Physical World Assumptions and Software World Realities (and Why There are More P2P Software Providers than Ever Before)

Rebecca Giblin*

Abstract. *Rights holders have been successful in every major copyright action brought against peer-to-peer (P2P) software providers. By 2005, those behind Napster, Aimster, Grokster, Morpheus and Kazaa have each been held liable for their users' infringements and effectively exited the market. But those successes did not result in any reduction in the availability of P2P file sharing software. In fact, the opposite occurred: soon after the U.S. Supreme Court ruled in favor of rights holders in* Grokster*, there was exponential growth in the number of P2P file sharing applications available. This Article argues that this came about because the pre-P2P and current U.S. secondary liability laws were and are based on a number of physical world assumptions that are simply not tenable in the software context. After identifying those assumptions, and contrasting them with the relevant software world realities, the Article demonstrates that the explosion in the number and availability of P2P apps can be traced directly to the Supreme Court's failure to recognize the mismatch between the two paradigms.*

* Dr. Rebecca Giblin was the Kernochan Center Visiting International Intellectual Property Scholar at Columbia Law School while preparing this article, and is a faculty member at Monash University, Australia. Particular thanks are owed to Professors Jane Ginsburg and Mark Davison for their many generous hours reading previous drafts and discussing the ideas explored in this Article. Giblin is also grateful to Professors Rochelle Dreyfuss, Jacqueline Lipton, Sam Ricketson, Peter Jaszi and Melissa de Zwart, as well as Professor Alfred Yen and the other participants of the 2008 Works-in-Progress Intellectual Property Colloquium, for their contributions in reading and/or commenting on the source material for this work. This Article is drawn from the author's monograph, *Code Wars: 10 Years of P2P Software Litigation* (December 2011) (unpublished manuscript) (on file with the author), which chronicles the decade-long struggle between rights holders and P2P software providers, tracing the development of the fledgling technologies, the attempts to crush them through litigation and legislation, and the remarkable ways in which they evolved as their programmers sought ever more ingenious means to remain one step ahead of the law. Please refer to the book for fuller analysis of the issues, theories and cases discussed within the Article, and for discussion about what comes next in the continuing battle against P2P-facilitated infringement. This Article was double-blind reviewed by an expert in the field in accordance with the Australian Department of Innovation, Industry, Science and Research peer review requirements.

INTRODUCTION: A UNIQUE VULNERABILITY TO ANTIREGULATORY CODE

When the advent of P2P file sharing technologies in the late 1990s brought about a torrent of infringement, rights holders responded in the same way they always had: by targeting the intermediaries that provided the infringement-enabling technologies.[1] Suing gatekeepers has long been the orthodox legal response in situations where enforcement against individuals will predictably be ineffective, and this was a textbook example.[2] The number of participating infringers was so high, pursuing them so costly, and the chances of their being apprehended so remote, that the threat of direct infringement—even with the possibility of astronomical penalties—left individual infringers largely unmoved.[3]

As Professor Tim Wu has pointed out, until recently, copyright law was "entirely dependent on gatekeeper enforcement"—the gatekeepers being the publishers, manufacturers and others that were "capable of copying and distributing works on a mass scale."[4] Traditionally, rights holders had considerable success in using legal doctrines based on these principles of gatekeeper enforcement to shut down activities that facilitated copyright infringement.[5] Such activities ranged from swap meets whose proprietors tacitly permitted vendors to sell infringing records, to dance halls whose operators failed to secure licenses allowing visiting bands to perform copyrighted music, to advertising agencies that created campaigns for purveyors of "suspiciously" cheap records.[6] Such enforcement efforts were also

1. Regarding this history of pursuing intermediaries for third party infringement, *see, e.g.*, Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417 (1984); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999). *See also Univ. of New South Wales v Moorhouse* [1975] 133 CLR 1 (Austl.); CCH Canadian Ltd. v. Law Soc'y of Upper Canada, [2004] S.C.R. 339 (Can.); CBS Songs Ltd. v. Amstrad Consumer Electronics Plc. [1988] A.C. 1013 (H.L.) (U.K.).

2. *See* Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 56–57 (1986). For an excellent discussion of the theory behind indirect liability from an economist's perspective, *see also* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006).

3. *See* David Lindsay, *Internet Intermediary Liability: A Comparative Analysis in the Context of the Digital Agenda Reforms*, (24)1&2 COPYRIGHT REP. 70, 73 (2006) ("As pursuing individual infringers is costly, questions ar[i]se regarding the liability of intermediaries that are not involved with the publication of material, but that participate in the communication, location or storage of material."); Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the DMCA's Anti-Device Provisions*, 19 HARV. J.L. & TECH. 111, 156 (2005) (arguing that rights holders pursue secondary infringers "[b]ecause of the economic reality of pursuing direct infringers"); Alfred C. Yen, *Third-Party Copyright Liability After Grokster*, 91 MINN. L. REV. 184, 186 (2006–2007) ("The normal remedy for copyright infringement is litigation against infringers. However, the number of computer-based infringers is so large that copyright holders cannot find and sue them all.").

4. Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 712 (2003).

5. *See, e.g.*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996); Dreamland Ball Room v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929); Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 399 (S.D.N.Y. 1966).

6. *See Fonovisa*, 76 F.3d 259; *Dreamland Ball Room*, 36 F.2d 354; *Screen Gems-Columbia Music*, 256 F. Supp. 399.

successful in deterring many future market entrants from engaging in the kind of conduct that had previously resulted in liability, and thus further limiting eventual third party infringement.[7] When they commenced their ten-year struggle to apply the same principles to P2P software providers, rights holders undoubtedly expected to achieve the same outcome. But things did not go according to plan. Although they prevailed in every major court action instituted against P2P providers, software developers remained unfazed. By 2007, more software programs facilitating P2P file sharing were available than ever before.[8] The average number of users sharing files on P2P file sharing networks at any one time was nudging 10 million, and it was estimated that P2P traffic had grown to comprise up to ninety percent of all global Internet traffic.[9] At that point, rights holders tacitly admitted defeat. Abandoning their long-held strategy of suing key P2P software providers, they closed the P2P software litigation chapter and diverted enforcement resources to other areas, particularly global efforts to persuade or compel Internet service providers to police infringing users.[10]

To understand why those lengthy, expensive and ultimately successful efforts to shut down individual P2P file sharing technologies had little or no impact on the availability of file sharing software, it is necessary to understand something about the unique properties of software code. For many years now it has been recognized that code can have regulatory effects—or, as Professor Lawrence Lessig famously put it, "code is law."[11] As he explains, "[t]he software and hardware that make

7. *See* Thomas Hays, *The Evolution and Decentralisation of Secondary Liability for Infringements of Copyright-Protected Works: Part 1*, 28(12) EUR. INTELL. PROP. REV. 617, 617 (2006) (describing the way in which predigital era "[s]econdary infringements . . . were, for the most part, crude, marginal transactions, the subjects of swap meets and unlicensed kiosks").

8. There are no reliable statistics regarding the number of applications available from Napster onwards, but the post-*Grokster* upward trajectory in the number of P2P applications under development is evidenced by data from the SourceForge open source software repository at different points in time. On October 24th, 2007, a little more than two years after the *Grokster* decision was handed down, the site hosted some 2,180 projects in its "file sharing" category. By December 23rd of the following year, that number grew to 3,502. SOURCEFORGE, http://www.sourceforge.net (last visited Nov. 7, 2011).

9. *See* Eric Bangeman, *P2P Traffic Shifts Away from Music, Towards Movies*, ARS TECHNICA (July 6, 2007), http://arstechnica.com/tech-policy/news/2007/07/p2p-traffic-shifts-away-from-music-towards-movies.ars [hereinafter Bangeman, *P2P Traffic Shifts Away from Music*]. *See also* Eric Bangeman, *P2P Responsible for as Much as 90 Percent of All 'Net Traffic*, ARS TECHNICA (Sept. 3, 2007), http://arstechnica.com/old/content/2007/09/p2p-responsible-for-as-much-as-90-percent-of-all-net-traffic.ars.

10. *See* Alain Strowel, *The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringements?*, *in* COPYRIGHT ENFORCEMENT AND THE INTERNET 147 (Irini A. Stamatoudi ed., 2010); Peter K. Yu, *The Graduated Response*, 61 FLA. L. REV. 1373 (2010); Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009) (giving a detailed analysis of this trend across a variety of jurisdictions).

11. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999). Those famous words were first enunciated by architecture and media professor William J. Mitchell, who, in the context of explaining the significance of cyberspace, wrote that "[o]ut there on the electronic frontier, code is the law." WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN 111 (1995). For more on this idea that code regulates, *see* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 201 (1997) (predicting—two years before Napster was

cyberspace what it is constitute a set of constraints on how you can behave."[12] For example, software code may regulate behavior by imposing a password requirement on users seeking to gain access to a particular service.[13] Historically, rights holders have used a variety of code-based measures as part of their efforts to promote compliance among end users, with the most notable example being Sony's disastrous rootkit experiment.[14] In the P2P file sharing context, however, the idea that code regulates is less significant than the separate but related idea that code can be antiregulatory in effect. As Wu explains, "the reason [why] code matters for law at all is its capability to define behavior on a mass scale. This capability can mean constraints on behavior, in which case code regulates, but it can also mean shaping behavior into legally advantageous forms."[15] Wu analogizes such antiregulatory programmers to tax lawyers. "[They look] for loopholes or ambiguities in the operation of law (or, sometimes, ethics). More precisely, [they look] for places where the stated goals of the law are different than its self-defined or practical limits. The designer then redesigns behavior to exploit the legal weakness."[16]

As will become clear, post-Napster P2P developers engaged in precisely this kind of behavior, routinely seeking to code their software in ways that sidestepped the limits of the existing law whilst nonetheless facilitating vast amounts of infringement.[17] Those behind the Grokster and Morpheus file sharing applications were so successful in coding their way around the existing law that the U.S. Supreme Court had to recognize a new theory of liability to defeat them.[18] Such technologies highlighted the copyright law's peculiar vulnerability to attack by antiregulatory code. However, the reasons for that vulnerability remain largely unexplored. The best effort to do so comes from Wu's groundbreaking article

developed—that "there will be a continuing technological struggle between content providers, their customers, their competitors, and future creators"); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, U. CHI. LEGAL F. 335, 335–43 (1996) (exploring the role of software in structuring the online environment); Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 320 (2005) (canvassing a number of different ways in which code can be and is in fact used to regulate behavior); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896–97 (1996) (exploring the idea that software can constrain or "regulate" behavior) [hereinafter Lessig, *Reading the Constitution in Cyberspace*]; Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 568–74 (1998) (arguing that technology is a source of rulemaking separate from traditional law, and analogizing features of the "lex informatica" to traditional legal regulation); R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457 (2005) (elaborating on the code/law relationship, particularly the substitutability of code and law).

12. LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, *supra* note 11, at 89.

13. *Id.*

14. *See, e.g.*, Robert McMillan, *Sony Rootkit Settlement with States Reaches $5.75M*, INFOWORLD (Dec. 21, 2006), http://www.infoworld.com/d/security-central/sony-rootkit-settlement-states-reaches-575m-558.

15. Wu, *When Code Isn't Law*, *supra* note 4, at 707–08.

16. *Id.* at 708.

17. *See infra* pp. 78–95.

18. There is some controversy as to whether that theory was in fact new, or simply an addition to an existing theory. *See* Rebecca Giblin, Code Wars: 10 Years of P2P Software Litigation 89–91 (Dec. 31, 2011) (unpublished manuscript) (on file with author).

When Code Isn't Law, in which he identifies two bases for it.[19] The first is the law's longstanding reliance on gatekeeper enforcement mechanisms, mentioned above.[20] Gatekeeper enforcement schemes are premised on the idea that relatively few people are capable of widespread copying and distribution.[21] Thus, as Wu explains, they "have an obvious weakness: [t]hey depend on a specialized good or service remaining specialized."[22] P2P file sharing technologies subvert that assumption by placing the ability to efficiently and cheaply distribute books, movies, music and other content in the hands of individual consumers. The second reason is the dearth of normative support for the law from individual users.[23] Wu's reasoning on this point is based on empirical studies that suggest that individual end users have a widely held belief that copying copyrighted material for a friend is acceptable, whereas selling it on a commercial basis is not.[24] Wu argues that P2P file sharing applications "brilliantly" exploit this distinction between commercial and noncommercial copying:

> P2P clients create no sensation or impression of stealing . . . . Instead, the user is invited to a "community" of peers who exchange song files. A user, importantly, has no sense that she is "selling" copyrighted materials. The design therefore exploits the distinction between the acceptance of noncommercial copying and the nonacceptance of commercial copying. While the economic consequences of peer filesharing could be large, the superficial absence of commercial exchange makes filesharing more acceptable under the norms of home copying.[25]

Thus, by eliminating gatekeepers, and by exploiting the fact that many individuals do not have any ethical problem with "sharing" content with others online, Wu argued that P2P software providers have sometimes managed to avoid the law's traditional enforcement measures.[26]

This Article posits that there is also a third reason for that vulnerability: one that explains not only why the pre-P2P secondary liability law proved so peculiarly unsuited to the task of dealing with purveyors of antiregulatory code but also why even successful litigation against P2P software providers failed to curb its spread. It is premised on the idea that software is radically and fundamentally different from physical world technologies. The U.S. pre-P2P secondary liability law evolved from decades of decisions relating almost exclusively to physical world scenarios and technologies.[27] Necessarily, the resulting principles were based on

19. Wu, *When Code Isn't Law*, *supra* note 4.
20. *Id.* at 683.
21. *Id.* at 683, 685.
22. *Id.* at 716.
23. *Id.* at 683.
24. *Id.* at 724.
25. *Id.* at 724–25.
26. *Id.* at 685, 716–17, 722–26.
27. *See,* e.g., Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Kalem Co. v. Harper Bros., 222 U.S. 55 (1911); Fonovisa, Inc. v. Cherry Auction Inc., 76 F.3d 259 (9th Cir. 1996); Gershwin Pub. Corp. v. Columbia Artists Mgmt. Inc., 443 F.2d 1159 (2d Cir. 1971); Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304 (2d Cir. 1963); RCA Mfg. Co. v. Whiteman, 114 F.2d 86 (2d

certain assumptions that had long proved correct in the physical world paradigm. But there is a gap between those physical world assumptions and the realities of P2P software development, which this Article dubs the physical world/software world divide. With reference to it, this Article presents a new theory that explains why, despite being ultimately successful in holding individual P2P software providers liable for their users' infringement, the litigation strategy failed to bring about any meaningful reduction in the amount of P2P development and infringement.

