scene in an attempt to address these unresolved crises in the online environment.

---

75. *Grokster*, 125 S. Ct. 2764 (holding Grokster and StreamCast liable for third parties' acts of copyright infringement where companies distributed device with clear intent to promote its infringement capabilities).

76. *See* Pamela Samuelson, *Legally Speaking: Did MGM Really Win the* Grokster *Case?*, COMM. A.C.M., Oct. 2005, at 19, 24 ("[A]s long as technology developers do not actively induce user infringements, they can continue to innovate and rely on the *Sony* safe harbor."). Content providers have also reached agreements with peer-to-peer application providers. BitTorrent, for instance, has set up a process with the Motion Picture Association of America (MPAA) by which DMCA takedown procedures for infringing content will be "expedited." *See* Press Release, MPAA, BitTorrent and MPAA Join Forces: Companies Aim to Protect Film Copyrights (November 22, 2005), *available at* http://www.mpaa.org/MPAAPress/2005/2005_11_22.pdf. Such agreements, however, are likely to have only limited impact, since they do not guarantee compliance by other providers of competing applications.

77. *See infra* Part V.A.

One way this is happening is through suits filed by the content industry against ISPs in an attempt to force them to disclose contact information of allegedly infringing subscribers. If copyright owners were able to serve subpoenas to ISPs every time they believed an individual user was infringing their copyright, ISPs would face a substantial burden.[78]

Several legal initiatives advocate making ISPs liable for peer-to-peer traffic.[79] Copyright holders have also put forward a proposal for ISPs to voluntarily adopt a self-regulatory "code of conduct."[80] Under the proposed code, ISPs would agree to install filtering technology to block services and/or sites that "are substantially dedicated to illegal file sharing or download services."[81] ISPs would be further required to retain data (beyond the data required by law enforcement agencies) to help identify copyright infringements.[82] Data retained by ISPs and users' identities would be handed over to the copyright holders in the event of a complaint (not a court order) against a user for copyright infringement.[83]

The more general context of ISP liability suggests that recent signs of emerging copyright liability for peer-to-peer traffic may be part of a general trend to reconsider the scope of liability for online intermediaries. Several courts have already questioned the broad immunity granted to ISPs under Section 230 of the Telecommunications

78. *See* Brief for United States Internet Industry Association et al. as Amici Curiae in Support of Verizon's Opposition to Motion to Enforce Subpoena at 23–24, *In Re* Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015 & 03-7053), *available at* http://www.eff.org/legal/cases/RIAA_v_Verizon/20020913_ccia_amicus_brief.pdf (arguing that large-scale issuance of subpoenas would substantially burden ISPs).

79. Several scholars have also made more general arguments advocating ISP liability. *See* Douglas Lichtman & Eric A. Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006) (arguing that, because Internet service providers control gateways, they should bear some responsibility for their role in propagation of viruses and malicious code).

80. *See* John Kennedy, CEO and Chairman, IFPI, Music is Driving Growth in Digital Commerce (Mar. 3, 2005), *available at* http://www.ifpi.org/site-content/press/inthemedia14.html; European Digital Rights, EDRI-gram, ISP Self-Regulation Proposal Entertainment Industry (Apr. 6, 2005), http://www.edri.org/edrigram/number3.7/takedown. Similar proposals to establish filtering systems were introduced by IFPI a few years ago. *See* Nils Bortloff, *IFPI's Contribution to the WIPO—Study on Practical Experiences on "Notice and Take-Down Procedures"*, 11 ENT. L. REV. 153, 156–57 (2000).

81. *See* Charles Arthur, *IFPI Drafts 'Code of Conduct' for ISPs*, THE REGISTER (Apr. 12, 2005), http://www.theregister.co.uk/2005/04/12/ifpi_drafts_code_of_conduct/.

82. *Id.*

83. *Id.*

Act.[84] Recent legislation has also called for ISPs to collaborate with law enforcement authorities in detecting and monitoring suspected criminal and terrorist activities.[85]

2. *Safe Harbor Provisions and Peer-to-Peer*

Could ISPs be held liable for peer-to-peer infringing traffic? Peer-to-peer architecture allows Internet users to search for files directly on the computers of other Internet users and to download directly from those computers. Within this architecture, ISPs act as passive conduits for the transmission of information sent or received by their subscribers using peer-to-peer programs. ISPs facilitate peer-to-peer networks in two ways: first, users transmit files through ISP networks; second, files exchanged are temporarily stored on the ISP's facilities. Unless exempted under section 512, these activities could make ISPs liable—either as direct infringers or, more likely, as contributory infringers.[86]

Does the safe harbor regime of section 512 apply to ISPs facilitating infringing peer-to-peer traffic? It is arguable that the DMCA grants ISPs immunity as mere conduits even if they carry peer-to-peer communications.[87] The courts addressing this issue, however, have thus far reached different conclusions.

This question was recently raised in *Recording Industry Association of America v. Verizon Internet Services, Inc*.[88] and *In re Charter*

84. *See, e.g*., Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003) ("There is no reason inherent in the technological features of cyberspace why First Amendment and defamation law should apply differently in cyberspace than in the brick and mortar world. Congress, however, has chosen for policy reasons to immunize from liability for defamatory or obscene speech 'providers and users of interactive computer services' when the . . . material is 'provided' by someone else."); John Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) ("As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1) . . . . Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?").

85. *See generally* Michael Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH 6 (2003).

86. Compare to the law of the European Union. *See* Council Directive 2000/31, 2000 O.J. (L 178) 3 (EC) [hereinafter Electronic Commerce Directive].

87. *See* Neil Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1, 13 (2003) ("[T]he DMCA provides ISPs with complete immunity from liability for monetary damages and sharply limits the availability of injunctive relief where the ISP acts merely as a conduit for user transmissions.").

88. 351 F.3d 1229 (D.C. Cir. 2003).

Communications.[89] In both cases, the RIAA sought to identify and sue individuals who were allegedly committing copyright infringement by sharing music files on peer-to-peer networks. The RIAA was able to obtain the IP addresses of infringing individuals and sought the disclosure of their names and contact information from the ISPs by using subpoenas pursuant to section 512(h).[90] This provision allows copyright holders to obtain the information necessary to bring a suit against individual infringers.[91] While copyright owners can obtain the IP addresses of alleged infringers, only ISPs have access to subscribers' contact information, including street addresses and phone numbers.[92] The question for the courts in both cases was whether section 512(h) applies to an ISP which acts only as a mere conduit for data transferred between two Internet users, as in the case of peer-to-peer file sharing.

The Court of Appeals for the D.C. Circuit in *Verizon* and the Court of Appeals for the Eighth Circuit in *Charter* both found that section 512(h) does not cover ISP conduit functions pursuant to section 512(a), since ISPs cannot remove or disable access to infringing materials when acting merely as a conduit.[93] Both cases were decided based on interpretation of the complex language and structure of the statute; the courts concluded that section 512(h) was tailored to address situations in which an ISP could remove materials or disable access to materials on its network after being notified by the copyright holder of the existence of the infringing materials.[94] Any subpoena request, the courts explained, must include a "copy of a notification

89. 393 F.3d 771 (8th Cir. 2005).

90. *Id*. at 774.

91. A section 512(h)(3) subpoena authorizes and requires the ISP receiving it to disclose to the requesting copyright owner "information sufficient to identify" the alleged infringer. 17 U.S.C. § 512(h)(3) (2000). Copyright holders may also obtain information on copyright infringers in peer-to-peer networks using alternative legal procedures. For instance, owners could file a "John Doe" lawsuit, along with a motion for third party discovery of the identity of the anonymous "John Doe" defendant. Dissenting in *Charter*, Judge Murphy rejected this option as "costly and time consuming." *Charter*, 393 F.3d at 782 (Murphy, J., dissenting).

92. In *Verizon*, plaintiff RIAA had used tracking programs to ascertain the IP addresses and user names of subscribers. Verizon was ordered by subpoena to provide physical addresses, phone numbers, and email addresses of these subscribers. *See Verizon*, 351 F.3d at 1232.

93. *Charter*, 393 F.3d at 776; *Verizon*, 351 F.3d at 1235.

94. *See Charter*, 393 F.3d at 775–76. A notice is therefore required as a precondition for takedown. The court refers to the notice and take down provisions which apply to sections 512(b)-(d), which in turn apply to storage functions and not to transmission functions covered by section 512(a). *See* 17 U.S.C §§ 512(b)(2)(E), (c)(1)(C), (d)(3) (2000). The satisfaction of the notification requirement of section 512(h)(4) is a condition precedent to issuance of a subpoena.

described in subsection [512](c)(3)(A)."[95] When an ISP functions as a mere conduit, the notification requirement cannot be met, since allegedly infringing files reside on hard drives of individual users and therefore no removal of files is possible.[96] Consequently, a notice to an ISP concerning its function as a mere conduit would be ineffective in such instances.

The *Verizon* decision goes further, discussing the general applicability of the DMCA to peer-to-peer architecture. Analyzing the Act's legislative history, the court concluded that the DMCA was adopted to address a different technological infrastructure. Peer-to-peer technology was not merely unknown to Congress, but was inconceivable at the time—peer-to-peer software was "not even a glimmer in anyone's eye when the DMCA was enacted."[97] The legislative history, as interpreted by the court, suggests that the DMCA was crafted to address the needs of the existing technological infrastructure, and not to provide a general basis for addressing new technologies.[98] Whatever the purpose of the DMCA, the court believed that a new architecture might require a new balance, and that it was the province of Congress to change the law in order to address new and unforeseen Internet architecture and accommodate competing interests.[99]

The Eighth Circuit majority decision in *Charter* followed the same reasoning.[100] In a substantial dissent, Judge Murphy expressed the concern that the decision would "block copyright holders from obtaining effective protection against infringement through conduit service providers."[101] The dissent found section 512(h) to be *more* important to copyright owners when the ISP is a conduit, since in such circumstances ISPs cannot directly remove or disable access and therefore must go after direct infringers. Copyright holder action

95. *Charter*, 393 F.3d at 775; *see also Verizon*, 351 F.3d at 1232.

96. *See Verizon*, 351 F.3d at 1235 ("Infringing material obtained or distributed via peer-to-peer file sharing is located in the computer (or in an off-line storage device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the ISP can neither 'remove' nor 'disable access to' the infringing material because the material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers computers."); *see also Charter*, 393 F.3d at 776–77.

97. *Verizon*, 351 F.3d at 1238.

98. *Id.*

99. *Id.*

100. *Charter*, 393 F.3d at 777 (holding that section 512(h) applies only to ISPs engaged in storing copyrighted materials and not to conduits for transmission of materials of others).

101. *Id.* at 778 (Murphy, J., dissenting).

against individual users, the dissent argued, is "the only practical means" to protect copyright in the peer-to-peer context.[102]

The majority opinions in *Verizon* and *Charter* and the dissenting opinion in *Charter* reflect fundamentally different views of the purpose of the safe harbor provisions and suggest very different approaches to law and technology. The majority in *Charter* perceived the safe harbor provisions as a social bargain, striking a balance between the need to promote the continued growth of electronic commerce—by immunizing ISPs from liability for infringing use of their system—and to enforce intellectual property rights and minimize online piracy.[103] The dissent, by contrast, viewed the DMCA as legislation that primarily sought to address piracy.[104] ISPs were shielded from liability for infringement by their customers in exchange for assistance in the enforcement efforts of copyright owners.[105] In fact, the safe harbor provisions were intended to create "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment . . . ."[106]

Both *Verizon* and *Charter* found that the DMCA reflected a balance of interests that fit the old architecture, and that new technology would require reconsideration of this balance. The dissent in *Charter*, however, did not believe that peer-to-peer technology raised any new considerations. It did note, however, that peer-to-peer increases the threat of piracy and may require more assistance of ISPs in enforcing copyright.[107] Therefore, if a new balance is necessary, it would re-

---

102. *Id.* at 779.

103. *Id.* at 774 (majority opinion).

104. Judge Murphy admits that "[i]n enacting the DMCA Congress sought to protect both the interests of copyright holders and of internet service providers concerned about their own liability for infringement by their customers," but perceives the legislative solution as limiting the liability of ISPs in exchange for "more direct means to attack digital piracy." *See id.* at 778 (Murphy, J., dissenting).

105. The intent of Congress in enacting the DMCA was to address "massive piracy" of copyrighted works over digital networks without hampering technological development of the internet by the threat of third party liability for service providers. ISPs were only shielded from monetary and injunctive liability in exchange for their assistance in identifying subscribers who engage in acts of piracy over the networks and in removing or disabling access of infringers to protected works when technically possible.

Id. at 782 (citation omitted).

106. *Id.*

107. *Id*. at 779 ("Congress recognized the need to address infringement through conduit service providers in the DMCA, and its opening section applies to networks which transmit infringing materials in the direction of their users.").

quire a tilt towards stronger means for enforcing copyright and a broadening of the scope of ISP liability.

This analysis demonstrates the limits of the DMCA as technologically specific legislation. The DMCA relies on a specific architecture and assumes a specific technological state of art. It was designed to address a mainly centralized architecture, in which communication among users involved different functions of service providers, hosting content on large servers or linking to content posted by others. Peer-to-peer architecture, by contrast, is decentralized and allows users to search for files stored in the libraries of other users. The function of ISPs within peer-to-peer networks is merely that of a conduit, facilitating the transfer of files through its network.

3. Strict Liability for Infringing Peer-to-Peer Traffic?

Could ISPs be held strictly liable for peer-to-peer infringing traffic? Direct liability for copyright infringement under sections 501 and 106 of the Copyright Act requires a showing that one is engaged without authorization in conduct that is exclusively reserved to copyright owners.[108] These rights include the exclusive right to copy and distribute copyrighted works. Unlicensed copies of copyrighted works will normally constitute a copyright infringement, unless exempted or otherwise authorized by the applicable copyright law.

The most obvious ground for copyright liability arises from the fact that ISPs carry peer-to-peer traffic. An ISP acting as a conduit for peer-to-peer traffic could be held liable for infringing copyright by virtue of copying (including temporarily copying) and transmitting copyrighted materials without authorization. A preliminary question would be whether temporary files which reside on the ISP's systems, or are temporarily stored in the ISP system cache (*i.e.*, temporary storage of files previously delivered by the ISP), constitute copying, and if so, whether this copying is permitted by law.

The first case to address the liability of ISPs for infringing materials posted by their users was *Playboy Enterprises, Inc. v. Frena*.[109] This case involved a BBS (bulletin board system) which allowed users

108. "[T]he owner of a copyright . . . has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies . . . (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies . . . of the copyrighted work to the public . . . and (5) . . . to display the copyrighted work publicly." 17 U.S.C. § 106 (2000). Engaging in or authorizing any of these actions without permission violates the exclusive rights of the copyright owner and constitutes infringement of the copyright. *See* 17 U.S.C. § 501.

109. 839 F. Supp. 1552 (M.D. Fla. 1993).

to upload and download photographs, some of which were infringing copies of photographs owned by Playboy. Even though no copying was actually done by the defendant, the court considered the services provided by the defendant to constitute distribution of infringing materials, and therefore found the defendant liable for direct infringement of copyright.[110] This decision remained controversial and was criticized both for its legal analysis and the legal policy it established. The main concern of critics was that the basic functions of online intermediaries, which involve copying, distribution, and public performance, would require authorization under copyright law. Applying a strict liability standard to ISPs would prevent new intermediaries from functioning and the Internet industry from flourishing.

Soon after, in 1995, this standard was rejected in a preliminary injunction issued by the district court in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[111] In contrast to *Frena*, the *Netcom* court held that ISPs providing Internet access or bulletin board service are not liable for direct copyright infringement under section 106 of the Copyright Act.[112] The decision was based on a rather innovative interpretation of copyright law and on policy reasoning. Legally speaking, although copyright infringement is based on strict liability principles—no knowledge needs to be proved—it still requires actual conduct, an "aspect of volition or causation," which is absent when someone simply owns a system that others use to make copies.[113] The court concluded that the mere functioning of a conduit did not involve sufficient volition to establish copyright liability.

The *Netcom* court further noted that it would be unreasonable to make ISPs strictly liable for infringing content distributed by their users, since ISPs cannot reasonably prevent such activity, nor can they deter or screen out infringing bits.[114] Explicitly articulating the policy considerations underlying its holding, the court stated that it would not make sense to hold liable "countless parties, whose role . . . is nothing more than setting up and operating a system that is necessary for the

110. *Id.* at 1555–59.

111. 907 F. Supp. 1361 (N.D. Cal. 1995).

112. *See id.* at 1372–73.

113. *See id.* at 1370 ("Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.").

114. *Id.* at 1372–73. This may no longer hold true today. It may be technically possible for an ISP to prevent infringements. The question is whether we believe this would be desirable.

functioning of the Internet."[115] The function that constitutes the basis for liability of mere conduits is the same function without which the Internet as a medium would be crippled.[116]

The *Netcom* case was a preliminary decision by a district court. Due to its rigorous analysis and long-term significance for the blooming Internet industry, however, it has been religiously followed by many courts addressing the copyright liability of ISPs.[117] The legislative history of the DMCA describes it as "the leading and most thoughtful judicial decision to date."[118] The *Netcom* decision is particularly relevant to the potential liability of ISPs for infringing peer-to-peer traffic, since it dealt with an ISP providing Internet access, which is the primary function of ISPs in facilitating peer-to-peer systems.

For a long time, the scope of the *Netcom* analysis was unclear. It was argued that the DMCA safe harbor provisions codified and supplanted the *Netcom* holding.[119] Under this view, Congress endorsed *Netcom*'s limited liability principles but elected to implement them rather narrowly, exempting only a selective list of functions performed by ISPs.[120] Such a view also laid the groundwork for a narrow reading of the DMCA exemptions. If an ISP is not eligible for any of

---

115. *Id.* at 1372.

116. *Id.*

117. *See, e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1078 (9th Cir. 2004); Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1178 (N.D. Ill. 1997); Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 931–32 (N.D. Cal. 1996); *see also* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.05[C] (1997); 2 PAUL GOLDSTEIN, COPYRIGHT § 6.4 n.93 (2d ed. 2005 Supp.).

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

119. See, for instance, appellant's argument in *CoStar Group, Inc. v. LoopNet Inc.*, 373 F.3d 544 (2004), that the DMCA safe harbor provisions codified the *Netcom* holding as an affirmative defense:

> In contrast to *Netcom*, the policy balance struck in the DMCA does not altogether prohibit plaintiffs from bringing direct infringement claims against "passive" ISPs. To the contrary, the DMCA presupposes the continued existence of such claims, and responds by codifying the *Netcom* rule as an affirmative defense to such claims. But the affirmative defense is not automatically available to an ISP, even if it is "passive" in *Netcom*'s sense of the word. Rather, any ISP may seek immunity within the DMCA safe harbors—even a non-"passive" ISP—but it must satisfy certain conditions to qualify.

Brief of Appellants at 25, *CoStar*, 373 F.3d 544 (No. 03-1911), *available at* http://www.eff.org/legal/ISP_liability/CoStar_v_Loopnet/costar_brief.pdf.

120. The legislative history suggests that Congress intended to codify "the core of current case law dealing with the liability of on-line service providers, while narrowing and clarifying the law in other respects." H.R. REP. NO. 105-551, pt. 1, at 11; *see also* S. REP. NO. 105-190, at 19–20 (1998).

these exemptions, it remains strictly liable for direct infringement under section 106 of the Copyright Act.[121]

This narrow reading of the DMCA safe harbor provisions was rejected by the Court of Appeals for the Fourth Circuit in *CoStar Group, Inc. v. LoopNet Inc.*[122] The court held that Congress's intention in enacting section 512 was not to preempt *Netcom* but to leave it to the courts to freely construe the Copyright Act and define the scope of liability; the safe harbor regime does not deny the original defenses against and limitations on liability as set forth in *Netcom*.[123] Rather, the Fourth Circuit held that it was Congress's intention "'to leave current law in its evolving state,'" while creating safe harbors that would allow ISPs to survive.[124]

The court further held that an ISP cannot be held directly liable without volition or causation.[125] Interpreting section 106, the majority held that to establish direct liability it is necessary to show actual infringing conduct with causality: "There must be actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the copyright owner."[126] Thus, the majority found that neither automated copying, nor the storage and transmission of copyrighted materials when directed by others, was enough to constitute infringement. In the same way, simply owning a machine that enables the preparation of infringing copies would not result in strict liability for the machine owner, because the passive ownership and management of an electronic Internet facility does not satisfy the volition or causation required under *Netcom*.[127] An ISP is analogous to the owner of a traditional copying machine who makes it available to the public. Moreover, the conduct in which ISPs typically engage when they function as conduits hardly involves copying within the meaning of section 106(1).[128] To constitute copyright infringement, the system must make copies, namely, "material objects . . . in which a

121. *See* Brief of Appellants, *supra* note 119, at 26–27.