It will do so over the following four parts. Part I begins by identifying four physical world assumptions on which pre-P2P secondary liability law was implicitly based. Part II introduces the secondary liability law, and highlights the ways in which secondary liability law manifests those assumptions. Part III outlines the way in which the law evolved as it was applied to P2P software providers. Finally, Part IV demonstrates that the subsequent explosive growth in the number and variety of P2P software applications available was a direct consequence of the secondary liability law's failure to recognize its own underlying physical world assumptions, and the ways in which software world realities depart from them.

I. PHYSICAL WORLD ASSUMPTIONS

Since the theory underlying this Article focuses its inquiry on the characteristics of software code that make software code different and unique as compared to physical world equivalents, it is necessary to conceptually separate software from hardware. Software refers to the "programs and other operating information used by a computer," while hardware is the physical equipment necessary to execute software's commands.[28] The definition of "code" adopted in the existing legal literature typically conflates the two by defining "code" as the "information technology architecture," or "the hardware and software," that constitutes a particular technology.[29] It is easy for these lines to become blurred, since software is increasingly incorporated into much of the hardware we use in day to day life (including our MP3 players, personal video recorders, cars, microwave ovens and more). However, it is necessary to separate them in this context, since the equation of hardware and software risks masking the unique characteristics of software code on its own account, and particularly the ways in which it differs from the physical world technologies that came before it.

Cir. 1940); Dreamland Ball Room v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929); Polygram Int'l Pub. Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314 (D. Mass. 1994); Harper v. Shoppel, 26 F. 519 (C.C.S.D.N.Y. 1886).

28. *Software Definition*, THE NEW OXFORD AMERICAN DICTIONARY 1612 (Erin McKean ed., 2d ed. 2005).

29. *See, e.g.*, EGBERT DOMMERING & LODEWIJK ASSCHER, CODING REGULATION 2 (2006); LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, *supra* note 11, at 6; Kesan & Shah, *supra* note 11, at 320. *But cf.* Lessig, *Reading the Constitution in Cyberspace*, *supra* note 11, at 896.

A. EVERYBODY IS BOUND BY PHYSICAL WORLD RULES

This first assumption that everyone is bound by the rules of the physical world underlies much of pre-P2P secondary liability law, and is the most abstract and poorly understood of the four. Understanding it requires delving into some of the conceptual differences between software worlds and physical worlds. Consider what we know about the physical space we occupy. We have an immediate and intuitive understanding about how it works.[30] "Apples, when released fall down, not up. Actions are causally related to consequences. We expect things to behave sensibly. Our intuitive notion of what is 'sensible' is based on common-sense experiences, learned from earliest childhood, and rooted in the physical world."[31] As M. Ethan Katsh explains:

> In the "real world," time and space are ever-present constraints, with the laws of physics frequently limiting many of our desires to do something or be somewhere. The list of constraints to which we accommodate ourselves is significant. We respect the laws of gravity. We understand that no more than one object can occupy the same place. We recognize that we can only be in one place at one time and that there are some places we cannot go to because there is not enough time or because they are too far away.[32]

What is less well understood is that physical world rules do not necessarily apply to software. In fact, neither the laws of physics nor any other law or principle known in the physical world has any application in the virtual context.[33] In the words of Professor Joseph Weizenbaum:

> There is a distinction between physically embodied machines, whose ultimate function is to transduce energy or deliver power, and abstract machines. i.e., [sic] machines that exist only as ideas. The laws which the former embody must be a subset of the laws that govern the real world. The laws that govern the behavior of abstract machines are not necessarily so constrained. One may, for example, design an abstract machine whose internal signals are propagated among its components at speeds greater than the speed of light, in clear violation of physical law.[34]

Unbound by physical world rules, software code is incredibly malleable.

30. Boris Beizer, *Software is Different*, *in* 10 ANNALS OF SOFTWARE ENGINEERING 293, 295 (Dilip Patel & Yingxu Wang eds., 2000).

31. *Id.*

32. Katsh, *supra* note 11, at 341–42.

33. *See* JOSEPH WEIZENBAUM, COMPUTER POWER AND HUMAN REASON 111 (1976). *See also* Beizer, *supra* note 30, at 296; Alan M. Davis, *Fifteen Principles of Software Engineering*, 111(6) IEEE SOFTWARE 94, 94 (1994); William Greubel, *A Comedy of Errors: Defining "Component" in a Global Information Technology Market—Accounting for Innovation by Penalizing the Innovators*, 24 J. MARSHALL J. COMPUTER & INFO. L. 507 (2006); Juris Hartmanis, *Turing Award Lecture: On Computational Complexity and the Nature of Computer Science*, 37(10) COMM. OF THE ACM 37, 39 (1994); Katsh, *supra* note 11, at 341–42; Yingxu Wang, *Keynote Lecture: On the Informatics Laws of Software*, PROC. OF THE FIRST IEEE INT'L CONF. ON COGNITIVE INFORMATICS, 132 (regarding the idea that software is not bound by physical laws).

34. WEIZENBAUM, *supra* note 33, at 111.

Indeed, Professor James Moor identified "logical malleability" as software code's revolutionary characteristic.[35] The medium's inherent freedom and flexibility led Weizenbaum in 1976 to famously describe computer programmers as creators of "universes of virtually unlimited complexity."[36] That unrestrained capability can, of course, be reined in by other code: as Lessig explains, "[d]ifferent code makes differently regulable networks. Regulability is thus a function of design."[37] However, the Internet was deliberately designed to be as free and open as possible for future developers and, as a result, developers of Internet-based P2P file sharing programs face very few code-based constraints.[38] All of this means that entities in a software world "can be made . . . to overlap, interconnect, and interact in ways that are not possible or feasible in the physical world."[39] Thus programmers can write software with functionality that is unrestrained by the physical world's limitations.

Copyright law evolved in response to decades of litigation involving physical world scenarios and technologies. The intuitive and unacknowledged understanding that we all have of the physical world's constraints has inevitably played a large role in informing the law's response to those scenarios. There can be no doubt that judges must sometimes have been influenced by unspoken and unacknowledged assumptions that if certain things were infeasible, impossible or impractical in the physical world, they were infeasible, impossible or impractical *full stop*. Since these assumptions held in the physical world context, the secondary liability law worked well for a long period of time, and secondary infringements were limited—being "for the most part, crude, marginal transactions, the subjects of swap meets and unlicensed kiosks."[40] But as the P2P software cases demonstrate over and over again, secondary liability principles based on the assumption that physical world rules apply can result in unanticipated outcomes when applied to situations where they simply do not.[41] For example, a law that implicitly assumes that knowledge of a wrongdoing will be a natural corollary of a defendant's culpability may struggle to respond to a defendant that utilizes encryption software to eliminate such knowledge. This might be the kind of

35. James H. Moor, *What is Computer Ethics?*,16(4) METAPHILOSOPHY 266, 269 (1985).

36. WEIZENBAUM, *supra* note 33, at 115.

37. LAWRENCE LESSIG, CODE VERSION 2.0 34 (2006).

38. *See* STUART BIEGEL, BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 187–211 (2001) (providing an analysis of the effects changes to the code or architecture of the Internet may have); STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 40–49 (1994) (providing further information on the philosophies of the Internet's creators); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815 (2004) (providing a detailed explanation of the way in which the Internet is coded, and why that structure allows free development of new protocols such as those needed for P2P file sharing); Barry M. Leiner et. al., *A Brief History of the Internet*, INTERNET SOCIETY, http://www.isoc.org/internet/history/brief.shtml (last visited Nov. 11, 2011) (providing a history of the way in which the Internet was developed).

39. Katsh, *supra* note 11, at 339.

40. Hays, *supra* note 7, at 617.

41. *See infra* pp. 78–95, 112–117.

phenomenon that Mitchell Kapor and John Perry Barlow were hinting at when they observed in 1990 that "the old concepts of property, expression, identity, movement, and context, based as they are on physical manifestation, do not apply succinctly in a world where there can be none."[42]

B. DEVELOPING AND DISTRIBUTING DISTRIBUTION PRODUCTS IS EXPENSIVE

The final three assumptions identified in this work are less abstract, and build upon one another. The first relates to cost. As Professor Jessica Litman has observed, "[o]ur copyright law was designed in an era in which mass distribution of copies of works required a significant capital investment."[43] There can be no doubt that the creation of physical world distribution technologies capable of vast amounts of infringement, such as printing presses, photocopiers, and VCRs, typically requires large investments in research, development and infrastructure.[44] Even if the initial invention of a physical world distribution technology is achieved cheaply—and history is filled with examples of hobbyist inventors on shoestring budgets making amazing breakthroughs—developing it for marketing, mass manufacturing, promotion and delivery all require considerable amounts of cash. [45]

The sizeable investment long inherent in the development, manufacture and delivery of physical distribution technologies created high barriers to market entry that limited the number of manufacturers to relatively few—something that has long made it easier for content owners to enforce their rights against secondary infringers.[46] One of the reasons that the copyright law evolved to rely on gatekeeper enforcement measures, as outlined above, was because these factors prevented end users from participating in widespread dissemination of copyrighted works. As Professor Jane Ginsburg explains:

> Copyright owners have traditionally avoided targeting end users of copyrighted works. This is in part because pursuing the ultimate consumer is costly and unpopular. But the primary reason has been because end users did not copy works of authorship—or if they did copy, the reproduction was insignificant and rarely the subject of widespread further dissemination. Rather, the entities creating and disseminating copies (or public performances or displays) were intermediaries between the creators and the consumers: for example, publishers, motion picture producers, and producers of phonograms. Infringements, rather than being spread throughout the user population, were concentrated higher up the chain of distribution of works. Pursuing the intermediary therefore offered the most effective way to enforce copyright interests.[47]

42. Mitchell Kapor & John Perry Barlow, *Across the Electronic Frontier*, ELECTRONIC FRONTIER FOUNDATION (July 10, 1990), http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/eff.html.

43. Jessica Litman, *The Copyright Revision Act of 2026*, 13 MARQ. INTELL. PROP. L. REV. 249, 253 (2009).

44. Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 255 (2006).

45. *See generally* TIM WU, THE MASTER SWITCH (2011) (providing many such examples).

46. Zittrain, *supra* note 44, at 255.

47. Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters,*

A further corollary to the large investment necessary to create such technologies is that their providers are likely to be easily identifiable and deep-pocketed, making them attractive defendants in the event they step out of line.

C. DISTRIBUTION TECHNOLOGIES ARE DEVELOPED FOR PROFIT

The third physical world assumption is that distribution technologies are developed for profit. As Professor Jonathan Zittrain has observed, "[b]efore the advent of modems and networks, major physical-world infringers typically needed a business model because mass scale copyright infringements required substantial investment in copying and distribution infrastructure."[48] Thus the assumption that developers of distribution technologies would do so for profit was inextricably tied to the large investments that were considered to be an integral part of developing and distributing it in the first place: once that initial investment had been made, there was strong motivation to obtain some financial return. This traditional need to make a massive investment and then to recoup those expenses has significant implications. As Paul Ganley has explained:

> The normal phases of R&D, product design, manufacture, unit testing and distribution all help to constrain the wilder excesses of copyright infringing potential. The inherent checks and balances in the structure of legitimate businesses help to ensure that companies will shy away from such costly and time consuming exercises if they believe there is no legitimate avenue for them to recoup their substantial investment.[49]

This assumption was reflected in various theories of secondary liability for copyright infringement. It is most explicit in the vicarious liability doctrine, of which one element is a "direct financial interest" in the infringement.[50] However, the imposition of contributory liability has also often appeared to be inspired largely by the profit motives of the defendants.[51]

Once again, this assumption worked to keep the total number of providers relatively small. It also probably helped to keep them in line. Few providers were likely to skirt the edges of the law too closely, since litigation by aggrieved rights holders would cut dramatically into their anticipated profits.

---

and Copyright in Cyberspace, 95 COLUM. L. REV. 1466, 1488 (1995).

48. Zittrain, *supra* note 44, at 255.

49. Paul Ganley, *Surviving Grokster: Innovation and the Future of Peer-to-Peer*, 28(1) EUR. INTELL. PROP. REV. 15, 22 (2006).

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

51. For example, in *Gershwin Publishing Corp. v. Columbia Artists Management Inc.*, the case in which the modern contributory infringement framework was developed, the Court's finding of liability seemed influenced by the fact that the defendant had significantly profited from the infringing concerts, although profit was not, strictly speaking, an element of the tort. *See* 443 F.2d at 1162. Similarly, in *Fonovisa Inc., v. Cherry Auction Inc*, it seems that the Court was influenced by the fact that Cherry Auction was profiting from the increased revenue that resulted from the infringement. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

D. RATIONAL DEVELOPERS OF DISTRIBUTION TECHNOLOGIES WILL NOT SHARE THEIR SECRETS WITH THEIR CONSUMERS OR THEIR COMPETITORS

The final relevant assumption is that providers of distribution technologies are unwilling to share the secrets of their inventions. This follows closely from the assumption that distribution technologies are expensive to develop. Having spent money to research, develop, manufacture and distribute a technology, the provider has no incentive to share that technology with its competitors. This is another reason why the gatekeeper enforcement regime worked so well before software-based distribution technologies emerged. The disinclination to allow technologies to be copied helped further limit the number of technology providers, and enabled gatekeeper-based laws to effectively keep them under control.

The following Part highlights the way in which these physical world assumptions manifest in the pre-P2P secondary liability law. The subsequent sections then trace the ways in which the failure of courts to recognize these assumptions—and how software world realities could depart from them—led directly to an upsurge in the number of P2P file sharing applications under development.

II. THE PRE-P2P LAW

The pre-P2P U.S. copyright law imposed secondary liability on a defendant in accordance with two common law doctrines—contributory and vicarious infringement. Secondary liability can only accrue after some primary infringement has occurred.[52] Though the two doctrines have historically sometimes been combined and confused, they are now accepted as being wholly independent.[53] As will be seen, both doctrines evolved almost exclusively with reference to physical world technologies and scenarios.

A. VICARIOUS LIABILITY

Vicarious liability for copyright infringement developed from *respondeat superior*, a legal doctrine concerned with the liability of employers for the torts of

52. *See, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 929 (2005).

53. *See, e.g.*, Universal City Studios, Inc. v. Nintendo Co., 615 F. Supp. 838, 857 (S.D.N.Y. 1985) (finding that vicarious liability is "established if it is shown that a party, with knowledge of infringing activity, induces, causes, or materially contributes to the infringing conduct of another"). The definition applied in *Universal City Studios* actually refers to the separate doctrine of contributory infringement; in contrast, vicarious liability has no knowledge element. *See also* Telerate Sys., Inc. v. Caro, 689 F. Supp. 221, 227–28, n.8 (S.D.N.Y. 1988) (suggesting that in "the intellectual property context," vicarious and contributory liability are interchangeable); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261–64 (9th Cir. 1996); Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971). A standard combining elements of both contributory and vicarious liability has been proposed and emphatically rejected. *See* Demetriades v. Kaufmann, 690 F. Supp. 289, 294 (S.D.N.Y. 1988). *But see, e.g.*, *Grokster*, 545 U.S. at 930 (demonstrating that the doctrines are now accepted as being independent).

their employees.[54] Its roots lie in the tort theory of enterprise liability, which posits that enterprises should internalize losses that are caused by their existence as a cost of doing business, under the rationale that businesses that cause losses ought to be responsible for their rectification.[55] This encourages risk creators to guard against losses, and, if they occur anyway, to provide compensation to victims and spread the cost of doing so amongst those who have benefited from the risk-creating activity.[56] The modern formulation of vicarious liability for copyright infringement evolved from two distinct lines of authority: the so called "dance hall" cases, which held music venue proprietors liable where they financially profited from infringements committed by independent musicians at their premises, and the "landlord" cases, in which defendants avoided liability as long as they had no real financial interest in that infringement or ability to prevent it from occurring.[57] These parallel lines of authority were unified in 1963 by the Second Circuit in *Shapiro, Bernstein & Co. v. H.L. Green Co*.[58] Since then, vicarious liability has been accepted as accruing whenever "the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials."[59]

Several physical world assumptions are inherent in this formulation of vicarious infringement. Firstly, the doctrine is heavily premised on the assumption that everybody is bound by physical world rules. As outlined above, the intuitive and unacknowledged understanding that we have of the physical world's constraints obviously informed the law's response to earlier cases. If certain things were infeasible, impossible or impractical in the physical world, it was assumed—probably without any explicit thought being given to the matter at all—that they would be infeasible, impossible or impractical full stop. In the vicarious liability context, this is manifested particularly clearly in the doctrine's treatment of control. Decades of physical world precedent in the vicarious liability context suggested that persons who culpably facilitated a third party's infringement would generally have some control over that infringement. In physical world scenarios, such as

54. *Fonovisa*, 76 F.3d at 261–62.

55. *Compare* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1843 (2000) [hereinafter Yen, *Internet Service Provider Liability*], *with* MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A][3] (2009) (arguing that contributory liability is based on enterprise liability—"A separate avenue for third-party liability in the copyright sphere is contributory infringement, which forms an outgrowth of the tort concept of enterprise liability"). However, the theory of enterprise liability does not seem to justify or support contributory liability, which is concerned with knowledge of, and participation in, the third party infringement. Instead, it is concerned with holding liable those that are best able to prevent losses regardless of their knowledge. In these circumstances, Professor Yen's opinion should be preferred. *See generally* Gregory C. Keating, *The Theory of Enterprise Liability and Common Law Strict Liability*, 54 VAND. L. REV. 1285, 1286 (2001) (providing a more detailed examination of enterprise liability).

56. Yen, *Internet Service Provider Liability*, *supra* note 55, at 1843, 1846.

57. *See, e.g.*, Deutsch v. Arnold, 98 F.2d 686 (2d Cir. 1938); Dreamland Ball Room v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929).

58. Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963).

59. *Id.* at 307.

where a swap meet organizer rents stalls to infringers, or where a department store owner leases space where bootleg records are sold, control flows naturally from the parties' involvement, and it is often difficult to imagine how it could be eliminated without considerable loss of efficiency or profit.[60] Accordingly, the law evolved to require some degree of control over third party infringement before liability would attach. Since most facilitators of infringement could not practicably eliminate control in the physical world context, this worked well as a mechanism for identifying wrongdoers.

Vicarious liability's modern formulation is also implicitly premised on two other physical world assumptions: the related ideas that developing, manufacturing and disseminating distribution products to market is expensive, and that distribution technologies that facilitate widespread infringement are developed for profit. These assumptions flow from one another: If it is expensive to develop a distribution technology, then it makes sense to assume that it will not be developed unless there is a reasonable prospect of recouping that initial investment. These assumptions are apparent in the second element of the doctrine, which requires there to be a direct financial interest in the third party infringement in order for liability to accrue.[61] This was part thought to be a suitable indicator of liability, since, as discussed in the previous Part, anybody who had invested the time and money necessary to facilitate any significant amount of infringement was assumed to be seeking some profit in return. The corollary was that anybody who was facilitating infringement without the anticipation of any financial profit was such a small fry as to not be worth pursuing.

B. CONTRIBUTORY LIABILITY

The second doctrine in American law's pre-P2P secondary liability toolkit was contributory liability, which has its roots in a fundamental common law principle known as joint tortfeasor liability.[62] Direct or indirect intellectual property infringement constitutes a tort, and joint tortfeasor liability provides that one who knowingly participates in or furthers a tort is jointly and severally liable with the primary tortfeasor.[63] In contrast to vicarious liability, which is concerned with relationships, contributory liability emphasizes fault.[64] Its basis is the idea "that one who directly contributes to another's infringement should be held accountable."[65] That origin dictates the focus of the doctrine. It is intended to

60. *See Fonovisa*, 76 F.3d 259; *Shapiro, Bernstein & Co*, 316 F.2d 304.

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

62. *See, e.g.*, Harper v. Shoppel, 26 F. 519 (C.C.S.D.N.Y. 1886) (one of the earliest cases to apply principles of joint tortfeasorship to copyright infringement).

63. Jane C. Ginsburg & Sam Ricketson, *Inducers and Authorisers: A Comparison of the U.S. Supreme Court's Grokster Decision and the Australian Federal Court's KaZaa Ruling*, 11(1) MEDIA & ARTS L. REV. 1, 2 (2006); Alfred C. Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-To-Peer*, 55 CASE W. RES. L. REV. 815, 826 (2005) [hereinafter Yen, *Sony*]. *See also* Screen Gems-Columbia Music, Inc., v. Mark-Fi Records, Inc., 256 F. Supp. 399, 403 (S.D.N.Y. 1966).

64. Alfred C. Yen, *Third-Party Copyright Liability After Grokster*, *supra* note 3, at 195.

65. *Fonovisa*, 76 F.3d at 264.

capture those who are significantly involved in copyright infringement—who have "acted in concert" with the primary infringer—in situations where that conduct technically falls outside the definition of direct infringement.[66]

Contributory liability was given life independent of its joint tortfeasorship origins in the landmark decision of *Gershwin Publishing Corp. v. Columbia Artists Management Inc*.[67] In that case, the Second Circuit held that contributory liability exists where "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another."[68] Knowledge may be actual or constructive, but should precede the infringing activity.[69] Timely knowledge of third party infringement is not sufficient in itself for liability to accrue: the defendant must also have "induced, caused, or materially contributed" to that infringement.[70] While the issue of liability for "inducing" infringement would eventually assume tremendous significance in the P2P context, pre-P2P contributory liability authorities paid scant attention to what it meant to "induce."[71] Instead, they focused primarily on the concept of "material contribution," and in so doing divided relevant acts of assistance into two broad categories.[72] The first covered situations where a company or individual had directly participated in the third party's infringement, for example through the provision of labor.[73] The second encompassed situations where the defendant's contribution to the infringement was to supply the site, facilities or materials used by the third party to facilitate the infringement.[74] Since P2P software providers participate in their users' infringements by providing the tools that enable them to commit those acts, it was the latter line of authority that was to prove crucial in the P2P context.

The scope and content of the modern contributory liability law is also driven by a number of under-recognized physical world assumptions. Since the pre-P2P law suggested that a defendant's knowledge should be held at a time it could do something to prevent the third party infringement, control is a de facto element of contributory liability.[75] Accordingly, the above discussion of the physical world assumptions underpinning vicarious liability's control element is supported in the contributory liability context as well. The knowledge element can also separately

66. *See* PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 8.1 (3d ed. 2005) (note I have updated all references to Goldstein to reflect the 2011-1 supplement). *See also* Jeffrey Lewis, *The Yellow Submarine Steers Clear of U.S. Copyright Law: The Ninth Circuit Re-examines the Doctrine of Contributory Infringement*, 18 LOY. L.A. INT'L & COMP. L. REV. 371, 378 (1996).

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

68. *Id.* at 1162 (internal note omitted).

69. *See* NIMMER, *supra* note 55, at § 12.04[A][3][a]; Craig Grossman, *The Evolutionary Drift of Vicarious Liability and Contributory Infringement: From Interstitial Gap Filler to Arbiter of the Content Wars*, 58 SMU L. REV. 357, 381 (2005). *See, e.g.*, Schuchart & Assocs. v. Solo Serve Corp., No. SA-81-CA-5, 1983 WL 1147, at *1, *7 (W.D. Tex. June 28, 1983).

70. *Gershwin*, 443 F.2d at 1162.

71. Yen, *Third-Party Copyright Liability After Grokster*, *supra* note 3 at 195.

72. *See* GOLDSTEIN, *supra* note 66, at § 8.1.

73. *See id.*

74. *See id.*

75. *See, e.g.*, Grossman, *supra* note 69 at 382.

be seen as being premised on the assumption that physical world rules have universal application. Contributory liability is intended to hold accountable those defendants that are significantly involved with copyright infringements, to the extent that they can be seen as being somehow personally at fault for that tort being committed.[76] Knowledge, held at the time that the defendant was materially contributing to that infringement, has traditionally been seen as a good indicator of this.[77] That's because, in the physical world cases that shaped the law, such knowledge tended to flow naturally from liability-attracting conduct. For example, it is unlikely that a swap meet proprietor that provides the site and facilities for widespread infringement could avoid knowing that its premises are being put to that purpose, or for the organizer of a concert to avoid knowing that unlicensed music is going to be performed. In such physical world scenarios, knowledge flows as a consequence of the ordinary course of business and is not something that can easily be avoided by a defendant who is culpably contributing to that infringement.

The development of contributory liability's material contribution element similarly indicates reliance on physical world assumptions. As signposted above, the law evolved to recognize two types of assistance that might satisfy this element: direct assistance such as the provision of labor, or the supply of the "site and facilities" necessary to facilitate that infringement.[78] Years of physical world precedent demonstrated that culpable facilitators of copyright infringement fell within one or other of these categories, and it seems that courts simply did not envisage the possibility that it might be possible for vast amounts of copyright infringement to be facilitated in the absence of either.

C. SAFE HARBORS

The pre-P2P secondary liability law also featured some carve-outs from liability. These primarily consisted of the DMCA safe harbors and the staple article of commerce or *Sony* doctrine. The DMCA safe harbors played a very minimal role in the P2P software litigation, and this Article will not explore them further.[79] *Sony*, however, played a prominent role. The doctrine was formulated by the U.S. Supreme Court in 1984 in response to litigation seeking to hold the manufacturer of

76. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) (providing that "one who directly contributes to another's infringement should be held accountable").

77. *See, e.g.*, Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); *Fonovisa*, 76 F.3d at 264.

78. GOLDSTEIN, *supra* note 66, at § 8.1.

79. For a fuller examination of the DMCA safe harbor regime, *see id.* at §§ 8.31–8.55; Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1346, 1369–72 (2004); Mike Scott, *Safe Harbors under the Digital Millennium Copyright Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 99 (2005-2006); Yen, *Internet Service Provider Liability*, *supra* note 55, at 1881–85; Zittrain, *supra* note 44, at 265–70. Regarding the application of the safe harbors in P2P litigation, *see* Robert A. Gilmore, *Peer-to-Peer: Copyright Jurisprudence in the New File-Sharing World, the Post Grokster Landscape of Indirect Copyright Infringement and the Digital Millennium Copyright Act*, 5 FLA. COASTAL L.J. 85, 116–119 (2004).

the Betamax tape recorder liable for the infringements of its users.[80] The Court responded to that argument by importing a doctrine from the patent law, holding that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes."[81] It then went even further, adding: "[i]ndeed, it need merely be capable of substantial noninfringing uses."[82]

However, the *Sony* decision left a number of vital questions unanswered. It was never made clear what exactly it meant to be "merely capable" of noninfringing uses, whether the protection extended to both secondary liability doctrines, how substantiality or commercial significance of noninfringing use should be measured or whether infringement could ever be significant enough to disqualify a provider from receiving the protection.[83] These uncertainties long lay dormant until the emergence of rampant online infringement brought the law relating to secondary liability for copyright infringement to the forefront of public attention.