122. *See CoStar*, 373 F.3d at 552.

123. The DMCA "did not preempt the decision in *Netcom* nor foreclose the continuing development of liability through court decisions interpreting §§ 106 and 501 of the Copyright Act." *Id*. at 552–53.

124. *Id.* at 553 (quoting S. REP. NO. 105-190, at 19). Therefore, the court concluded, a safe harbor is a floor, not a ceiling, exempting what was necessary for the survival of the ISPs. *Id.*

125. *Id*. at 550.

126. *Id*.

127. *Id.*

128. *Id.* at 556.

work is *fixed*."[129] A system like that in *CoStar* creates copies, but they are not fixed for more than a transitory period. The transitory nature of the copies is both quantitative, in that their duration is temporary, and qualitative, in that copies are in transition and are automatically transmitted to others. Therefore, there is no liability for passively storing materials at the direction of users, as when an ISP-owned electronic facility responds automatically to user input without the ISP's intervening conduct.[130]

The court in *CoStar* even went a step further, holding that screening and gate-keeping functions automatically performed by the ISP do not constitute volition. Screening, the court said, is analogous to setting up a guard to prevent users from infringing copyright. It does not suggest an intention to seek out or select materials for publication.[131]

Copying facilitated by ISPs in the course of peer-to-peer operation is ancillary to the copying of files initiated and executed by the users of the peer-to-peer networks. Copies created on the ISP's system are automatic and involve no human intervention. The ISP is a passive conduit for transmission of copyrighted materials initiated by others. It is therefore unlikely that ISPs will be held directly liable for infringing copies automatically created by peer-to-peer users. The same analysis would apply to other potential claims of copyright infringement such as the distribution of copies or making copyrighted materials available.

4. Secondary Liability

a. Standard of Liability

As discussed in the previous section, it is unlikely that ISPs will be held strictly liable for infringing peer-to-peer traffic. A second ground for ISP liability for infringing peer-to-peer traffic is secondary

129. 17 U.S.C. § 101 (2000) (emphasis added).

130. In fact, the circumstances described in *CoStar* are more challenging than those raised by ISPs facilitating peer-to-peer traffic. The defendants in *CoStar* operated a website which actually stored the infringing materials. In an ISP/peer-to-peer situation, no copy is ever actually saved on the system, although many transitory copies are created online. *See CoStar*, 373 F.3d at 550–51.

131. *See CoStar*, 373 F.3d at 556. The dissent disagreed, arguing that screening is not passive conduct, but rather an affirmative act which involves discretion, and therefore implicates volition (defined as "the act of willing or choosing"). *Id.* at 560 (Gregory, J., dissenting) (internal quotations omitted). Unlike *Netcom*, where copying by the ISP was incidental and automatic and therefore passive, in the case of LoopNet's system, there was human intervention involving a choice to publish. Since the defendant in this case was able to actually screen the materials, the dissent found that the defendant resembled a traditional publisher and should likewise be liable. *Id.* at 560–61.

liability. Secondary liability under copyright law is grounded in common law principles, and imposes liability on one who contributes to direct infringement by "intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it."[132]

In its 2005 decision in *Grokster*, the Supreme Court expanded the scope of secondary liability for copyright infringement, defining it more broadly than it had previously been understood in the technological context. *Grokster* dealt with the liability of product distributors—specifically, distributors of peer-to-peer technology—for "acts of copyright infringement by third parties."[133] Yet, the fundamental point of *Grokster* applies to the general scope of secondary liability.

Prior to *Grokster*, there was more or less a homogenous set of rules regarding secondary liability, for which *Sony Corp. of America v. Universal City Studios, Inc.* was a common ground.[134] In the early days of the doctrine of contributory infringement, a distinction was maintained between providing "the site and facilities" used for direct infringement (*i.e.*, dance halls, swap meets)[135] and providing devices which could be used to infringe copyright (*i.e.*, VCRs).[136] The distinction between facilitators and device manufacturers blurred in the online environment, where services, products, and facilities are merged.

The first decision to address contributory liability of an ISP was *Netcom*, in which the court made the critical move from strict liability to secondary liability,[137] thus introducing the need to establish that the defendant knew of the infringing activity by direct infringers.[138] Liability upon notice, although far more limited than strict liability, created a high degree of uncertainty regarding the scope of liability of ISPs. Knowledge was established if the ISP was notified of the copyright infringement, unless the ISP could not reasonably verify the likelihood of infringement, the validity of copyright, or the absence of fair use.[139]

---

132. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2776 (internal citations omitted).
133. *Id.* at 2770.
134. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
135. *See, e.g.*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (discussing pirated copies sold at swap meet).
136. *See, e.g*., *Sony*, 464 U.S. 417.
137. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1371, 1373 (N.D. Cal. 1995); *see also supra* Part III.B.3.
138. *See Netcom*, 907 F. Supp. at 1373.
139. *See id.* at 1374.

The Court of Appeals for the Ninth Circuit has further developed the standard of knowledge necessary for contributory liability, by distinguishing between *actual knowledge* and *constructive knowledge* of the infringing activity.[140] Evaluating this standard in *A & M Records, Inc. v. Napster*, *Inc.,* the court found that Napster had *actual* knowledge of its users' infringement, because it acquired specific information of the infringing activity and failed to act to prevent it.[141] The court then turned to examine whether Napster also had, as the district court found, *constructive knowledge* (as distinct from actual knowledge), namely, whether it had reason to know of the infringing activity. Since the Court in *Sony* did not define the requisite level of knowledge,[142] the Ninth Circuit in *Napster* chose to incorporate *Sony*'s principle into the knowledge requirement:

> Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material. To enjoin simply because a computer network allows for infringing use would, in our opinion, violate *Sony* and potentially restrict activity unrelated to infringing use.[143]

The Court of Appeals for the Ninth Circuit's decision in *Grokster* pushed this distinction between actual knowledge and constructive knowledge a little further, holding that it is necessary to show actual knowledge at the time during which the defendant materially contributes to the infringement.[144] Constructive knowledge could only apply when a device *is not* capable of non-infringing uses, since it is obvious that the manufacturer and distributors knew of the infringement. It is only where there is non-infringing use alongside the infringing uses that *actual knowledge* is required.[145]

---

140. Other cases have applied similar standards. *See*, *e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1076–77 (9th Cir. 2004) (holding that actual knowledge is not required for contributory infringement, that *reason to know* will suffice to sustain liability, and that, since notice was properly served, AOL could have had reason to know that its USENET network was being used for infringing activity).

141. 239 F.3d 1004, 1021 (9th Cir. 2001) ("[I]f a computer system operator learns of specific infringing materials available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement.").

142. As the *Napster* court explained: "The *Sony* Court declined to impute the requisite level of knowledge where the defendants made and sold equipment capable of both infringing and 'substantial non-infringing uses.'" *Id.* at 1020.

143. *Id.* at 1021 (citations omitted).

144. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1162 (9th Cir. 2004).

145. *Id*. at 1161.

Considering the same distinction between actual knowledge and constructive knowledge while addressing the issue of contributory liability, the Seventh Circuit's decision in *Aimster* held that encryption of file exchanges constitutes "willful blindness,"[146] *i.e.,* constructive knowledge. Yet, on other grounds, the *Aimster* decision is a notable exception. In place of contributory liability, the court suggested a different rule: ISPs should be held liable if they failed to act against copyright infringement, unless they show that it would be disproportionately costly to take measures to reduce infringement.[147]

b. ISP Secondary Liability for Infringing Peer-to-Peer Traffic

ISPs could be subject to secondary liability for infringing peer-to-peer traffic under a few different categories. The precondition for all categories of secondary liability is direct infringement by a third party, and it is fair to assume that peer-to-peer networks are prominently employed for sharing copyrighted files without authorization.[148]

To be liable for contributory infringement, the defendant must materially contribute to the direct infringement by users.[149] Material contribution may take the form of inducing, encouraging, assisting, or otherwise facilitating the infringement by providing the means or the facilities for the infringing acts. ISPs could be found to contribute to the infringing behavior by connecting, facilitating links to, and hosting websites that distribute infringing applications or the "torrent files" used by the BitTorrent application. Indeed, the content industry has launched successful legal attacks on websites distributing torrent files.[150] However, there is nothing new in this legal outcome, which is

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

147. *Id.* at 653.

148. Given that many of the files exchanged on peer-to-peer networks are copyrighted, and that copies are created, distributed and made available without the authorization of the copyright owner, it is fair to assume that the prominent use of peer-to-peer networks is infringing copyright.

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

150. The MPAA launched a legal campaign against BitTorrent file-swapping networks, targeting websites that acted as directories for available files on the network. *See* John Borland, *MPAA Targets Core BitTorrent, eDonkey Users*, CNET NEWS.COM (Dec. 14, 2004), http://news.com.com/MPAA_targets+core+BitTorrent%2C+eDonkey+users/2100-1025_3-5490804.html?tag=nl. Websites such as SuprNova.org and Youceff.com provided links to meta-data files ("torrent" files), which identify the content of the file and include information about how to reach the relevant tracker server. Tracker servers keep a global registry of all the downloaders and seeds of a particular file, and respond to users' requests with a list of peers who have chunks of the requested file. The user must then contact these peers directly for downloading the necessary chunks. The advantage of this central directory structure is that it al-

based on the same principles under which website owners and ISPs have been held liable for sites that distribute infringing materials. Notice and take down has been efficient for that purpose in the past, and the hosting of infringing torrent files could still be addressed under the DMCA's safe harbor regime.