III. THE P2P LITIGATION

When MP3 files of popular copyrighted music first began appearing online in early 1997, the Recording Industry Association of America adopted a strategy of aggressively targeting the owners of the hosting servers with takedown notices to get them pulled offline.[84] Although individuals simply reuploaded them at other locations, the strategy proved highly effective. The constant removal of pages resulted in attempts by Internet users often being met with "file not found" errors, making the process time-consuming and frustrating.[85] By the end of 1999, "[s]earches for MP3 files that had typically been posted on Web sites, FTP sites, and newsgroups often proved fruitless."[86] Professor Stuart Biegel has observed that, at this point, "many commentators predicted that the controversy was ending and that the RIAA had won."[87]

80. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 420 (1984).

81. *Id.* at 442.

82. *Id.*

83. *See* David G. Post, Annemarie Bridy & Timothy Sandefur, '*Nice Questions' Unanswered: Grokster, Sony's Staple Article of Commerce Doctrine, and the Deferred Verdict on Internet File Sharing*, CATO SUP. CT. REV. 235, 246 (2004–2005) [hereinafter Post, *'Nice Questions' Unanswered*]. *See also* Jay Dratler, *Common-sense (Federal) Common Law Adrift in a Statutory Sea, or Why Grokster was a Unanimous Decision*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 413, 427–428 (2006).

84. From 1998, such takedown demands became formalized by the DMCA safe harbor provisions, which are, among other things, contingent on the "expeditious" removal of allegedly infringing content upon receipt of notice. *See* 17 U.S.C. § 512 (2006). Matt Oppenheim, then the senior vice president of business and legal affairs for the RIAA, estimated that copyright owners had "probably sent out well over half a million DMCA . . . cease and desist notices" by June 2003. *See Online News Hour - Forum: Copyright Conundrum*, PUB. BROAD. SERV. (June 2003), http://www.pbs.org/newshour/forum/june03/copyright5.html.

85. JOSEPH MENN, ALL THE RAVE: THE RISE AND FALL OF SHAWN FANNING'S NAPSTER 29 (2003).

86. *See* BIEGEL, *supra* note 38, at xii.

87. *Id.*

However some users persevered, and one of those happened to complain to his college roommate about the frustrating glut of dead links.[88] That roommate was Shawn Fanning, who reasoned that the shortcomings of existing online music distribution could be bypassed by developing an application that maintained a fluid index that could tell users what music was available at any given moment.[89] It would be far less vulnerable to takedowns because the content would be hosted by individuals rather than corporations, and its real-time structure would make it impervious to the scourge of dead links.[90] Fanning executed these ideas in a program called Napster, releasing the first beta version on June 1, 1999.[91] An unprecedented surge of infringement followed.[92] So did a lawsuit by record companies. [93]

A. NAPSTER

While Napster's real-time index facilitated communications between infringing users, it did not itself engage in any direct infringement: the actual transfers of content occurred directly between the hosting and requesting users.[94] Accordingly, the lawsuits alleged that Napster, Inc. was secondarily liable for the infringements committed by its users, and the plaintiffs sought a preliminary injunction to shut it down.[95]

Napster's users had clearly engaged in the direct infringement that is a prerequisite to secondary liability.[96] The real issue was whether Napster, Inc. was sufficiently likely to be held contributorily or vicariously liable for those infringements so as to justify the award of a preliminary injunction against it. The District Court held that it was, and on appeal, the Ninth Circuit unanimously upheld almost all of the lower court's conclusions.[97] In doing so, however, it struggled mightily to apply existing physical world precedent to the code-based Napster technology, and its judgment would prove highly vulnerable to exploitation by speculators who better understood the differences between the two paradigms.

88. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000).

89. MENN, *supra* note 85, at 27 (2003).

90. *Id.* at 34.

91. Wu, *When Code Isn't Law*, *supra* note 4, at 728.

92. *See* Zittrain, *supra* note 44, at 281 (describing Napster as "the open air drug market of copyright infringement").

93. *See* Courtney Macavinta, *Recording Industry Sues Music Start-Up, Cites Black Market*, CNET NEWS, (Dec. 7, 1999, 7:45 PM), http://news.cnet.com/Recording-industry-sues-music-start-up%2C-cites-black-market/2100-1023_3-234092.html.

94. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1012 (9th Cir. 2001).

95. A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

96. *Id.* at 911–15. *See also* Jane C. Ginsburg, *Copyright Use and Excuse on the Internet*, 24 COLUM. J.L. & ARTS 1, 30–34 (2000) (providing a more detailed examination of the District Court and then the Ninth Circuit's treatment of the fair use argument); Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 287–90 (2002).

97. *A&M Records*, 114 F. Supp. 2d at 920, 922; *A&M Records*, 239 F.3d at 1004.

1. Contributory Liability

Although it upheld the District Court's finding that Napster, Inc. was likely to be held contributorily liable for its users' infringements, the Ninth Circuit's reasoning departed from that of the lower court in a number of critical ways. The most significant disagreement concerned the scope of the *Sony* doctrine.[98] One of the longstanding uncertainties surrounding its application was whether or not the *Sony* Court had intended the protection to apply to all forms of secondary liability, as opposed to just contributory or vicarious infringement.[99] This uncertainty arose from the notoriously confusing terminology in the area. In its judgment, the Supreme Court used the terms "contributory" and "vicarious" liability interchangeably, without acknowledging that they actually constituted two independent doctrines within the copyright law, and without making clear whether it intended to use the terms in their broad or narrow senses.[100] This meant that, when it held that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes," it was unclear whether it was referring to contributory liability in the broad sense (to cover all forms of secondary liability) or the narrow.[101]

The District Court had seemingly treated *Sony* as a blanket defense, one that would protect Napster, Inc. from any form of secondary liability—whether contributory or vicarious—as long as its product was capable of substantial noninfringing uses.[102] However, the Ninth Circuit held that *Sony* was in fact far less broad than that, and applied only to contributory liability.[103] Narrower still, it interpreted it as merely being "a gloss" on that doctrine's knowledge element.[104] As noted above, the knowledge element of contributory liability can generally be satisfied by either actual or constructive knowledge.[105] In *Sony*, after finding that the defendant had no actual knowledge of the third-party infringement, the Court had then "declined to impute the requisite level of knowledge" because its product was "capable of both infringing and 'substantial noninfringing uses.'"[106] The Ninth Circuit interpreted this as meaning that it could not impute to Napster constructive

98. *See A&M Records*, 239 F.3d at 1019–22.

99. *See, e.g.*, Post, *'Nice Questions' Unanswered*, *supra* note 83, at 246; Elizabeth Miles, Note, *In re Aimster & MGM, Inc. v. Grokster Ltd.: Peer-to-Peer and the Sony Doctrine*, 19 BERKELEY TECH L.J. 21, 26 (2004).

100. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 435 (1984) (observing that "vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another").

101. *Id.* at 442. *See also* Miles, *supra* note 99, at 26; Post, *supra* note 83, at 246.

102. *A&M Records*, 114 F. Supp. 2d at 916.

103. *A&M Records*, 239 F.3d at 1022.

104. Jesse Feder, *Is Betamax Obsolete? Sony Corp. of America v. Universal City Studios, Inc. in the Age of Napster*, 37 CREIGHTON L. REV. 859, 881 (2004); Ginsburg & Ricketson, *supra* note 63, at 4.

105. *See supra* notes 68–70 and accompanying text.

106. *A&M Records*, 239 F.3d at 1020 (citing Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984)).

knowledge of third party infringement simply because its technology could be used to infringe the plaintiffs' copyrights.[107]

If *Sony* only operates to prevent the imputation of constructive knowledge, the consequence is that it offers no protection in circumstances where the defendant has actual knowledge of third party infringement. The Ninth Circuit upheld the lower court's findings that Napster, Inc. had materially contributed to the infringing activity by providing the necessary "site and facilities," and that it did in fact have actual knowledge of its users' infringements.[108] In light of the latter finding, it was not strictly necessary for the Court to consider whether the rule in *Sony* would have allowed knowledge to be imputed. Nonetheless, it chose to do so, and the resulting analysis gave Napster's successors considerable food for thought. The analysis suggested that *Sony* operates somewhat differently depending on whether the technology at issue is a product or a service.[109] If a product, *Sony* bars constructive knowledge of third party infringements from being imputed as long as it is capable of substantial noninfringing uses.[110] Where a defendant provides a service, however, *Sony* operates to prevent the provider from being liable for contributory infringement by virtue of the mere fact that its system's structure allows for infringement to occur, and says that the service provider has no general duty to monitor for infringement.[111] However, it does not extend so far as to prevent contributory liability from being imposed where the operator learns of specific infringing material available via the system and fails to take steps to remove it.[112]

Thus the Ninth Circuit distinguished products (such as the Napster application that was used to download infringing music) from ongoing services (such as Napster, Inc.'s provision of the servers and the search engine that enabled that infringement to take place).[113] Because of the more favorable treatment given to product providers, Zittrain argues that the decision "implies that had Napster merely built the Napster server and client software and then conveyed the server operation to someone else, it likely would have escaped liability under *Sony*."[114] By suggesting that constructive knowledge can only be imputed where a defendant has some ongoing control over the infringing activity, the Ninth Circuit sent a clear message to future developers that they could avoid liability by eliminating such control—as long as they also ensured that they had no actual knowledge of end user infringement.

2. Vicarious Liability

The Ninth Circuit upheld the District Court's finding that Napster, Inc. had a

107. *Id.* at 1020–21.
108. *Id.* at 1021–22.
109. *Id.* at 1020–22.
110. *Id.* at 1020–21.
111. *Id.* at 1021.
112. *Id.*
113. *Id.* at 1020.
114. Zittrain, *supra* note 44, at 278.

direct financial interest in its users' infringements on the basis that "the availability of infringing material 'act[ed] as a draw' for customers," and because its "future revenue [was] directly dependent upon 'increases in user-base.'"[115] However, it diverged from the lower court's reasoning when addressing the second element of the tort.

The District Court held that Napster, Inc. had the right and ability to supervise its users' infringements because it could "police" the Napster system.[116] The Ninth Circuit agreed, but introduced a vital caveat: that Napster, Inc. could avoid vicarious liability despite its ability to police third party infringement if it exercised that right "to its fullest extent."[117] It noted that Napster, Inc.'s ability to police infringement was limited by the fact that the software was not coded to "'read' the content of indexed files, other than to check that they [we]re in the proper MP3 format."[118] In these circumstances, it held, Napster, Inc.'s right to police was limited to finding infringing content via its indexes, and terminating the access of infringing users in accordance with its contractual ability to do so.[119] Since Napster, Inc. had not actually exercised this power to the fullest extent, the caveat did not protect it from liability. However, the fact it was introduced at all is surprising in light of vicarious liability's roots in enterprise liability.[120] That doctrine has traditionally imposed strict liability on the supervising party where a wrong occurs, regardless of fault.[121] This encourages risk creators to guard against losses, and, if they occur anyway, to spread the cost of providing compensation to victims across those who have benefited from the risk-creating activity.[122] It is intended to maximize the ability of the person who has suffered from the wrong to obtain a remedy.[123] The idea that a defendant can escape liability by exercising its right to police to the fullest extent seems contrary to that objective. And, of course, by telling technology providers that they will not be vicariously liable if they eliminate their ability to control or police their systems, the Court incentivized them to try and do just that.

The case was remanded back to the District Court to modify its injunction in accordance with the Ninth Circuit's findings.[124] Napster never managed to satisfactorily comply with the revised injunction, and on July 1, 2001, its servers were switched off for good, instantly damming its stream of free music.[125]

115. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001).
116. A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 920–21 (N.D. Cal. 2000).
117. *A&M Records*, 239 F.3d at 1023.
118. *Id.* at 1024.
119. *Id.*
120. *See* Yen, *Internet Service Provider Liability*, *supra* note 55, at 1843.
121. *See* Keating, *supra* note 55, at 1286.
122. *See* Yen, *Internet Service Provider Liability*, *supra* note 55, at 1856.
123. *See* Michael W. Carroll, *Disruptive Technology and Common Law Lawmaking: A Brief Analysis of A&M Records, Inc. v. Napster, Inc.*, 9 VILL. SPORTS & ENT. L.J. 5, 25–27 (2002).
124. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).
125. John Borland, *Database "Upgrades" Keep Napster Down*, CNET NEWS (July 6, 2001, 11:00 AM), http://www.news.com/Database-upgrades-keep-Napster-down/2100-1023_3-269367.html?tag=item.

3. Roadmap to Avoiding Liability

The message sent by the Ninth Circuit to Napster's successors was clear: create a product that achieves the same end result as Napster, but eliminate any control over the resulting third party infringement, and you will escape liability for both contributory and vicarious infringement. In reaching its decision, the Ninth Circuit relied heavily on an assumption that some ongoing service was a necessary aspect of facilitating large scale infringement via P2P file sharing software. From a physical world viewpoint that makes perfect sense. Napster, Inc. was essentially acting as a facilitator between those that offered infringing content and those that wanted to obtain it, and in the physical world it is difficult to see how such "matchmaking" could possibly occur in the absence of any ongoing service. Decades of physical world precedent gave illusory support to the court's assumption: After all, if it was practicable for facilitators of large scale third party infringement to eliminate control and knowledge of that infringement, those secondary liability doctrines would undoubtedly have evolved very differently. In these circumstances, it must have seemed to the Court that this was a good basis for distinguishing Napster (which it wanted to hold liable) from technologies like Sony's Betamax (which it did not).

But the Ninth Circuit's solution failed to take into account the differences between the physical and virtual paradigms. When Fanning sat down to code a solution to the glut of dead links, he gave no thought whatsoever to the scope and content of the existing secondary liability law, or to whether his solution might fall foul of it.[126] As it happened, the centralized architecture he adopted fell squarely within the existing doctrine. However, that design was not the only way to facilitate large scale P2P infringement. The Ninth Circuit's decision provided a "roadmap" to avoiding liability.[127] That map read: "Don't be at the center of the P2P network and be sure not to have any ability to police the network. Intentionally relinquish control over the software."[128] Seeking to do so, they took advantage of the flexibility of software code to come up with more and more innovative and anarchic designs that attempted to eliminate Napster's liability-attracting elements whilst facilitating precisely the same end result.[129] The providers of three such technologies, Aimster, Grokster and Morpheus, were particularly blatant in their attempts to code their way out of liability,[130] and the very different responses of the Seventh and Ninth Circuits to those efforts provide grist for an instructive comparison.

126. MENN, *supra* note 85, at 34.

127. Randal C. Picker, *Rewinding Sony: The Evolving Product, Phoning Home and the Duty of Ongoing Design*, 55 CASE W. RES. L. REV. 749, 760 (2005).

128. *Id.* at 760.

129. *See* Ginsburg & Ricketson, *supra* note 63, at 4. *See also* Wu, *When Code Isn't Law, supra* note 4, at 734 (2003); Diane Leenheer Zimmerman, *Daddy, Are We There Yet? Lost in Grokster-Land*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 75, 82 (2005–2006) [hereinafter Zimmerman, *Daddy, Are We There Yet?*].

130. *See generally* Giblin, Code Wars, *supra* note 18, at 46–73.

B. AIMSTER

The Aimster software largely mimicked Napster's design, with one vital addition; it also encrypted all network communications between users.[131] This effectively prevented everybody except the originating and receiving users from having actual knowledge of infringement. Its creator John Deep argued that this made it "impossible [for him] to know exactly what files were being shared."[132]

Trusting that he had successfully coded Aimster to fall outside the strict confines of the existing contributory liability law, Deep brazenly bragged that Aimster more closely resembled the physical-world Betamax than the software-based Napster. "Napster used central computer servers, which could or did know what music files were being swapped. Aimster is more like a VCR; users might pirate movies, but the VCR manufacturer has no knowledge of it."[133] This was a blatant attempt to exploit the physical world/software world divide. Recognizing that the existing secondary liability law had evolved in reliance on the physical world assumption that culpable defendants would not easily be able to eliminate knowledge of third party infringement, Deep had simply coded his technology in a way that eliminated the possibility of his ever having actual knowledge, and relied on the *Sony* doctrine to prevent constructive knowledge from being imputed. Unfortunately for him, the District Court did not appear to appreciate the logic underlying that decision, and it granted a preliminary injunction enjoining the defendants from secondarily infringing the plaintiffs' copyrights.[134] Deep appealed to the Seventh Circuit.[135]

Deep's efforts to exploit the physical world/software world divide by eliminating control and knowledge of third party infringements placed the Seventh Circuit in an unenviable position. He had neatly sidestepped decades of authority dictating that knowledge was an essential corollary to contributory liability by inserting a few extra lines of code into a basic piece of software. A strict application of the physical world principles reiterated by the Ninth Circuit in *Napster* would likely have resulted in Deep avoiding liability simply because of the way he coded his software regardless of his behavior.[136] However, the Seventh Circuit refused to allow that to happen, and instead departed from Napster's reasoning in a way that implicitly recognized the differences between physical technologies and their software-based counterparts.

1. Contributory Liability

The first point of diversion related to the significance of a defendant's technology being capable of substantial non-infringing uses. The Ninth Circuit in

131. *In re* Aimster Copyright Litig., 334 F.3d 643, 646 (7th Cir. 2003).

132. Yen, *Sony*, *supra* note 63, at 840 (citing *In re Aimster*, 334 F.3d at 646).

133. Alec Klein, *Going Napster One Better: Aimster Says Its File-Sharing Software Skirts Legal Quagmire*, WASH. POST, Feb. 25, 2001, at A1.

134. In re Aimster Copyright Litig., 252 F. Supp. 2d 634, 665 (N.D. Ill. 2002).

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

136. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–24 (9th Cir. 2001).

Napster had treated the phrase "capability of substantial non-infringing uses" with considerable deference, going so far as to chastise the District Court for failing to give proper consideration to Napster's actual and potential legitimate uses.[137] By contrast, the Seventh Circuit actually eliminated "capability of substantial noninfringing uses" as *Sony*'s trigger.[138] Under its analysis, a product's current or future capability for substantial noninfringing uses is only the first step towards being protected under *Sony*. Once it has been established that a product has both infringing and noninfringing uses, it is then necessary to make "some estimate of the respective magnitudes of these uses."[139] That is, the Seventh Circuit treated the product's capability of substantial noninfringing uses as "a necessary, rather than a sufficient, condition" to the avoidance of liability.[140] Under this test an Internet file sharing service like Aimster cannot prevent knowledge from being imputed simply because it is capable of substantial noninfringing uses. Instead, it must show "that it would have been disproportionately costly for [it] to eliminate or at least reduce substantially the infringing uses."[141] By requiring the relative costs and benefits of defendant technologies to be taken into account in determining liability, and at least implicitly acknowledging that code-based technologies can be much easier to modify, including post-distribution, than their physical counterparts, this approach forces software providers to take more accountability for their design decisions.

The Seventh Circuit also disagreed with the Ninth Circuit's interpretation of *Sony* in other ways. The Ninth Circuit in *Napster* had interpreted *Sony* as operating only to prevent constructive knowledge of infringement from being imputed if a defendant's product was capable of substantial noninfringing uses.[142] But if the defendant had actual knowledge of infringement, it could be contributorily liable regardless of the nature of its product.[143] The Seventh Circuit disagreed with the District Court's analysis in *Napster* on two counts. Firstly, it held that *Sony* extended to ongoing services as well as products, giving such providers a greater degree of protection.[144] Secondly, it disagreed that defendants with actual knowledge should automatically lose *Sony's* protection, holding that this would sometimes be "contrary to the clear import of the *Sony* decision."[145] The basis of this finding seemed to be that Sony itself had avoided liability even though it must have known that a significant proportion of its users were in fact putting the Betamax to infringing uses.[146] Accordingly, the Court found that if the provider of a service that facilitated infringing as well as noninfringing uses had actual knowledge of the infringement but would have found it "highly burdensome" to

137. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).
138. Zittrain, *supra* note 44, at 283.
139. *In re Aimster*, 334 F.3d at 649.
140. Zittrain, *supra* note 44, at 283.
141. *In re Aimster*, 334 F.3d at 653.
142. *See* discussion *supra* p. 74.
143. *See id.*
144. Zittrain, *supra* note 44, at 283.
145. *In re Aimster*, 334 F.3d at 648–49.
146. *Id.* at 649. *See also* Zittrain, *supra* note 44, at 282–83.

prevent the infringement, it may be inappropriate to hold it liable.[147] That is, a service provider's knowledge and ability to prevent its users from infringing would certainly be a relevant consideration in determining its liability, but liability should not be automatically imposed on that basis alone.

When applied these principles to Aimster, the Seventh Circuit held that Deep's utilization of encryption amounted to willful blindness, and that Deep could not rely on it "to prevent himself from learning what surely he strongly suspects to be the case: that the users of his service—maybe *all* the users of his service—are copyright infringers."[148] The Court then went on to consider whether Aimster nonetheless ought to be protected under *Sony*. It noted that the Aimster tutorial featuring infringing examples was an "invitation to infringement" that went beyond anything Sony had done, and that Club Aimster was intended solely to facilitate access to the most popular—and "invariably" copyrighted—music downloads.[149] The Court held that while this evidence "d[id] not exclude the *possibility* of substantial noninfringing uses of the Aimster system, [it was] sufficient . . . to shift the burden of production to Aimster to demonstrate that its service has substantial noninfringing uses."[150] The Court considered that the Aimster defendants could not avoid liability by showing that their technology was physically capable of being put to noninfringing use if in fact it was only ever used to infringe.[151]

Even if Deep had managed to prove that the Aimster service had substantial noninfringing uses, this would not have been sufficient to avoid liability. Instead, under the Seventh Circuit's analysis, Aimster would have then been obliged to demonstrate that it would have been "disproportionately costly" to eliminate or substantially reduce the infringement.[152] Deep would have failed to do so since he did not "present evidence that the provision of an encryption capability *effective against the service provider itself* added important value to the service or saved significant cost."[153] Accordingly, the Seventh Circuit concluded that Deep was likely to be held liable for contributory infringement if that matter was to proceed to trial. [154]

2. Vicarious Liability

The Seventh Circuit was undecided about whether Deep was also vicariously liable for Aimster's users' infringements, and did not decide the matter. However, it noted that the Supreme Court did not hold Sony vicariously liable even though, by eliminating the fast forward function, it could have dramatically reduced the

147. *In re Aimster*, 334 F.3d at 648–49.
148. *Id.* at 650–51.
149. *Id.* at 651–52.
150. *Id.* at 652.
151. *Id.* at 651.
152. *Id.* at 653.
153. *Id.*
154. *Id.* at 653.

level of infringement.[155] Accordingly, it considered that Deep's failure to remove Aimster's encryption feature and monitor its network may not be enough to render him vicariously liable for the resulting infringement.[156]

An attempt to appeal the Seventh Circuit's decision failed when the U.S. Supreme Court denied certiorari.[157]

C. GROKSTER AND MORPHEUS

The Seventh Circuit's unwillingness to be seduced by the undeniable logic of Deep's argument meant the failure of this attempt to use antiregulatory code to fall outside the existing law. But as the following section will demonstrate, the providers of Grokster and Morpheus enjoyed considerably more success, persuading the Ninth Circuit to strictly apply physical world law to their software based technologies, and successfully exploiting the physical world/software world divide all the way to the U.S. Supreme Court.

The Morpheus and Grokster file sharing clients were powered by the Gnutella and FastTrack P2P protocols. Protocols are sets of rules that govern how a technology will operate.[158] Clients are implementations of those rules.[159] Gnutella was written secretly in just two weeks by two programmers who sought to eliminate Napster's liability-attracting elements, whilst facilitating the same end result.[160] Their ultimate employer, AOL (then deep in merger negotiations with content giant Time Warner), did not share this interest, and the program was quickly withdrawn.[161] But it had already been downloaded thousands of times, and within days source code successfully implementing the protocol had been released into the public domain—although whether obtained solely as the result of reverse-engineering efforts or with the surreptitious assistance of the original renegade developers has never been entirely clear.[162]

Although independent programmers continued to develop the software, their success was mixed. Frankel and Pepper had ingeniously coded Gnutella to create a fully distributed network with no centralized features.[163] This meant that all of the tasks that would normally be performed by central servers were instead shared

155. *Id.* at 648, 654.

156. *Id.* at 654–55.

157. Deep v. Recording Indus. Ass'n of Am., Inc., 540 U.S. 1107 (2004).

158. *A Beginner's Guide to BitTorrent*, BITTORRENT, http://www.bittorrent.com/help/guides/beginners-guide (last visited Oct. 30, 2011).

159. *Id.*

160. Gene Kan, *Gnutella*, *in* PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 94, 95 (Andy Oram ed., 2001).

161. *Id.*

162. *See* Christopher Jones, *Open-Source "Napster" Shut Down*, WIRED NEWS (Mar. 15, 2000), http://www.wired.com/news/print/0,1294,34978,00.html. *See also* Kan, *supra* note 160, at 96; WALLACE WANG, STEAL THIS FILE SHARING BOOK: WHAT THEY WON'T TELL YOU ABOUT FILE SHARING 24 (2004).

163. Kan, *supra* note 160, at 95.

equally amongst every individual on the network.[164] The absence of any centralized points meant that if any part of the Gnutella network were to be shut down, it would have little effect on the rest. This design eliminated the centralized elements that had led to Napster's downfall. But, the trade-off was that it also eliminated much of the efficiency that had contributed to Napster's success.

Gnutella's biggest problem was a lack of scalability, the ability to expand capacity as the network grew.[165] Since its decentralized design forced all network traffic to go through all users, and each message transmitted on the network took up a certain amount of bandwidth, the network inevitably became more heavily burdened as the number of users and messages increased.[166] Napster had addressed that problem by adding more and more servers to its central array as more users joined its network.[167] Lacking the ability to respond the same way, the Gnutella network eventually crashed under the weight of its traffic, remaining out of operation for over a month.[168] Despite Gnutella's problems, users hungry for free music continued to utilize it, and the day after Napster was permanently shut down, Gnutella's usage surged by seventeen percent.[169]

The Napster model was technically robust, but legally vulnerable, while Gnutella was technically frail, but less clearly liable under the existing law. European entrepreneurs Niklas Zennström and Janus Friis spied opportunity in this situation, and hired a team of Estonian programmers to create the FastTrack protocol.[170] Fasttrack was carefully designed with enough centralization to operate with a satisfactory degree of efficiency, whilst having little enough [little enough of what? This is vague: little enough *centralization*] to avoid its providers being liable for its users' infringements under the existing law.[171] As Wu puts it, FastTrack sought to "strike a balance between suability and scalability."[172]

The software implementing the protocol was incorporated into the Kazaa Media Desktop ("KMD") client software.[173] Its solution to the problems that plagued Napster and Gnutella was to utilize a hybrid network architecture that took advantage of the heterogeneity of its users. Upon connecting to the network, users would automatically be designated either a node or a supernode.[174] Nodes were

164. Wu, *When Code Isn't Law*, *supra* note 4, at 731.

165. *Id.* at 732–33.