It is also arguable, however, that, by transferring and routing the infringing files (through the operation of peer-to-peer networks), the ISP's network provides the "site and facilities" for the infringement to take place. Based on *Netcom*,[151] *Napster*,[152] and, more recently *Ellison v. Robertson*,[153] the courts are likely to find material contribution in providing a service that allows for the automatic distribution of files, infringing and non-infringing, when the ISP knows (or should know) of the infringing activity and continues to aid it by enabling the distribution of copies.[154] Since ISP facilities are capable of significant non-infringing use, it would be necessary to show "reasonable knowledge of specific infringing files" at the time during which the ISP materially contributed to the infringement.[155] Acquiring such knowledge may depend on the particular design of the ISP's facility. As further discussed in Part IV, the choices of ISPs regarding design are likely to be affected by the liability standard; if knowledge is necessary for establishing liability, ISPs may redesign their systems to minimize the information they provide on peer-to-peer activities.

Vicarious liability could be another basis for holding an ISP

---

lows filtering out faked files and therefore increases the functionality and speed of the network. Such infrastructure, however, creates easily identifiable targets for litigation and makes BitTorrent vulnerable to legal suits by copyright owners. *See* J.A. POUWELSE ET AL., THE BITTORRENT P2P FILE-SHARING SYSTEM: MEASUREMENTS AND ANALYSIS (2005), *available at* http://www.isa.its.tudelft.nl/~pouwelse/Bittorrent_Measurements_6pages.pdf.

151. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1373–75 (N.D. Cal. 1995).

152. A & M Records, Inc., v. Napster, Inc., 239 F.3d 1004, 1019–22 (9th Cir. 2001).

153. Ellison v. Robertson, 357 F.3d 1072, 1080–81 (9th Cir. 2004) (holding that AOL's storage of Robertson's infringing materials on its USENET servers for fourteen days was "intermediate and transient" for purposes of Section 512(a), but that AOL would be entitled to safe harbor immunity only if it took reasonable steps to implement policy providing for termination of service access to repeat infringers, as required by section 512(i)).

154. In *Netcom*, the court found that the plaintiff had raised a genuine issue of fact regarding the liability of an access provider for infringing materials briefly residing on its servers, citing evidence that "with an easy software modification Netcom could identify postings that contain particular words or come from particular individuals," and delete those postings from its system (thereby preventing their propagation). *See Netcom*, 907 F. Supp. at 1376.

155. *Napster,* 239 F.3d at 1021, 1027; *see also* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1161–62 (9th Cir. 2004); *supra* Part III.B.4.a.

secondarily liable for peer-to-peer traffic. To prove vicarious infringement, copyright owners must show that ISPs benefit financially from the infringing activity and that they have the right and ability to supervise the infringers.[156] ISPs have, of course, benefited tremendously from peer-to-peer networks, which draw new subscribers to their service and create a demand for more high-speed bandwidth.[157] Yet, vicarious liability does not seem to present the strongest basis for liability of ISPs for the infringing behavior of their users. Peer-to-peer networks connect users of many ISPs, and do not reside on any particular ISP facility. In such circumstances, whether ISPs have the right and ability to control the behavior of peer-to-peer users may not be a trivial question.[158]

Finally, it is necessary to consider the potential liability of ISPs under the inducement theory. ISPs are often mainstream, well-financed, risk-averse entities, and are therefore less likely to explicitly encourage infringing conduct. Even if some users are using peer-to-peer networks for infringing copyrights, their infringements are neither induced nor encouraged by ISPs. Yet, as the following discussion demonstrates, if receiving benefits and failing to undertake sufficient preventive measures could constitute intent for the purpose of establishing inducement, ISPs could be vulnerable to liability under the inducement doctrine.

c. Grokster *Rule Examined*

The Supreme Court in *Grokster* paid tribute to the need to strike "a balance between the interests of protection and innovation."[159] The only Supreme Court case regarding secondary liability in copyright

156. *See* Gordon v. Nextel Commc'ns and Mullen Adver., Inc., 345 F.3d 922, 925 (6th Cir. 2003) (citing Shapiro, Bernstein & Co., Inc. v. H. L. Green Co., Inc., 316 F.2d 304, 307 (2d Cir. 1963)).

157. *See* Joanna Glasner, *P2P Fuels Global Bandwidth Binge*, WIRED NEWS, Apr. 14, 2005, http://www.wired.com/news/business/0,1367,67202,00.html (describing how increased use of bandwidth by peer-to-peer users drives ISP revenue). In the Ninth Circuit, to show vicarious infringement it is sufficient that the infringing activity draws customers. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263–64 (9th Cir. 1996). In *Ellison*, the Ninth Circuit found that even though access to USENET was not the primary reason why users join AOL, a fraction of AOL's earnings directly result from providing access to USENET. *Ellison*, 357 F.3d at 1079.

158. The legal right to control the use of an ISP facility is usually governed by the service agreement between the ISP and its subscribers. Yet, users of peer-to-peer networks could be subscribers of other ISPs and would not be bound by such an agreement. For further discussion on the technical ability of ISPs to supervise peer-to-peer networks, see *infra* Part V.A.

159. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2782 (2005).

law prior to *Grokster* was *Sony*, where the Court addressed secondary liability for infringement arising from the very distribution of a commercial product capable of infringing use.[160]

The majority opinion in *Grokster* understood the *Sony* decision as standing for the need to "leave[ ] breathing room for innovation and a vigorous commerce."[161] *Sony* struck such a balance "by holding that the product's capability of substantial lawful employment should bar the imputation of fault and consequent secondary liability for the unlawful acts of others."[162] The *Grokster* court's major point of departure from *Sony*, however, is in treating secondary liability as part of a whole set of theories, of which contributory infringement by "design or distribution of a product capable of substantial lawful use,"[163] is only a subset.

There are a few problems with this ruling. Most important are the ramifications of *Grokster* for network architecture and for innovation policy. The Court found inducement based, among other things, on Grokster's failure to undertake sufficient preventive measures against infringement. This broad interpretation invites legal intervention in shaping design through liability standards. This is further discussed in the next section below. A related consequence of the *Grokster* decision is the introduction of a super-category of liability, based on overreaching principles that are likely to enhance uncertainty and expand the scope of copyright.

The inducement doctrine as applied in *Grokster* creates an overlap between different categories of liability. The concurrence was aware of such potential overlap,[164] but failed to suggest an independent ground for liability. The *Grokster* rule, according to which contributory liability is only one subset of infringement liability, makes sense theoretically if one is truly able to distinguish between different categories of liability established on fundamentally different and independent grounds. That was the case with contributory infringement and vicarious liability, which include different elements and are based on different grounds. It is not the case, however, with the inducement doctrine under *Grokster*. Under this rule, liability by in-

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

161. *Grokster,* 125 S. Ct. at 2778. Pursuant to *Sony*, the court must "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 to freely engage in substantially unrelated areas of commerce." *Sony*, 464 U.S. at 442.

162. *Grokster*, 125 S. Ct. at 2782.

163. *Id.* at 2778.

164. *Id.* at 2783 (Ginsburg, J., concurring) ("While the two categories overlap, they capture different culpable behavior.").

ducement requires evidence of the following elements: (1) intent to bring about infringement; (2) distribution of a device suitable for infringing use; and (3) actual infringement by the recipients of the device.[165]

The new element required for inducement, which was not included in any of the existing categories of secondary liability, is intent. A closer look at this requirement, as applied by the Supreme Court in *Grokster*, reveals that intent could actually be proven by the same elements that establish vicarious and contributory liability.

The Court listed three types of evidence of intent in support of its finding that "respondents' unlawful objective is unmistakable":[166] (1) aiming to satisfy a known source of demand for copyright infringement—the markets comprising former Napster users,[167] which "indicate a principal, if not exclusive, intent on the part of each to bring about infringement";[168] (2) the failure to develop filtering tools;[169] and (3) the business model, in which the extent of the software's use determines the gains to the distributors.[170] This last test is particularly broad, since it is often the case that greater use of a product would increase revenues. The question is always whether the money is made from the infringing use.

Consider the following table:

---

165. *See id.* at 2780 (majority opinion).

166. *Id.* at 2782.

167. Designers of Grokster and other second generation peer-to-peer systems sought a shield under the *Sony* safe harbor. They did not conceal their attempt to target Napster's users, since their system offered users a different design. The difference in the design, however, was presumably affecting only the liability of the software provider. The infringing nature of file exchangers remained the same as in *Napster*.

168. *Grokster*, 125 S. Ct. at 2781. The Court emphasized marketing efforts such as targeting former Napster users to use OpenNap, "which was designed, *as its name implied*, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement." *Id.* at 2780 (emphasis added). The Court referred to basic promotion efforts, such as directing search engines to Grokster by tagging "Napster" or "free file sharing," and offering a program that is understood by these users to be the equivalent of Napster. *Id.* Grokster also placed links to the program in articles describing its ability to access popular copyrighted music. In addition, the Court noted that services like "Grokster" and "Swaptor" were "suggestively named." *Id.* at 2780–81.

169. *Id.* at 2781 ("[N]either company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant . . . we think this evidence underscores Grokster's and Streamcast's intentional facilitation of their users' infringement.").

170. The defendants made money by selling advertising space—the more software used, the more ads were sent out, resulting in greater advertising revenue. The Court notes, however, that this evidence alone is insufficient for establishing unlawful intent. *Id.* at 2781–82.

TYPE OF LIABILITY	DIRECT INFRINGEMENT BY PARTY OTHER THAN DEFENDANT	CONTRIBUTION	KNOWLEDGE	INTENT	FINANCIAL BENEFIT	RIGHT & ABILITY TO CONTROL INFRINGER
CONTRIBUTORY LIABILITY	Required	Required: Defendant ISP must "materially contribute" to the direct infringement by providing the means or facilities for the infringing acts.	Required: If the defendant ISP is capable of significant non-infringing use, must show "reasonable knowledge of specific infringing files" at the time of infringement.	Not Required	Not Required	Not Required
VICARIOUS LIABILITY	Required	Not Required	Not Required	Not Required	Required	Required
INDUCEMENT	Required	Not Required*	Not Required: Intent is arguably a higher standard than knowledge. Yet, simply awareness may satisfy this requirement.	Required: See Financial Benefit and note on Contribution for evidence of intent.	Not Required: Financial benefit, however, is considered evidence of intent–a required element.	Not Required

*But:

- Required elements include: (1) the distribution of devices suitable for infringing use; and (2) actual infringement by recipients of the device.
- Intent, another required element, could be established through: (1) contributing to direct infringement by satisfying a known source of demand for copyright infringement; or (2) failing to develop filtering tools.