166. *Id.* at 733.

167. MENN, *supra* note 85, at 120.

168. Wu, *When Code Isn't Law*, *supra* note 4, at 732.

169. *See* Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 519 (2003) (citing *Victory or Defeat?*, SALON (Feb. 12, 2001), http://archive.salon.com/tech/feature/2001/02/12/napster_reactions/print.html (quoting Kelly Truelove, CEO of Clip2)).

170. Tim Wu, *The Copyright Paradox*, 2005 SUP. CT. REV. 229, 239.

171. Wu, *When Code Isn't Law*, *supra* note 4, at 734.

172. *Id.* at 734.

173. *Universal Music Austl. Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289, 308, 311 (Austl.).

174. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1040 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

ordinary users, analogous to the individuals who connected to the Napster network.[175] Supernodes were the best resourced users, the individuals with the fastest Internet connections and most computer processing power, and they carried out duties similar to those that had been performed by Napster's central servers.[176] A user would unknowingly be designated a node or supernode depending on their resources and the current needs of the network.[177] Thus, instead of treating all users equally, it distinguished the users with the most powerful computers and the fastest Internet connections and then co-opted their resources to run the network. As a result, the FastTrack network was far less vulnerable to the bottlenecking and delays that plagued Gnutella.[178]

FastTrack and KMD were initially controlled by Zennström and Friis through their Dutch incorporated company Kazaa BV.[179] KMD's source code was a closely guarded secret, but after its July 2000 release, Kazaa BV also licensed the software to two other companies: Grokster Ltd., which distributed it as Grokster, and StreamCast Networks Inc., which implemented it as an early version of Morpheus.[180] At that point all three branded versions were identical in all essential respects. FastTrack's hybrid structure scaled much better than the original version of Gnutella, and although the Kazaa client alone was downloaded an estimated 317 million times in less than four years, the network never became too overloaded to function.[181] Since users of all three clients were connected to the same network and could seamlessly share files with one another, the FastTrack network rapidly became an even more popular destination for infringing content than Napster had ever been.[182]

It wasn't surprising then that the FastTrack technologies quickly became the primary enforcement target in the war against P2P file sharing. In late 2001, right holders near simultaneously instituted lawsuits in the U.S. and the Netherlands, with the U.S. litigation sweeping up Kazaa BV, Grokster Ltd. and StreamCast Networks Inc., alleging that they "created a 21st century piratical bazaar," and seeking to hold them liable for the copyright infringements of their users.[183] At the time the litigation began, StreamCast's Morpheus still utilized the FastTrack

175. *Id.*
176. *Id.*
177. *Id.*
178. Note that the Gnutella protocol eventually evolved to a similar supernode model, but its original iteration was the only one at issue in the litigation. *See id.* at 1033.
179. *Id.* at 1032.
180. *Id.*
181. *See* Strahilevitz, *supra* note 169, at 520; *Universal Music Australia Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289, 292 (Austl.).
182. *See Grokster*, 243 F. Supp. 2d at 1080. *See also* Jian Liang, Rakesh Kumar & Keith W. Ross, *Understanding KaZaA*, N.Y.U.—POLY, http://cis.poly.edu/~ross/Articles/UnderstandingKaZaA.pdf (last visited Nov. 25, 2011); John Borland, *Free vs. Fee: Underground Still Thrives*, CNET NEWS (May 30, 2003), http://news.com.com/ Free+vs.+fee+Underground+still+thrives/2009-1027_3-1009541.html.
183. *See* Complaint for Damages and Injunctive Relief for Copyright Infringement, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) (No. 01-CV-8541 SVW), *available at* http://www.jdsupra.com/post/documentViewer.aspx?fid=91f70069-f25c-4759-977c-c38980662120; *Grokster*, 259 F. Supp. 2d at 1031.

technology.[184] Soon afterward, however, a licensing dispute caused Morpheus users to be locked out of the FastTrack network, and StreamCast quickly created a new application based on the open source Gnutella.[185] Thus, although FastTrack's owners and licensees were undeniably the primary target of the lawsuit, the Gnutella technology became entangled in the mess, as well.[186] Each of the parties (other than Kazaa BV) cross-filed for summary judgment.[187]

Gnutella and FastTrack appear to have both been carefully engineered to exploit the physical world/software world divide by eliminating the control that was essential to liability under the post-*Napster* law. Neither of them utilized the kind of central server that was the basis of liability in *Napster*, and their developers had apparently followed the Ninth Circuit's roadmap carefully to ensure they did not provide any ongoing service or give their providers control over the networks.[188] Even if an attempt were made to shut them down altogether, the anarchic design of the networks would allow users to continue sharing files uninterrupted.[189] The defendants clearly hoped that, combined with the fact that their products were technically capable of substantial noninfringing uses, this would be sufficient to code their way out of liability under the existing law. That hope was to prove surprisingly well founded. The District Court found that the providers of Grokster and Morpheus could not be held liable for the staggering infringement they facilitated under the existing law, and granted summary judgment in their favor accordingly.[190] To the plaintiffs' dismay, the Ninth Circuit agreed.[191] In fact, as the following paragraphs demonstrate, it swallowed whole the defendant's arguments as to why their products' technical architecture prevented their being liable under the existing law.

1. Contributory Liability

The plaintiffs argued that *Sony* did not protect the defendants in this case because "the vast majority of the software use is for copyright infringement."[192] This argument was consistent with the approach taken by the Seventh Circuit in *Aimster*.[193] However, the Ninth Circuit declared that this "misapprehen[ded] the

184. The litigation was instituted in October 2001. *See Motion Picture and Recording Industries File Suit Against MusicCity and Others*, MOTION PICTURE ASS'N OF AMERICA (Oct. 3, 2001), http://www.mpaa.org/Press/KaZaA_Press_Release.htm. The lockout of Morpheus from the FastTrack network did not occur until February 2002. *See* John Borland, *Morpheus Looks to Gnutella for Help*, CNET NEWS (Feb. 27, 2002), http://news.com.com/2100-1023-846944.html.

185. *See* Borland, *Morpheus Looks to Gnutella for Help*, *supra* note 184.

186. *Id.*

187. *Grokster*, 259 F. Supp. 2d at 1031. Kazaa BV took a different path. The rest of the story is chronicled in Giblin, Code Wars, *supra* note 18, at 104–05, 127–36.

188. *See* Feder, *supra* note 104, at 881–82.

189. *See Grokster*, 259 F. Supp. 2d at 1041.

190. *Id.* at 1031.

191. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1160 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

192. *Id.* at 1162.

193. *See* discussion *supra* pp. 78–80.

Sony standard."[194] *Sony*, the Court explained, is relevant to the degree of knowledge necessary to make out contributory liability.[195] "If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement."[196] If however the product is capable of such noninfringing uses, as those in this case were, the *Sony* protection means that "the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement."[197] The Court then held that the products at issue were indeed capable of substantial noninfringing uses.[198] In a footnote, it observed that although the noninfringing uses may only constitute ten percent of the total, "the volume of use would indicate a minimum of hundreds of thousands of legitimate file exchanges."[199]

As a result of the Court's finding that the defendant technologies were capable of substantial noninfringing uses, contributory liability's knowledge element could only be satisfied by a finding of actual knowledge.[200] The Ninth Circuit then upheld the District Court's finding that such actual knowledge must be held at a time the defendant was contributing to the third party infringement or could do something to stop it.[201] This is something the defendants could technically never be capable of, since the way their software was coded meant that third party infringement always fell outside their control. Indeed, it seems overwhelmingly likely that, to ensure this very outcome, the defendant technologies had been coded to eliminate the liability-attracting Napster-style central index in the first place. This meant that not only was the knowledge element not satisfied on the evidence before the Court, but that it never could be as long as the defendants retained their existing technological designs.[202]

Even if constructive knowledge could have been imputed, the defendants would still have avoided a finding of contributory liability. Just as the code underlying the defendant software applications prevented the knowledge element from being made out, it also succeeded in ensuring that the defendants had not committed the requisite "material" contribution.[203]

The Court held that one way in which material contribution can be made out is where a defendant provides the "site and facilities" for infringement and "fail[s] to

194. *Id.*
195. *Id.* at 1160.
196. *Id.* at 1161.
197. *Id.* at 1161–62.
198. *Id.* at 1162.
199. *Id.* at 1162. Ginsburg and Ricketson have subsequently criticized this reasoning, pointing out that, when it comes down to it, the ninety percent proportion of infringing use is even "more extensive." Ginsburg & Ricketson, *supra* note 63, at 5.
200. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 380 F.3d 1154, 1162 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).
201. *Id.* at 1162–63.
202. *Id.* at 1163.
203. *See infra* pp. 86–88, discussing the Circuit Court's reasoning.

stop specific instances of infringement" once it has knowledge of them.[204] It then upheld the District Court's finding that the defendants could not be said to have supplied such "site and facilities"[205] since, as a consequence of the way the software was coded, "[i]nfringing messages or file indices d[id] not reside on defendants' computers, nor d[id] defendants have the ability to suspend user accounts."[206] The defendants were "not access providers, and they [did] not provide file storage and index maintenance."[207] Instead, "it [wa]s the users of the software who, by connecting to each other over the internet, create[d] the network and provide[d] the access."[208] Grokster's users connected or "bootstrapped" to the network via the preset list of root supernodes that were analogous to Napster's central servers, but since those nodes were not controlled by Grokster Inc. their existence made no difference to its liability.[209] In the Court's view, creating software that facilitated connection to independent networks without any need for assistance or intervention from the defendants was not a sufficiently "material" contribution to any resulting infringement.[210] Since the defendants had not provided the "site and facilities" for infringement, and in the absence of sufficient evidence that they had "materially contributed" in any other way, the contribution element was not satisfied.[211]

The Court's analysis fails to recognize that the main reason why the defendants did not provide the "site and facilities" necessary for infringement was almost certainly because they recognized that so-structuring their software was a direct route to liability, and therefore chose to engineer their products in a way that would place them outside the strict letter of the existing law. To then hold that they were not obliged to exercise the rights that they did have over the resulting software—again, because to do so would not be consistent with existing physical world precedent—seems to implicitly bless the continued exploitation of the differences between the physical and the virtual, and give technology providers a powerful advantage over rights holders.

2. Vicarious Liability

For similar reasons, the Ninth Circuit held that the defendants also fell outside the existing formulation of vicarious liability.[212] The sticking point, once again, was their carefully engineered inability to supervise the infringement. The plaintiffs had argued that their ability to alter their software in a way that would

204. *Grokster*, 380 F.3d at 1163.
205. *Id.*
206. *Id.*
207. *Id.* at 1163–64.
208. *Id.* at 1163.
209. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1040 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).
210. *See Grokster*, 380 F.3d at 1164–65.
211. *Id.* at 1164.
212. *Id.* at 1164–66.

"prevent users from sharing copyrighted files" meant that the defendants did in fact have the requisite right and ability to supervise the third party infringement.[213] However, the Court emphatically rejected this argument:

> In arguing that this ability constitutes evidence of the right and ability to supervise, the Copyright Owners confuse the right and ability to supervise with the strong duty imposed on entities that have already been determined to be liable for vicarious copyright infringement; such entities have an obligation to exercise their policing powers to the fullest extent.[214]

The Court further held that "the potential duty a District Court may place on a vicariously liable defendant is not the same as the 'ability' contemplated by the 'right and ability to supervise' test."[215] Thus, the Court held, "possibilities for upgrading software located on another person's computer are irrelevant to determining whether vicarious liability exists."[216] It explained that the requisite "'right and ability to supervise' describes a relationship between the defendant and the direct infringer."[217] Citing *Napster* "for the proposition that some degree of control over user behavior and the ability to terminate access were strong evidence of the control necessary to establish vicarious liability," the Court held that in this case there was no evidence of such a relationship.[218] "The sort of monitoring and supervisory relationship that has supported vicarious liability in the past is completely absent in this case."[219] The Court's analysis, and this conclusion in particular, is remarkable for its lack of enquiry into precisely why the relationship is different, and whether those differences ought to give rise to a different sort of treatment than those previous relationships. Instead of doing so, however, it simply chose to accept that the architecture created by the underlying software code was sufficient to prevent liability from attaching.

Finally, the Ninth Circuit rejected the plaintiffs' argument that "[t]urning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability," holding that "there is no separate 'blind eye' theory or element of vicarious liability that exists independently of the traditional elements of liability."[220] This contrasts with the approach taken by the Seventh Circuit, which held that the incorporation of encryption into Aimster's design constituted a form of willful blindness.[221]

Accordingly, the Ninth Circuit upheld the District Court's findings and granted

213. *Id.* at 1165–66.
214. *Id.* at 1166.
215. *Id.*
216. *Id.*
217. *Id.* at 1164.
218. *See* Yen, *Sony*, *supra* note 63, at 847. *See also* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1165 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).
219. *Grokster*, 380 F.3d at 1165.
220. *Id.* at 1166.
221. *In re* Aimster Copyright Litig., 334 F.3d 643, 650–51 (7th Cir. 2003); Andrew J. Lee, *MGM Studios Inc v. Grokster Ltd. & In Re Aimster Litigation: A Study of Secondary Copyright Liability in the Peer-to-Peer Context*, 20 BERKELEY TECH. L.J. 485, 503–04 (2005). *See also infra* discussion at page 80.

summary judgment in favor of the defendants.[222] The defendants' aim of aligning themselves more closely with the VCR than with Napster had clearly succeeded: the District Court expressly noted that "Grokster and StreamCast [were] not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights . . . Absent evidence of active and substantial contribution to the infringement itself, Defendants cannot be liable."[223] The combination of the defendants' coding their technologies to mimic the behavior of physical world hardware, and the Ninth Circuit's decision not to distinguish code-based from physical technologies, meant that the defendants successfully escaped liability under the existing law.[224]

3. Old Rules; New Game

So far this Article has demonstrated that the pre-P2P secondary liability law evolved almost exclusively with reference to physical world scenarios and technologies, and thus came to rely on certain assumptions that had almost invariably held good in the physical world context. One of the most significant was the idea that it would generally be infeasible, impossible or impractical for a person to culpably facilitate a third party's infringement without having some control over that infringement. This came to underpin the two doctrines that then governed secondary liability for copyright infringement. In the vicarious liability context this manifested in the requirement that the defendant has the "right and ability to supervise" the third party infringement.[225] In the contributory liability context, at least according to the Ninth Circuit's interpretation, it manifested in two ways: the principle that liability depends on whether the defendant has actual knowledge of the third party infringement at the time they are contributing to it and can do something to stop it, and the way in which the *Sony* defense provides less advantageous treatment (by allowing constructive knowledge to be imputed) where a defendant has ongoing control over the infringing activity.[226]

The reason why the law evolved in this manner was because, in the physical world scenarios that shaped it, control usually flowed naturally from the parties' involvement, and tended to be noneliminable except at the sacrifice of a considerable amount of efficiency or profit. Since secondary infringers could not practicably eliminate control, it worked well as a mechanism for capturing wrongdoers in the physical world context, and successfully limited the number of

222. *Grokster*, 380 F.3d at 1167.

223. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1043 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

224. Wu, *When Code Isn't Law*, *supra* note 4, at 738 (arguing that the decision "suggest[ed] that the changes in design 'worked,' at least with respect to negating the element of control that sealed Napster's fate").

225. Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

226. *Grokster*, 380 F.3d at 1162–63; A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001).

end user infringements.[227] However, as the P2P cases demonstrate, that physical world assumption doesn't necessarily hold in the software world context. It turns out that P2P providers do not have to play by the same rules as the swap meet organizers, department store owners and concert controllers that came before them, and that there were a number of ways in which they could code their software to ensure that it could facilitate enormous amounts of unauthorized copying without their having any relevant control.

The Seventh and Ninth Circuits were both faced with defendants that had deliberately coded their technologies to fall outside the strict boundary of the existing law. The Ninth Circuit played the new game with the old rules, strictly applying earlier precedent to P2P file sharing software in the same way it believed it had been applied to the Betamax VCR. But its application of existing physical world precedent to the defendant's code-based technologies caused it to conclude that the defendants should escape liability if their technologies were designed in a way that made it impossible for them to control their users' behavior—an outcome antithetical to what those principles were formulated to achieve. After all, one of the primary purposes of secondary liability law is to provide a remedy to large scale infringement where it would be inefficient to target direct infringers.[228]

Intuitively, this suggests "that creators of peer-to-peer networks are more likely to be held liable when their networks lead to the unchecked infringement of copyrighted works, and less likely to be held liable when their networks retain some ability to prevent infringement."[229] But the Ninth Circuit's analysis resulted in the opposite conclusion, actually encouraging software providers to design and unleash uncontrollable tools of infringement, even where infringement could be significantly reduced at minimal cost.[230] By continuing to apply principles that evolved with reference to physical technologies to virtual ones, Picker argues that the Ninth Circuit "ignores the new realities of networked products and what those should mean for ongoing design obligations."[231] The end result was that the Ninth Circuit allowed the defendants to code their way out of liability, and gave future defendants a bright line guide to achieving that same end.

In contrast, the Seventh Circuit seemed to recognize that some fundamental characteristic distinguished Aimster from its physical world predecessors, and responded by coming up with some new rules of its own.[232] In beginning to acknowledge the differences between code-based and physical technologies, the Seventh Circuit imposed a previously unheard of form of "code-based gatekeeping" liability on software providers that forced them to be more

227. Hays, *supra* note 7, at 617 (describing predigital era secondary infringements as "for the most part, crude, marginal transactions, the subjects of swap meets and unlicensed kiosks").

228. Mark A. Lemley, *Inducing Patent Infringement*, 39 U.C. DAVIS L. REV. 225, 228 (2005); Yen, *Sony*, *supra* note 63, at 849.

229. Yen, *Sony*, *supra* note 63, at 848.

230. *Id.* at 848–49. *See also* Craig Steckley, *MGM v. Grokster: A Disincentive for Technological Responsibility*, 7 TUL. J. TECH. & INTELL. PROP. 299, 310–11 (2005).

231. Picker, *supra* note 127, at 757.

232. *See supra* pp. 78–81.

accountable for their design decisions.[233] This approach diverted from the strict application of preexisting precedent by suggesting that the relative amounts of infringing and noninfringing uses, as well as how easily infringement could have been avoided, should be taken into account in determining secondary liability. This approach considers the "relative costs and benefits" of defendant technologies, and acknowledges that code-based technologies can be much easier to modify, including postdistribution, than their physical counterparts.[234]

However, there are problems with this approach as well. As Yen points out, existing theories of secondary liability were not formulated to take such aspects into account.[235] The Seventh Circuit was only able to render them relevant by stretching the *Sony* protection to cover the Aimster-shaped loophole. Additionally, although the Court seemed to recognize some of the inherent differences between the code-based and physical paradigms, it did so only implicitly. As a result, the broader principles it developed to respond to Aimster are also applicable to physical technologies, resulting in a continued conjunction of unlike technologies. As this Article makes clear, application of identical principles to the physical world and the software world can lead to ill-fitting outcomes. Continued equation of the two stifles genuine debate over the differences between the two paradigms, and whether it may be appropriate to apply different liability standards to code-based and physical world technologies. Some of the criticisms that have been leveled at the Seventh Circuit's decision are attributable to the fact that the principles it enunciated in Aimster apply equally to both. For example, one major disparagement is that the Seventh Circuit's approach "contemplates a broad range of sweeping preemptive design changes . . . if a cost-benefit analysis, including evidence of current uses of the technology in question" suggests that it is appropriate to do so.[236] Zittrain has described these design changes as "analogous to requiring a VCR maker to remove the fast forward or record buttons."[237] The fact that the Supreme Court rejected such a proposal when deciding *Sony* makes advocates for retaining that decision's protections critical of this reasoning. If physical and virtual technologies were distinguished from one another, however, with the effect that the Seventh Circuit's solution did not apply to physical world technologies like the Betamax, its merits might have been more clearly apparent.

Giving more direct consideration to the differences between the technologies could also result in better-tailored solutions for widespread infringement facilitated by P2P software. By not explicitly recognizing the differences between physical world and software world technologies, the Seventh Circuit's reasoning remains vulnerable to exploitation to those who do so. This is particularly the case with respect to its analysis regarding the knowledge element. The Seventh Circuit thwarted the Aimster defendants' efforts to code their way out of contributory

233. Zittrain, *supra* note 44, at 286 (2006).
234. *See also* Picker, *supra* note 127, at 749.
235. Yen, *Sony*, *supra* note 63, at 818–19.
236. Zittrain, *supra* note 44, at 285–86.
237. *Id.* at 286 (internal note omitted).

liability's knowledge element by using the willful blindness framework.[238] In the absence of willful blindness however, it seems that contributory infringement still requires actual or constructive knowledge to be made out before liability can accrue.[239] This suggests that a P2P provider may still code its way out of liability if it eliminates the requisite degree of knowledge without being willfully blind to that infringement within the meaning of the existing law—a loophole just begging to be exploited by a future Johnny Deep. If the judgment had expressly recognized the differences between physical and virtual technologies, instead of attempting to be broad enough to cover the unique characteristics of each, it may well have resulted in more precise and targeted standards. As it stands, the Seventh Circuit's approach prevented the defendants from succeeding in their attempt to code their way out of liability under the existing law, but it also resulted in a doctrine of uncertain breadth and probable prejudice to future technologies.

4. In the Supreme Court

The combination of the circuit split and the high stakes prompted the Supreme Court to grant certiorari and hear the content industry's appeal.[240] Eventually, it unanimously reversed the Ninth Circuit's decision to uphold summary judgment, introduced a third theory of secondary liability and strongly hinted that the defendants ought to be held liable under that newly minted doctrine on remand.[241]

The likely reason for the Supreme Court's reliance on a third theory of secondary liability was that its members were unable to agree on what the staple article of commerce doctrine actually stood for, as publicly demonstrated by the decision's two conflicting concurrences.[242] The compromise was that the Supreme Court preserved the *Sony* doctrine as a shield that may operate to protect a technology provider from contributory liability, but it was made clear that it does not preclude liability where there is an actual intention to induce the third party infringement.[243] Accordingly, the Supreme Court held that the Ninth Circuit had "misapplied *Sony*, which it read as limiting secondary liability quite beyond the circumstances to which the case applied."[244]

238. *In re* Aimster Copyright Litig., 334 F.3d at 650–651.

239. *See, e.g.*, Bosch v. Ball-Kell, No. 03-1408, 2006 WL 2548053, at *12 (C.D. Ill. Aug. 31, 2006); Monotype Imaging, Inc. v. Bitstream, Inc., 376 F. Supp. 2d 877, 883 (N.D. Ill. 2005).

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

241. Note, however, that there is some controversy regarding whether the Supreme Court actually created a new theory of liability, or whether it merely clarified existing contributory liability principles. *See* Giblin, Code Wars, *supra* note 18, at 89–91.

242. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 916, 949 (2005) (Ginsburg, J., concurring) (Breyer, J., concurring).

243. *Id.* at 935–36.

244. *Id.* at 933.

5. It *is* Possible to Code Your Way Out of Vicarious and Contributory Infringement

By deciding the case on inducement, the Supreme Court sidestepped some very difficult questions. In its analysis the Ninth Circuit held that *Sony* is only relevant to contributory liability's knowledge element.[245] Even if knowledge becomes easier to make out because *Sony* does not apply, that counts for nothing if contributory liability's second element is not made out. The Supreme Court's vigorous debate over the scope and meaning of *Sony* masked the fact that the ingenious way in which the defendants coded their software convinced the Ninth Circuit that the contribution element could not be satisfied—a conclusion that lay undisturbed on appeal.[246] Effectively then, the defendants achieved their aim of coding their way out of contributory liability.

They apparently also succeeded in coding their way out of vicarious liability. The Supreme Court declined to consider whether the defendants were vicariously liable for their users' infringements and did not expressly disturb the Ninth Circuit's findings on this point.[247] Accordingly, the Court left open the possibility that parties can escape vicarious liability by deliberately engineering their products to evade control. Indeed, if anything, the Court actually increased the scope for future defendants to code their way out of vicarious liability. It did so via the very definition it gave for liability under this doctrine—that one "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it."[248] Despite citing the classic case of *Shapiro v. H.L. Green* as authority for this test, the Supreme Court's formulation actually represents a significant shift away from previous strict liability formulations. Under those formulations, liability is imposed where the appropriate relationship exists, regardless of whether the defendant exercises all of the control that it has over the third party infringer.[249] As Yen explains however, the Supreme Court's formulation "allows the defendant to escape liability by exercising control . . . . No longer does a defendant face liability even if she exercises control. To the contrary, she escapes liability if she exercises whatever control she has, even if she fails to stop the infringement."[250]

This approach is consistent with that taken by the Ninth Circuit in *Napster*, but it diverges significantly from previous vicarious liability case law and indeed seems inconsistent with the origins and rationale for the doctrine. This formulation suggests that even a half-decade after P2P software developers had started exploiting the existing law's physical world assumptions, the Supreme Court still did not fully understand how the rules of the game had changed. Unlike previous

245. *A&M Records*, 239 F.3d at 1020.

246. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1163–64 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

247. *Grokster*, 545 U.S. at 930 n.9.

248. *Id.* at 930 (citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963)).

249. Yen, *Third-Party Copyright Liability After Grokster*, *supra* note 3, at 228–29.

250. *Id.*

physical world technologies, code-based distribution technologies have proved capable of being designed to eliminate or dramatically reduce the amount of control necessary whilst still facilitating enormous amounts of infringement.[251] But, by redefining the vicarious liability doctrine to provide that there will be no liability where all possible control over the third party has been exercised, even if that fails to prevent the infringement, the Supreme Court apparently made it easier than ever for designers of P2P technologies to code their way out of vicarious liability.[252]

Thus the defendants had avoided contributory liability because their software's architecture apparently prevented the contribution element from being satisfied, and they had avoided vicarious liability because its design made it impossible for them to have the requisite right and ability to supervise third party infringement.[253] They had succeeded in coding their file sharing software in ways that fell outside of the existing U.S. secondary liability law. Stymied by the fact that existing secondary liability principles seemed to provide no remedy against these obvious scofflaws, the Supreme Court created a new theory of liability with which to defeat them.

6. Inducement

Just as in 1984, the Supreme Court looked to copyright's cousin, patent law, for inspiration. Section 271(b) of Chapter 35 of the United States Code had long provided that "whoever actively induces infringement of a patent shall be liable as an infringer."[254] The Supreme Court imported it wholesale, holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[255] This was a compromise by a Court which believed that the defendants should not escape liability for their behavior—but which was irreconcilably split as to whether they should be liable under *Sony*.

Officially, the Supreme Court remanded the matter to the district court to determine the defendants' liability under this new theory. However, it strongly suggested that liability ought to attach. Pointing to three "particularly notable" indicia of intent, the Court unanimously declared the defendants' "unlawful objective . . . unmistakable."[256]

The first factor was that "each [defendant] company showed itself to be aiming to satisfy a known source of demand for copyright infringement, the market

251. *See* Giblin, Code Wars, *supra* note 18, at 46–73. *See also* discussion *supra* pp. 78–95; discussion *infra* pp. 112–117.

252. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005)

253. *See id.*

254. 35 U.S.C. § 271 (2006). For useful perspectives on inducement liability in the patent context, *see generally* Charles W. Adams, *A Brief History of Indirect Liability for Patent Infringement*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 369 (2006); Lemley, *Inducing Patent Infringement*, *supra* note 228.