Obviously, there could be several grounds for liability here, and inducement could provide an independent basis for secondary liability. As shown in the table, the elements required to establish inducement are essentially the same as the elements required to establish existing categories of secondary liability. If a new category of liability is based on the elements already included in other categories, the boundaries between the different liability categories are blurred and the categories are likely to merge into one. Developers of new technologies that are capable of non-infringing use may therefore also be required to undertake action to filter out infringing behavior. The result is the abandonment of the *Sony* safe harbor, which leaves no protection for the interests of innovation.

The *Grokster* standard could make ISPs liable for infringing peer-to-peer traffic. This potential for liability, in turn, is likely to affect monitoring and filtering technologies as well as the design of peer-to-peer systems. As further discussed in the next section, new applications must be supported by existing infrastructure.

IV.
Law and Technology: A Normative Framework

A. Those Capable Shall Also Be Liable

What is the appropriate scope of ISP liability for infringing materials distributed by their users? What normative framework should guide us in determining the boundaries of liability? This inquiry is particularly important in the post-*Grokster* era, since third party liability for copyright infringement will now be much more open-ended. Rather than clarifying *Sony*'s "substantial non-infringing use" rule and designing a single standard for technologically-oriented contexts, the Court applied a general theory of liability, thus opening the door to infinite grounds of liability in cases involving technology. Exploring the link between liability rules and innovation is therefore necessary for defining the boundaries of liability.

Moreover, liability for *inducement*, the Supreme Court held, requires proof of intent. What makes inducement so attractive for courts addressing liability issues is that it presumably has no implications for innovation. If one specifically intends to induce infringing activity, then one can be held liable on that ground alone, and courts are presumably relieved from having to balance copyright interests and freedom to innovate.

Yet, as applied by the Court in *Grokster*, inducement may have particularly significant consequences for system design. Under the in-

ducement doctrine, as applied by the Supreme Court, a *failure to diminish infringements* could prove an unlawful objective. This interpretation of inducement implies an affirmative duty to develop tools that would diminish infringement.[171] It follows that under certain circumstances, intermediaries, such as ISPs, might also have a duty to implement preventive measures. Under what circumstances should ISPs be required to undertake active steps to address copyright infringement?

Law and economics literature offers a normative framework for analyzing the scope of secondary liability. From an economic standpoint, liability for harm caused by one person should be imposed on third parties if they are able to prevent that harm in a cost effective way.[172] If ISPs can cheaply prevent the harms caused by infringement, including distinguishing lawful from unlawful users at a reasonably low cost, they should be accountable for their users' wrongdoings.[173] A similar standard was used by Judge Posner in the *Aimster* decision to define the liability of online service providers:

> Even when there are non-infringing 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.[174]

Some advocates of ISP liability, on the other hand, argue that it might still be efficient under some circumstances to hold ISPs liable, even when it would be prohibitively expensive for an ISP to distinguish legal from illegal copyright activity.[175] This is most likely to be

---

171. That is, of course, only if there is an indication of unlawful objective—but the problem is that the evidence in *Grokster* was somewhat circular.

172. *See generally* Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986); *see also* Assaf Hamdani, *Gatekeeper Liability*, 77 S. CAL. L. REV. 53, 98–108 (2003–2004) (applying similar analysis to securities context).

173. *See* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003). Under this negligence rule, ISPs would be liable if a "failure to take economically reasonable precautions results in a harm." *Id.* at 405.

174. *In re* Aimster Copyright Litig., 334 F.3d 643, 653 (7th Cir. 2003).

175. *See* Lichtman & Landes, *supra* note 173, at 404–05 ("[A]n entity like America Online would have a hard time differentiating the unlawful transmission of Mariah Carey's copyrighted music from the perfectly legitimate transmission of uncopyrighted classic music."). On the other hand, Lichtman has elsewhere proposed making ISPs liable to other potential hazards in the online environment. *See* Lichtman & Posner, *supra* note 79.

the case when there is a substantial public interest in eliminating the illegal use.

A major concern regarding ISP liability is that ISPs would fail to distinguish between legitimate and harmful behaviors and would opt for policies that eliminate any potentially risky behavior, even when those behaviors could be socially beneficial. The danger of eliminating potentially beneficial behaviors is even greater when one considers the ramifications of liability for infrastructure. As the following analysis shows, liability may affect design, thereby eliminating the potential benefits of peer-to-peer networks altogether.

The economic framework of secondary liability reflects the *least cost avoider* approach, which places the burden of avoiding the harm on the cheapest cost avoider. Accordingly, if ISPs are able to diminish or reduce copyright infringement by peer-to-peer networks, they must do so. This standard offers the familiar analysis of negligence, which simply requires the court to determine what technological measures are currently available and at what cost. Nevertheless, grounding liability in the availability and cost of technological preventive measures is theoretically unsound and fails to capture the complexity of technological markets. Consequently, as explained in the next section, it cannot provide a sound basis for regulating ISPs.

B. Analytic Flaws

A legal duty to implement preventive measures, unless they are disproportionately costly, presumes a particular view of technology and technological progress. Implicit in this analysis is that technological development is an independent phenomenon, determined by the laws of nature or some other intrinsic set of rules. Its potential development, in this view, is affected only by the material resources available and the limits of human cognition. Technologies are presumably out there, waiting for the courts to simply determine whether they provide a cost-effective solution to prevent, or at least reduce, the harm. Based on such evidence, the courts would determine whether a failure to implement these technologies should result in liability.

The main flaw in this analysis is that it fails to see technology as a dynamic parameter, and it overlooks the interconnection between law and technology. Technology does not stand alone. Rather, it is developed within a specific social and economic context. Technological progress is affected by a variety of factors, such as technical needs, economic structures, social processes, social values, scientific progress, and sometimes even plain coincidence and luck.

Laws can affect technological progress and the availability of technology. The most obvious example is when a particular technology is outlawed. Some laws directly regulate technology and technological development. Section 1201, added by the DMCA, for instance, explicitly outlaws the manufacturing of any technology that is primarily designed for the purpose of circumventing technological measures that protect copyright.[176] Laws may further outlaw human cloning technology, or strictly forbid any use of embryonic stem cells in the research and development of new drugs. Laws that prohibit the development or implementation of certain technologies create disincentives for developing those technologies. Thus, legal exposure under the DMCA anti-circumvention provisions may chill investment in circumvention technologies. Even if the law cannot entirely prevent technologies from emerging, especially where new technologies are often introduced outside the law's jurisdiction, banning certain technologies makes them riskier and therefore more expensive to develop.

Laws may also regulate technology by mandating specific design. The most detailed example of a technological capability requirement is the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which requires that telecommunications infrastructure enable wiretapping by the government pursuant to a lawful authorization or a court order.[177] The Audio Home Recording Act of 1992 (AHRA) is another example,[178] requiring all digital audio recording devices to implement Serial Copy Management System (SCMS) or similar technological measures which allow for the creation of an unlimited number of first generation copies but no second generation copies.[179]

Nonetheless, the consequences of laws for design are often more subtle. Such influences are especially likely when laws shape the markets in which technology occurs. The availability of specific applications may often require investment in research and development to produce specific technical solutions. Intellectual property laws may affect such incentives by offering protection to some technologies while denying protection to others.

---

176. 17 U.S.C. § 1201 (2000).

177. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2000)).

178. Pub. L. No. 102-563, 106 Stat. 4237 (codified at 17 U.S.C. §§ 1001–1010 (2000)).

179. 17 U.S.C. §1002(a). Furthermore, AHRA, like the DMCA anti-circumvention provisions, prohibits devices and services directed at tampering with the copy control mechanisms of digital recording devices. 17 U.S.C. § 1002(c).

Several commentators have acknowledged the link between liability and innovation, raising concerns that a high level of uncertainty regarding the scope of liability could stifle innovation.[180] Liability that is based on applying abstract principles, rather than concrete rules, is especially likely to increase uncertainty. For instance, the unclear scope of the inducement theory of liability is one reason why *Grokster* could have long-term consequences, regardless of whether it would actually deter current distributors of existing peer-to-peer applications. Developers of new technologies may find it difficult to predict the scope of their liability, and may choose to be excessively cautious. Furthermore, the risk of liability may chill investment in new technologies.

Liability rules may also affect the availability of technologies by shaping the behavior of market players who engage in the development of new technologies. Potential liability could impact the development of new technologies by increasing the demand for specific designs and inducing investments in developing particular technologies. Liability based on the failure to implement precautions against copying, for instance, may increase demand for certain applications that prevent copying or filter out copiers. Such a demand is likely to induce greater investments in research and development, which are likely to make these technologies available sooner. The price of new technologies could also be affected by liability. Strong demand for certain technologies would stimulate competition among innovators—competition that is likely to improve the effectiveness of technical solutions and reduce their price.

Consequently, the availability and cost of certain technologies would be the outcome of applying specific legal rules. Applying the least cost avoider approach in the context of dynamic technological environments would therefore lead to a form of circular reasoning: we would hold parties liable for failing to employ cost-effective (*i.e.*, efficient) measures, while the cost and availability of such measures would themselves be affected by the liability rule. Therefore, as I have argued elsewhere, technological development cannot be considered exogenous to liability analysis.[181]

It is arguable that incentives to develop new technologies have always been affected by legal rules, but the pace of technological change made it reasonable to treat the incentives as fixed. The nineteenth-century steam engines that released sparks on the railway and

180. *See, e.g.*, Lemley & Reese, *supra* note 25.

181. NIVA ELKIN-KOREN AND ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE 100–07 (2004).

sometimes caused fires in nearby farmers' fields developed into the much safer locomotives of the twentieth century.[182] The ease with which information technologies can be shaped and modified and the pace of technological change suggest that in the information environment, the least cost avoider approach should be applied with greater caution. Since the availability and cost of preventive measures could be affected by legal rules, these parameters cannot be the sole basis for liability. Liability that arises from the cost of preventive measures is based on a snapshot of technology at any given time, overlooking the long-term impact of legal rules on the availability of such technologies. This is a particularly shaky foundation for information policy, given the rapid pace of technological change. Therefore, courts and policy makers defining the scope of secondary liability should take into account the long-term ramifications for design.

C. Designing Liability While Considering Design

The most recent example of the dialectic relation between liability rules and design is the change introduced in the BitTorrent file-sharing program. BitTorrent was designed to improve the efficiency of downloading in peer-to-peer systems by permitting simultaneous uploading and downloading of fragments of files.[183] In order to share a file in BitTorrent, a user must first create a torrent file, which operates as a pointer. The torrent file does not contain the shared file itself. Rather, it contains relevant information regarding the shared file, such as its file name and size, the hash of each block in the file, and the address of a "'tracker'" server, which directs uploading and downloading of packets through BitTorrent. The tracker maintains a log of which users are downloading the file and where the file and its fragments reside.[184] Users who want to download a file must first download its torrent and communicate with the tracker at regular intervals to receive up-to-date information.[185] The BitTorrent trackers have been a key resource for anti-piracy efforts in identifying infring-

182. Steam locomotives were used by Pigou to demonstrate the traditional economic analysis of externalities. A. C. PIGOU, THE ECONOMICS OF WELFARE (AMS Press 1978) (1932).

183. BitTorrent was developed by Bram Cohen and was first released in 2001. *See* Clive Thompson, *The BitTorrent Effect*, WIRED, Jan. 2005, at 151.

184. The user who has all the fragments of the file is called a "seeder." The BitTorrent client (the one who created the torrent file in the first place) is then started as a "seed node," allowing other users to connect and commence downloading. When other users finish downloading the entire file, they can "reseed" it and become an additional source for the file. *See* Wikipedia, *BitTorrent*, http://en.wikipedia.org/wiki/Bittorrent.

185. *See id.*

ers who downloaded and shared copyrighted material. They were the first to be sued in the current content industry battle against BitTorrent.[186] After a few major tracker websites were shut down,[187] a new beta version of BitTorrent was released, eliminating the need for websites that aggregate torrent files, *i.e.*, the trackers.[188] With no central features, the new design makes it more difficult for copyright holders to track and shut down illegal file sharing.[189]

It is anticipated that peer-to-peer networks will adjust themselves to increasing legal pressure as well. A new type of peer-to-peer network, recently announced, allows users to establish a secured network available only to trusted members. The goal is to create a closed network, a "Darknet," permitting secure communication that cannot be penetrated by governments or corporations.[190] The declared purpose is to avoid censorship and facilitate political freedom among members of the community.[191]

A similar example is the system addressed in *Aimster*.[192] The defendant operated a central-server, peer-to-peer, file sharing system, in which all communication among users was encrypted and decryption was performed by the recipient of the files.[193] By using en-

186. LokiTorrent was a famous torrent website with 680,000 active registered members and 1.8 million hits per day. It was shut down in January 2005, after the MPAA filed suit. *See* Michael Ingram, *LokiTorrent Caves to MPAA*, SLYCK NEWS, Feb. 10, 2005, http://www.slyck.com/news.php?story=661.

187. Major websites such as SuprNova.org and elitetorrents.org were shut down after being sued by copyright owners. *See* Seán Byrne, *SuprNova.org Has Closed Down Its BitTorrent Service for Good*, CDFREAKS.COM, Dec. 20, 2004, http://www.cdfreaks.com/news/11089; Thomas Mennecke, *MPAA, FBI and U.S. Customs Shut Down EliteTorrents*, SLYCK NEWS, May 25, 2005, http://www.slyck.com/news.php?story=802.

188. The new version was announced in May 2005. *See* BitTorrent, BitTorrent Goes Trackerless: Publishing with BitTorrent Gets Easier!, http://www.bittorrent.com/trackerless.html (last visited Mar. 6, 2006) ("As part of our ongoing efforts to make publishing files on the Web painless and disruptively cheap, BitTorrent has released a 'trackerless' version of BitTorrent in a new release.").

189. It has been suggested, however, that BitTorrent files could still be identified, since even without tracker sites, someone still hosts the infringing files. *See* Renai LeMay, *BitTorrent Enemies Face New Hurdle*, CNET NEWS.COM, May 20, 2005, http://news.com.com/BitTorrent+enemies+face+new+hurdle/2100-1032_3-5715093.html; *see also* Quinn Norton, *May the Source Be with You*, THE GUARDIAN, June 2, 2005, *available at* http://www.guardian.co.uk/online/story/0,3605,1496722,00.html.

190. *See* John Markoff, *File Sharers Anonymous: Building a Net That's Private*, N.Y. TIMES, Aug. 1, 2005, at C1 [hereinafter *File Sharers Anonymous*]; John Markoff, *A Safer System for Home PC's Feels Like Jail to Some Critics*, N.Y. TIMES, June 30, 2003, at C1.

191. *See File Sharers Anonymous*, *supra* note 190.

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

193. *Id.* at 646.

crypted communication, Aimster hoped to shield itself from actual knowledge of unlawful uses of its system and thereby avoid contributory liability. In fact, when Aimster was sued by the recording industry, the company argued that since the files were encrypted, it lacked the necessary knowledge regarding infringing uses that liability for contributory infringement requires.[194] The Court of Appeals rejected this argument, holding that the use of encryption to avoid liability amounts to willful blindness and therefore constitutes knowledge sufficient for liability.[195]

Shaping new technologies through liability rules could be tricky. It must take into account the implications of liability on a complex environment, in which both market and non-market players are acting. A negligence standard, for instance, could prove counterproductive for enhancing efficient prevention. Developers of new technologies would typically tailor their applications to address the needs of a specific market niche, and would therefore be affected by the interests of content providers and ISPs.

If ISPs are made liable only when preventive means are available, there will likely be less investment in applications that allow peer-to-peer control at the level of the network. The reason is that ISPs are the potential buyers of such technologies. They would neither invest in, nor otherwise encourage the development of, such measures, fearing that the resulting technologies would increase their potential liability. Entrepreneurs would lack any incentive to develop such applications if they are unlikely to be purchased by ISPs.

Strict liability, by contrast, may boost investment in technologies for controlling peer-to-peer file sharing. Strict liability of ISPs for peer-to-peer file sharing would induce investment in the creation of filters and blocking measures. As further explained in the next section, strict liability is likely to encourage redesign of the architecture of peer-to-peer networks and to shape it in the form of distributed broadcast.

Obviously, copyright owners may also have incentives to develop peer-to-peer management tools, but they are only able to control the content itself and cannot directly affect the design of distribution channels. Once a copyrighted work is decrypted, it can be distributed freely through the network. Governing the distribution infrastructure requires the cooperation of ISPs. Therefore, control over the infrastructure makes ISPs a key player in content providers' enforcement

194. *Id.* at 650.
195. *Id*.

campaigns. Liability may thus affect architecture by determining the types of preventive means that are likely to be developed and whether development will focus on redesigning distribution flows in peer-to-peer networks or encrypting individual pieces of content.

So far, the analysis has suggested that innovation is produced only by markets. New technologies, however, can also be introduced by non-market players. Peer production projects, which take advantage of collaboration among users,[196] as well as technological breakthroughs by individual developers, could challenge peer-to-peer management tools. Peers engaged in collaborative projects or individuals engaged in innovative breakthroughs will often act voluntarily, driven by non-monetary incentives. Non-market players' research agendas are affected by intrinsic incentives, and not necessarily by capital. Consequently, the development of such subversive technologies would be less susceptible to external interests and less affected by liability.[197]

When capital is unnecessary for the production of new technologies, there is no capital to risk on an adverse legal judgment. The increased risk and cost associated with liability is unlikely to deter potentially disruptive technologies under such circumstances. New technologies are therefore likely to be introduced by non-commercial players who are challenging existing dominant technologies and threatening to eventually overturn them.

This observation may have significant consequences for defining the scope of liability in the information environment. Allocating liability and defining the scope of liability determines who bears the cost of updating systems in order to address continuous challenges by new technologies. A legal doctrine which considers a *failure to diminish* copyright infringement as a basis for liability implies a legal duty to take precautions against potential harm. A general duty to develop filtering tools may shift the cost of enforcement from copyright owners to ISPs and technology designers. Therefore, a duty to filter strengthens the bundle of rights granted *de facto* to copyright owners,

196. Peer production of informational goods requires the creative input of individuals and access to other informational goods which are non-rivalrous. *See* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 404–05 (2002).

197. *See* RICHARD M. STALLMAN, *Free Software: Freedom and Cooperation*, *in* FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN 155, 162, 171 (Joshua Gay ed., 2002) (explaining political agenda behind Free Software Foundation and GNU/Linux software); *see also* Josh McHugh, *The Firefox Explosion*, WIRED, Feb. 2005, at 92 (describing development of open source browser Mozilla, later Firefox, by two students).

allowing them to shift the cost of enforcement to ISPs rather than leaving it for negotiation between the parties.

V.
TECHNOLOGY AND BUSINESS: ISPS AND PEER-TO-PEER

A. What ISPs Could Be Doing About Peer-to-Peer Infringing Traffic

The Court of Appeals for the D.C. Circuit, in the *Verizon* case, concluded that there are fundamental differences between web distribution and peer-to-peer networks that render the DMCA inapplicable to the latter technology.[198] What are these differences, and are they likely to affect the consequences and, therefore, the desirability of secondary liability?

In the case of peer-to-peer file sharing, ISPs are no longer hosting infringing materials. The distribution of illegal materials takes place at the edges; the materials are hosted by individual computers, beyond the reach of the ISPs. Blocking or removing materials from these computers would be an invasion of privacy. ISPs do, however, design the gateways through which users must pass to use the Internet.[199] They are therefore capable of shaping many aspects of their users' online experience. They can make access to some sites easier than others and, using filtering software, can block some materials altogether. ISPs may also block individual users' access, and track their online activities.[200]

Is there anything ISPs could do about allegedly infringing peer-to-peer traffic? Web-based file sharing delivered from centralized servers to decentralized peers, file sharing facilitated through a central server (the Napster model), and distributed networks composed of peers sharing files directly (the Grokster model) all make use of ISP bandwidths and routing functions. Acting as a conduit for peer-to-peer traffic, however, infringing materials do not normally reside on ISP networks but are only transmitted through the network like any direct communication among users. Yet, there are many ways in

198. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003).

199. Search engines could also be thought of as gatekeepers, controlling the extent to which information becomes effectively accessible to users. The Internet developed an information glut in which users are increasingly dependent upon search engines for locating useful information. Content that is undetectable or otherwise remains unlisted in search results is practically nonexistent to the user since chances of locating it without the proper information are slim.

200. These capabilities made ISPs the object of legislation aimed at blocking access to obscene or child pornography materials. *See* 18 U.S.C. §§ 2251–2252 (2000).

which copyright owners could seek ISP assistance in enforcing copyright.

One way to facilitate copyright enforcement is through data retention and disclosure. ISPs may provide a robust database of online activities that make use of their network. Peer-to-peer communication leaves digital traces both on the client computer and on ISPs' servers. ISPs record this information as an integral part of their operations, and often retain it for system maintenance and billing purposes. Even users who manage to disguise their identity online by using a dynamic IP system, surfing through an anonymizer service, or encrypting their traffic by self-help means would normally be identifiable to the ISP for the purpose of technical support and payment of their monthly bills. ISPs are able to combine information regarding online identities and activities with the contact information for legal entities needed to impose legal liability. Having both technical connections and contractual relationships with subscribers, ISPs could identify users who are suspected of copyright infringement and provide copyright holders with the necessary contact information.

Furthermore, scrutiny of peer-to-peer traffic could be made possible through bandwidth monitoring or detection of peer-to-peer exchanges. Obviously, subscribers consume bandwidth for many legal purposes, such as Voice over Internet Protocol (VoIP) and web cameras. Still, this sort of monitoring could provide copyright holders with a short list of potential offenders.

Finally, ISPs could assist in private enforcement against copyright offenders. They could effectively prevent access to infringing materials by terminating the accounts of subscribers identified as engaging in massive peer-to-peer infringement. Terminating an account, however, is arguably a harsh sanction, since subscribers would normally use their account for both infringing and non-infringing activity, and there might be several users on one account.[201] However, ISPs could undertake less drastic measures against particular peer-to-peer networks, or against suspicious activities within peer-to-peer networks. They could, for example, cease to support technical standards which facilitate peer-to-peer networks, or attempt to interfere with

201. In *Verizon*, the court drew a distinction between removing materials and terminating the offending subscriber's account. The RIAA had argued that Verizon was in a position to "disable access" to infringing materials by terminating the accounts of infringing users. The court, however, held the statutory language to "establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material . . . ." *Verizon*, 351 F.3d at 1235.

their functioning.[202] One notable example of this approach is the demand made by GEMA, a German rights organization for composers, lyricists, and publishers,[203] which asked forty-two access providers to poison their Domain Name System (DNS) servers in order to block sites that provide links to peer-to-peer files.[204] "DNS poisoning" is a corruption of the process of locating IP addresses at DNS servers.[205] The result would be that inquiries by end users would be passed to invalid addresses.

B. ISP Self-Interest Regarding Peer-to-Peer

Peer-to-peer is no doubt a "killer application" that has attracted many new users to the Internet, in general, and created a rising demand for broadband connections in particular. This has been true for the sharing of music files, but has become especially evident with growth in the sharing of video files, which consumes much more bandwidth. Indeed, peer-to-peer traffic is considered by many to be the major force behind the Internet's expedited growth, which has benefited the ISP industry. However, peer-to-peer traffic also involves some downsides for ISPs. Even though ISPs derive great benefits from peer-to-peer, they may have an independent interest in

---

202. One example of pressure put on ISPs to change technical standards concerns the music software of AOL. AOL disabled a feature of Winamp, its music software, which had been used to evade copy-protection features of digital music services. The software allowed for the conversion of copy-protected music files into files that could be burned onto CDs. Although similar software is available online, technical changes made by AOL could prevent bypassing technological protection of music files by a large number of users. *See* John Borland, *AOL Blocks Music-Copying Features*, CNET NEWS.COM, Feb. 18, 2005, http://news.com.com/AOL+blocks+music-copying+feature/2100-1027_3-5582618.html.

203. *See* GEMA Homepage, http://www.gema.de/engl/home.shtml (last visited Sept. 22, 2005).

204. Press Release, GEMA, GEMA Calls for Illegal Music Download Portals to Be Blocked (July 8, 2005), *available at* http://www.gema.de/engl/communication/press_releases/pm20050708.shtml.

205. Wikipedia explains that DNS poisoning takes place when computers connected to the Internet are using Domain Name System (DNS) servers provided by the ISPs to locate Internet addresses. "DNS cache poisoning is a technique that tricks a DNS server into believing it has received authentic information when, in reality, it has not. Once the DNS server has been poisoned, the information is generally cached for a while, spreading the effect of the attack to the users of the server. . . . This DNS server generally serves the ISP's own customers only and contains a small amount of DNS information cached by previous users of the server." Wikipedia, DNS Cache Poisoning, http://en.wikipedia.org/wiki/DNS_cache_poisoning (last visited Sept. 19, 2005); *see also* SearchSecurity.com Definitions, *Cache Poisoning*, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1085136,00.html (last visited Sept. 19, 2005).

managing peer-to-peer traffic and reducing the bandwidth it consumes.

One problem associated with peer-to-peer networks is the high volume of traffic. Peer-to-peer communication consumes a large portion of network bandwidth. This heavy use is due not only to the size of the files exchanged, but also to the large amount of bandwidth required for overhead and coordination (*i.e.*, search, protocol chatter).[206] Peer-to-peer networks take advantage of distributed resources made available by users who participate in uploading and downloading, thus increasing the bandwidth consumption at the network level. In this sense, peer-to-peer networks are simply shifting the cost of distribution from servers to access providers.

Moreover, under existing pricing schemes, users do not internalize the cost of network usage. Users of peer-to-peer networks often leave their computers logged on continuously, queuing several files for download when they are away. ISPs currently apply flat rates for unlimited use, which means that there is no monetary incentive for users to reduce their peer-to-peer traffic. Increasing the bandwidth is unlikely to reduce bandwidth use either, since peer-to-peer networks would simply adjust to the larger amount of bandwidth available.[207]

Another issue is the network congestion that is caused by traffic patterns. Peer-to-peer distribution involves copying of files directly from other users, some of whom subscribe to other ISPs. It often involves the presence of duplicated files in different peer-to-peer networks and communication among distant users, which increases the

---

206. *See* Alex Goldman, *Building a Better P2P Delivery System*, ISP-PLANET, June 12, 2003, http://www.isp-planet.com/equipment/2003/cachepliance.html:

> When a Gnutella client receives a search query, it broadcasts that search to all the nodes it is connected to. Users place a limit on the number of hops a query can travel, but if that number is seven, and each of the six clients the query reaches are connected to only 10 hosts (as well as the originator), the network will propagate 1 million copies of the query (this also assumes none of the 1 million are connected to each other). . . . Gnutella spent 55 percent of its bandwidth on overhead like pings and pongs, and 35 percent of traffic on queries. Gnutella Pro eliminated the ping and pong traffic, but the problem remained that queries occupied the vast majority of all traffic. In either case, the traffic on a node rises rapidly as the size of the Gnutella network grows.

Id.

207. *See, e.g.*, P-CUBE, CONTROLLING PEER TO PEER BANDWIDTH CONSUMPTION 5 (2003), http://downloads.lightreading.com/wplib/pcube/controlling_peer_to_peer.pdf. Acquired in 2004 by Cisco Systems, Inc., "P-Cube is a leading developer of IP service control platforms." Press Release, Cisco Systems, Cisco Systems to Acquire P-Cube, Inc. (Aug. 23, 2004), *available at* http://newsroom.cisco.com/dlls/2004/corp_082304.html.

distance traffic has to travel. This heavier traffic can clog an ISP's main Internet pipe, slowing down overall communication. The high volume of traffic and congested Internet gateways could slow the response time of the network and require increasing investments in network upgrades.[208]

A third issue has to do with predictability. It is not only the volume of traffic that is problematic, but also the unpredictable downstream and upstream bandwidth generated by peer-to-peer networks. Network architecture assumes a specific type of usage.[209] Current network design is asymmetric, assuming more downloading than uploading. This is consistent with the earlier model of web distribution, in which users downloaded materials from central servers. Web applications involved a large amount of downstream traffic for a single upstream request. The downstream/upstream ratio is different for peer-to-peer systems, since upstream traffic is necessary for uploading files. While any increase in downloading capacity benefits an ISP's subscribers, increased uploading capacity serves both subscribers and non-subscribers.[210] Furthermore, the unpredictability of peer-to-peer usage requires costly adjustments of the network.

C. Peer-to-Peer Central Management

ISPs cannot aggressively fight peer-to-peer. These applications attract new customers to their business. Peer-to-peer is considered to be a "killer application," one of the main attracting features of online access that draws new users, increases use, and therefore increases ISP revenues. Consequently, ISPs must seek technical solutions that will ease the difficulties created by peer-to-peer traffic without driving away that traffic altogether. Blocking peer-to-peer outright or limiting its use across the board are not economically viable options for ISPs; any ISP that implements such a policy is likely to lose market share. Most solutions depend on identifying peer-to-peer applications that run on the system, detecting peer-to-peer traffic and identifying users that make use of these systems.

ISPs are likely to avoid terminating users or disclosing their identities; indeed, ISPs will probably seek to avoid any voluntary actions

208. *See* Goldman, *supra* note 206. This may include ISP access equipment such as routers.

209. *See* P-CUBE, *supra* note 207, at 3.

210. Reducing upstream bandwidth creates significant savings in bandwidth occupied by peer-to-peer programs, and facilitates a more efficient management of ISP network resources. *See, e.g.*, Goldman, *supra* note 206 (describing benefits of new system which cuts peer-to-peer bandwidth use in half).

aimed directly at their own subscribers. Peer-to-peer users are hardly a small, isolated group. Rather, they represent an enormous market of millions of users. It is usually a bad business model to sue one's own customers, but in a competitive environment where users could easily shift to other providers, carrying out such policies would be especially detrimental to the interests of any single provider. Furthermore, identifying individual users and disclosing their identities could be expensive and therefore likely to increase the operating costs of ISPs.[211]

It therefore seems more probable that ISPs will address the challenges of peer-to-peer by shaping their architecture. They are most likely to implement technical measures that would facilitate peer-to-peer central management, as further discussed below.

D. Design and Legal Policy

Holding ISPs liable for peer-to-peer infringement is likely to centralize control mechanisms for managing peer-to-peer traffic. ISPs may have sufficient incentives to increase peer-to-peer management for the purpose of enhancing network efficiency. This may bring the interests of ISPs and copyright owners closer together. ISP interests, for that matter, may also coincide with the enforcement needs of government.

Liability for peer-to-peer traffic is likely to induce ISPs to implement central peer-to-peer management mechanisms in order to minimize their legal exposure.[212] A few systems promise to detect peer-to-peer traffic in the network, through deep-packet inspection.[213] Managing peer-to-peer traffic may also involve caching. Typically, an ISP maintains a cache of peer-to-peer traffic; when a request for a file shared on a peer-to-peer network is received, a router redirects the

211. *See* Gwen Hinze, International Affairs Director, Electronic Frontier Foundation, Briefing Paper: Internet Service Provider Safe Harbors and Expedited Subpoena Process In the U.S. Digital Millennium Copyright Act and Recent Bilateral Free Trade Agreement 9 (June 7, 2005), *available at* http://www.eff.org/IP/FTAA/ISP_june05.pdf.

212. This conclusion also shows why a negligence rule would be radically different from the doctrine of contributory liability as adapted for copyright law in *Sony*. While a negligence rule assumes that if a cost-effective preventive technology is available it must be implemented, *Sony* weighs the effect of liability on non-infringing use of technology. For the view that a negligence rule "is not radically different" than the *Sony* rule, see Lichtman & Landes, *supra* note 173, at 405–06.

213. This type of inspection goes deeper into the communication layer. *See* Goldman, *supra* note 206. An example of such a system is CacheLogic. *See* CacheLogic, The Impact of P2P and the CacheLogic P2P Management Solution, http://www.cachelogic.com/products/resource/Intro_CacheLogic_P2P_Mgmt_Solution_v2.1.pdf.

request to the ISP cache. The system analyzes every peer-to-peer connection to identify attempts to retrieve the file on any of the peer-to-peer networks (*e.g.*, Kaaza, Morpheus, or eDonkey). Before such requests are processed, the system checks for the availability of the file in the cache. Under the current regime such caching may invoke legal liability.

Peer-to-peer central management may come at the cost of shifting from a distributed network architecture to a centralized network that could be more easily governed. Central management of peer-to-peer would then be applied at the level of the architecture, and would not distinguish between legal and non-legal uses of peer-to-peer. Some users of peer-to-peer systems are engaging in non-infringing uses, such as fair use, time or space shifting, or the transmission of public domain material. For ISPs, it would not be cost effective to identify and exempt such users. Peer-to-peer management would have to apply to the system as a whole.

From a social welfare perspective, if we care about peer-to-peer, its central management is an undesirable outcome. As many commentators have noted, decentralized peer-to-peer systems have many advantages, including efficiency, security, and political freedom. The economic advantage of peer-to-peer is in making use of peers' technical resources to facilitate distribution. Nevertheless, even when peer-to-peer distribution is no more efficient than web-based distribution, it may be more stable and secure. For instance, a central server, seeking to address the simultaneous requests of millions of users (who might be seeking information about a newsworthy event), is probably more likely to fail than a peer-to-peer network faced with the same task.

Moreover, a major benefit of peer-to-peer decentralized distribution is its incorporation of individual input into a mass-distribution decision-making process. This distribution mechanism actually allows individuals to make their own decisions about which content to consume, which content to make available and when, and allows this decision-making process to operate on a large scale.[214] The changing structure of cost also affects quality of content: the low cost of distribution allows the distribution of marginal music that attracts only a

214. *See, e.g.*, *Sharing and Stealing*, *supra* note 15, at 11–15. Litman argues that the driving force of the Internet is communication—the desire of people to communicate and share. She challenges the content industry's basic assumption that stronger protection for copyrighted materials would promote the further development of Internet resources. In fact, she argues that what drives the Internet is not mass-produced, copyrighted content. Rather, much content is produced and made available by volunteers; the network then makes it more accessible and easily shared.

small group of fans. This change allows more meaningful participation of individuals in the production of culture, a development which in turn has political ramifications. In this way, peer-to-peer networks facilitate bottom-up participation. They also serve as a guarantee of freedom, since the lack of central control makes decentralized peer-to-peer networks less vulnerable to censorship. Finally, open architecture facilitates innovation by non-market players, as well as the development of subversive technologies that can challenge the existing technological paradigm.

Once the interconnection between the technology and liability rules is acknowledged, lawmakers are called upon to make choices. They must take into account the potential consequences of any legal regime for future technological advancement. Design choices made by ISPs are likely to be affected by liability rules. The law should not seek to govern the development of new technologies, however. Instead, legal policy in the information technology environment should focus on encouraging open architecture that will allow many technologies to flourish. This is especially true for ISPs that provide the infrastructure for online communication.

E. Design and Tax

Some commentators have argued that ISP liability for copyright infringement through file sharing may be justified, since its main result will be an increase in the price of Internet access—an increase sufficient to offset the increase in legal liability. From this perspective, liability is a kind of tax, distributing the harm of infringement on copyright holders among Internet users in general.[215] Proposed alternative schemes for addressing the peer-to-peer copyright crisis have taken the form of actual taxes, levies, or collective mandatory li-

215. *See* Lichtman & Landes, *supra* note 173, at 405.

> After all, instead of trying in vain to distinguish lawful from unlawful activity, a firm in this situation would simply increase its price and use that extra revenue to pay any ultimate damage claims. Legal liability, then, would function like a tax. In many instances such a tax would be welfare reducing in that higher prices discourage legal as well as illegal uses. But in some settings, discouraging both legal and illegal activity would yield a net welfare gain. This would be true where illegal behavior is sufficiently more harmful than legal behavior is beneficial; it would be true where the harms and benefits are comparable but illegal behavior is more sensitive to price; and it would be true where the benefits in terms of increased copyright incentives outweigh the harms associated with discouraging legitimate use.

Id.

censes.[216] For example, copyrighted works could be subject to a compulsory license, which would authorize peer-to-peer distribution while compensating copyright owners through levies on services or equipment that benefit from peer-to-peer traffic.

Liability may have significant financial consequences. It would require ISPs to invest in peer-to-peer management tools, and more importantly, to keep their systems updated against attempts to subvert those tools. If ISPs become actively involved in enforcement efforts, the cost of enforcing copyrights would go down. Some of the cost borne by copyright owners would be shifted to ISPs and distributed among ISP subscribers. The increased cost is likely to be spread among ISP users, thus increasing the cost of Internet access for the entire community of users. Furthermore, unlike a tax, liability is likely to encourage ISPs to engage in more aggressive copyright enforcement efforts, in order to minimize their exposure. The levy option would authorize peer-to-peer usage in return for a fee and would thereby allow the public to take advantage of the opportunities it creates while still compensating rights holders.

The fact that liability may affect design choices makes it significantly different from any of the other suggested regimes. Proposed levies are intended to compensate copyright owners for the loss associated with peer-to-peer exchanges, and at the same time to allow the public to benefit from the use of these systems. ISPs are not likely to respond to liability solely by increasing the prices they charge. They are, instead, likely to redesign their infrastructure and to implement technological measures that would minimize their legal exposure. Consequently, the public may lose many of its opportunities to benefit from the advantages of peer-to-peer.

VI.
CONCLUSION

Safe harbor provisions were a compromise, an attempt to resolve a clash between traditional content industries and the young information industry.[217] ISPs, caught in the midst of copyright wars and fearful of becoming targets in the campaign against piracy, were hoping to

216. *See, e.g.*, Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003); *Sharing and Stealing*, *supra* note 15, at 44; WILLIAM W. FISHER, PROMISES TO KEEP 199–258 (2004).

217. As long as the content industry continues to treat users as merely consumers, rather than as partners who participate in disseminating content, they will view peer-to-peer as a threat. *See Sharing and Stealing*, *supra* note 15, at 50 (arguing that consumer-to-consumer file trading could be economically beneficial to music industry because of opportunity for increased distribution of broader variety of music).

stay neutral and avoid assuming any responsibility as guardians of their community of users.

The content industries, terrified by the way the digital environment threatened to undermine the fundamentals of their business models and facing piracy of unprecedented magnitude, sought to enlist ISPs in their enforcement efforts. The end result was that ISPs were co-opted by copyright owners in copyright enforcement efforts.

Nevertheless, even if the DMCA represented a bargain between the interests of ISPs and copyright holders, it was far from a true social compromise. As this Article has shown, the development of technology is affected by a wide range of market and non-market forces. Network architecture and design may be influenced by the demands of ISPs and copyright owners. Such demands could, in turn, be shaped by liability rules. Market players are also affected by subversive technologies. Such technologies could be introduced by non-market players, including individual developers and peers collaborating in online communities. Market players must respond technologically to these challenges.

Peer-to-peer technology, which was first introduced by non-market players, confronted ISPs with a dilemma: it boosted their business, increasing the demand for broadband access and upgraded services, but at the same time required them to deal with the burden of increasing bandwidth consumption. It is very difficult for any single ISP to forego the peer-to-peer market entirely, since to do so might well mean losing market share. On the other hand, the excessive consumption of bandwidth by peer-to-peer applications shifts the cost of communication from the server level to the ISP network to a degree many ISPs would find intolerable.[218] The ISPs' interests may therefore tilt in favor of finding new technical solutions, including central management of peer-to-peer networks, which would turn peer-to-peer into a giant broadcast system provided and controlled by ISPs. In this regard, ISPs, copyright holders, and, for that matter, law enforcement agencies, may share interests.

The public interest, however, requires an open infrastructure. If we care about peer-to-peer as a guarantee of open technological markets and a promoter of political change, then the issue of ISP liability should not follow the DMCA legislative process and should not be left to private bargaining between copyright owners and ISPs. There are

218. Rather than investing in strong servers that can meet the demand of many users for the same file, each user can act as a server. Consequently, ISPs must support high bandwidth capacity for both uploads and downloads for every user.

many reasons, going far beyond their immediate interests, why ISPs should be exempted from copyright liability for peer-to-peer infringement. There is, in particular, a substantial public interest in promoting free speech and innovation and in protecting user privacy and anonymity.

Now that the piracy agenda is taking over, however, the lack of discussion on why ISPs should be exempted from liability has become even more notable. The decisions in *Verizon* and *Charter* called for a new balancing of party interests in the peer-to-peer environment. This Article suggests that, in designing the new liability rules, policymakers should take into account the interconnection between liability and design, and should make sure that design remains open to new, subversive technologies. This openness is the key to preserving innovation and guaranteeing open markets and freedom.