255. *Grokster*, 545 U.S. at 919.

256. *Id.* at 939–40.

comprising former Napster users."[257] In addition to advertising to Napster users (internal company documents made reference to Napster), Grokster appeared to have derived its name from Napster, and the defendants' software functioned similarly to Napster's.[258] The Court concluded that the defendants' "efforts to supply services to former Napster users, deprived of a mechanism to copy and distribute what were overwhelmingly infringing files, indicate a principal, if not exclusive, intent on the part of each to bring about infringement."[259]

The second factor was the defendants' failure to develop filtering tools or other mechanisms that would reduce the amount of infringement that occurred through the use of their software.[260] "[W]e think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement."[261] In a footnote, the Court went on to say that without "other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the *Sony* safe harbor."[262]

Third, the Court found it significant that the more the defendant technologies were used, the greater the advertising revenue earned by the defendants.[263] Once again the Court qualified this factor: "This evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear."[264] Thus it appears that the amount of revenue linked to infringement only becomes a relevant factor once there is some other evidence of bad intent. That is, if the business has encouraged that infringement in some way and the business model is reliant on infringement, that reliance can be taken into account in determining whether or not there was inducement. In this case there was evidence that the respondents' revenue was heavily reliant on infringement, with approximately ninety percent of all use infringing. This factor was the most tenuous of the three. Felten finds it "hard to think of *any* conceivable business model for a software company under which an increase in use of the product does not lead to an increase in revenue."[265] Zimmerman has pointed out that the defendants' being financially better off by virtue of their users' infringement would

> be the case to some degree with any dual use technology distributed by a profit-making entity. It would be surprising, for example, if Apple did not sell more iPods because some people value them as wonderful tools for the illicit downloading of

257. *Id.* at 939.
258. *Id.* at 937–38.
259. *Id.* at 939.
260. *Id.*
261. *Id.*
262. *Id.* at 939 n.12.
263. *Id.* at 939–40.
264. *Id.*
265. Edward Felten, *Business Model as Evidence of Intent*, FREEDOM TO TINKER (June 27, 2005, 5:24 AM), http://www.freedom-to-tinker.com/?p=856.

music, rather than merely as a way to download from legal channels.[266]

Combined, these indicia caused Tim Wu to describe the decision as an example of the "Miss Manners' School of Jurisprudence."[267] In his opinion, it was the brash and blatant way in which the P2P defendants went about achieving their goals that led to their undoing:

> The P2P companies were loud scofflaws, foreigners, and college students who blatantly encouraged illegal acts. KaZaA's successor by contrast, Apple's iTunes, may ultimately pose a greater threat to the recording industry, but it operates in a respectable way. Steve Jobs is a rebel with manners. And that has made all the difference.[268]

Taking the Supreme Court's broad hint that it ought to be held liable on remand, Grokster Ltd. chose to settle the lawsuit shortly after the Supreme Court's inducement decision was handed down.[269] StreamCast however elected to pursue the matter, and in September 2006, almost five years after the litigation commenced, summary judgment was finally entered against it on the basis that it had induced third party infringement.[270]

While the creation of the inducement doctrine filled the law's *Grokster* shaped hole, the Court did not take the opportunity to consider more fundamentally what it was about software-based file sharing technologies that justified treating them differently from their predecessors. As a result, the Supreme Court's new doctrine, like its predecessors, turned out to be based on a number of physical world assumptions that would turn out not to hold in the software context. As will become apparent, the mismatch between that decision's assumptions and the realities of P2P development was the main cause of the subsequent explosion in the number and variety of P2P applications, and the inevitable abandonment of the secondary liability campaign against P2P software providers.

IV. HOW *GROKSTER* LED DIRECTLY TO MORE P2P PROVIDERS

A. BATTLES WON. WAR LOST.

By 2005, rights holders had litigated their way to a considerably stronger position vis-à-vis technology providers than when they had commenced the litigation campaign against P2P software providers in 1999. But rather than pressing forward by ramping up the campaign, they chose instead to abruptly end

266. Zimmerman, *Daddy, Are We There Yet?*, *supra* note 129, at 92–93.

267. Tim Wu, *A Supreme Court Conversation: The Miss Manners School of Jurisprudence*, SLATE (June 28, 2005, 10:31 AM), http://www.slate.com/id/2121410/entry/2121673.

268. *Id.*

269. *See* Press Release, Recording Industry Association of America, Music Industry Announces Grokster Settlement (Nov. 7, 2005), http://www.riaa.com/print.php?id=81648953-2457-2877-94B4-D28C93625445 [hereinafter RIAA Press Release].

270. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 999 (C.D. Cal. 2006).

it.[271]

In part, this can be attributed to the fact that most existing commercial operators had engaged in the same kind of bad-acting behavior as that which had supported the finding of inducement in *Grokster* and, seeing the writing on the wall, quickly negotiated settlements and exited the market.[272] Lime Group LLC was the only major holdout in this category—and the last scalp claimed in the P2P litigation campaign: the District Court engaged in a straightforward application of the inducement doctrine, and this time had no hesitation in granting summary judgment in the plaintiffs' favor.[273]

But, this is not to say that P2P software development ceased after *Grokster* was handed down. In fact, the opposite is true. There was actually an explosion in the number of P2P file sharing programs available for users to download. By 2007, two years after *Grokster* was handed down, online software repository SourceForge listed literally thousands of file sharing software projects, each presumably being developed by an individual or corporation undeterred by the decisions against their predecessors and competitors.[274] Those programs were being put to enthusiastic use: the BigChampagne media measurement company estimated that during that same year, 9.35 million individuals were simultaneously sharing files on P2P networks at any one time.[275] The biggest challenge of all was coming from BitTorrent, a P2P distribution technology that was developed in 2002 by programmer Bram Cohen to facilitate the legitimate distribution of the enormous files favored by the jamband community.[276] Inevitably, however, the technology's ability to facilitate the online distribution of very large files in an efficient manner also made it the tool of choice for unauthorized distribution of movies, games and TV. As an unofficial online manual to the technology explains, "[i]t was not designed as a haven for pirates and copyright violation, it just happens to be *really*

271. Giblin, Code Wars, *supra* note 18, at 1.

272. *See, e.g.*, RIAA Press Release, *supra* note 274 (announcing the eventual settlement reached against Grokster, Ltd.); Rebecca Giblin, *Australia to Become 'Nerve Centre' for P2P Litigation?*, 7(5) COMPUTER REV. INT'L. 156 (2006) (regarding the settlement reached against those behind the Kazaa/FastTrack technologies); Nancy Gohring, *eDonkey, Record Industry Reach a Deal*, PC WORLD (Sep. 13, 2006), http://www.pcworld.com/article/127126/edonkey_record_industry_reach_a_deal.html (regarding the settlement with the provider of the eDonkey P2P file sharing software); Ed Oswald, *BearShare Settles with RIAA for $30M*, BETANEWS (May 5, 2006), http://betanews.com/2006/05/05/bearshare-settles-with-riaa-for-30m/ (announcing the settlement agreement reached between the RIAA and Gnutella-client Bearshare).

273. *See* Arista Records LLC v. Lime Group LLC, No. 06 CV 5936 (KMW), 2011 WL 1742029, at *1 (S.D.N.Y. May 2, 2011).

274. Original research performed on SOURCEFORGE, http://sourceforge.net/ (last visited Nov. 11, 2011) (On Oct. 24, 2007, author performed a search for "file sharing" projects, which yielded 2,180 results. Since that time, the number of file sharing projects on record has changed. Original documentation of this research is on file with the author.).

275. Bangeman, *P2P Traffic Shifts Away from Music*, *supra* note 9.

276. *See* Kim Peterson, *BitTorrent File-Sharing Program Floods the Web*, SEATTLE TIMES, Jan. 10, 2005, at C1. For detailed consideration of the jamband phenomenon and its fascinating history, *see* Mark F. Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law*, 21 BERKELEY TECH. L.J. 651 (2006).

good for it."[277] By 2007, BitTorrent usage was estimated to account for between 55 and 75% of global Internet traffic, with more than 100 million installations claimed worldwide.[278]

Popular websites host torrent files linking to a cornucopia of infringing movies, music, television shows and computer games, and display statistics suggesting that popular movies and TV shows are regularly downloaded thousands of times each.[279] Although the ephemeral and disparate nature of BitTorrent networks makes it difficult to accurately gauge the overall proportion of infringing use, a University of Ballarat-affiliated Internet Commerce Security Laboratory study, involving a sample of 1000 torrent files, concluded that 89% were definitely infringing and only 0.3% were definitely noninfringing (the remainder of the sample comprised pornographic movies, which were not conclusively categorized one way or another).[280] In total, 97.9% of all nonpornographic files were found to infringe copyright, and every one of the nonpornographic movies, music and TV shows was infringing.[281] Although the methodology of this study has been questioned, it does give some statistical weight to what has long been apparent—BitTorrent's infringing usage is extremely substantial.[282]

So why was it that P2P software development exploded in the wake of the *Grokster* decision? And why was it that, despite the huge level of infringement facilitated by those new file sharing programs, the litigation campaign against P2P software providers came to a halt so soon after that favorable judgment?

B. SOME SOFTWARE WORLD REALITIES

Once again, the answer to those questions lies in mismatches between physical world assumptions and software world realities. So far, this Article has focused largely on the first of the four physical world assumptions that were identified in Part I: the idea that physical world rules apply to all. That assumption manifested in a number of ways, including the development of secondary liability laws that

277. Melee, *The BitTorrent Bible* (Jan. 30, 2005), http://www.freeinfosociety.com/media/pdf/3939.pdf.

278. *See* Bangeman, *P2P Responsible for as Much as 90 Percent of All 'Net Traffic*, *supra* note 9; Bram Cohen, *Mark Cuban Says BitTorrent is Doomed, DOOMED!*, LIVEJOURNAL (Jan. 31, 2007), http://bramcohen.livejournal.com/35949.html. *See also About BitTorrent*, BITTORRENT, http://www.bittorrent.com/company/about (last visited Nov. 11, 2011).

279. *See, e.g.*, EZTV, http://www.eztv.it (last visited Nov. 11, 2011); NEWTORRENTS.INFO, http://www.newtorrents.info (last visited Nov. 11, 2011); THE PIRATE BAY, http://www.thepiratebay.org (last visited Nov. 11, 2011).

280. Robert Layton & Paul Watters, *Investigation into the Extent of Infringing Content on BitTorrent Networks*, INTERNET COMMERCE SECURITY LABORATORY (Apr. 2010), at 17, http://www.afact.org.au/research/bt_report_final.pdf.

281. *Id.* at 18.

282. *See* Renai LeMay, *Ballarat's BitTorrent Study 'Horribly Wrong': TorrentFreak*, PC WORLD (Jul. 26, 2010), http://www.pcworld.idg.com.au/article/354459/ballarat_bittorrent_study_horribly_wrong_torrentfreak/; *Ars Technica Forgets How Torrents Work, Cites Faulty Study*, POLITICS AND P2P (Jul. 23, 2010), http://ktetch.wordpress.com/2010/07/23/arstechnica-forgets-how-torrents-work-cites-faulty-study/.

were premised on the idea that culpable defendants would have some kind of control over third party infringers. When this assumption was shattered by the development of ever and more anarchic P2P distribution technologies, content interests agitated for laws that allowed for secondary liability to be imposed in the absence of control, culminating in the Supreme Court's decision in *Grokster*.[283] In the months after those decisions were reached, however, it must have slowly dawned on the victors that even these new and broadened formulations were going to be of very little assistance in stamping out the continued development of P2P file sharing applications that facilitated a vast amount of infringement.

In explaining why, the other three physical world assumptions that were introduced in Part I really came into play: the ideas that distribution technologies capable of facilitating vast amounts of infringement are expensive to create, that their developers will be motivated by profit and that their creators will try to keep their secrets from competitors. Each of these assumptions was premised on the idea that not just anyone could or would be able to create a technology capable of widespread copying or distribution. While they held true, the gatekeeper enforcement model remained an effective means of controlling large scale infringement. But this Part will demonstrate that those assumptions don't necessarily hold true in the software context—and that their inapplicability in the context of P2P file sharing software led directly and inevitably to the abandonment of the campaign against P2P software providers. It does so by identifying some key software world realities, and demonstrating how they contrast with those physical world assumptions.

1. A Code-Based Distribution Technology Capable of Vast Amounts of Infringement Can Be Created Very Cheaply

As explained in Part I, the creation of physical world distribution technologies capable of vast amounts of infringements—such as printing presses, photocopiers and VCRs—typically requires large investments in research, development and infrastructure.[284] As Litman explains, U.S. copyright law "was designed in an era

283. As well as pushing for revisions to the existing secondary liability law, lobbying efforts sought the enactment of more favorable legislation. The most significant outcome of these lobbying efforts was the INDUCE Act—later known as the Inducing Infringement of Copyrights Act—which was introduced to Congress in June 2004 and then referred to the U.S. Senate Committee on the Judiciary. If passed, it would have amended 17 U.S.C. § 501 to add a cause of action for "intentionally inducing" copyright infringement. The proposed legislation proved tremendously controversial, with suggestions that it would give rise to liability for such diverse products as the iPod, TiVo, the email "forward" function and even the *New York Times*. For a comprehensive summary of the products suggested to be under threat, *see* James Grimmelmann, *The LawMeme Reader's Guide to Ernie Miller's Guide to the INDUCE Act*, LAW MEME (Jul. 15, 2004, 2:19 PM), http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1549. After vociferous grassroots protests and technology industry lobbying, the bill never made it out of committee. *See* Bill Rosenblatt, *Induce Act Dead for This Year*, DRM WATCH (Oct. 14, 2004), http://www.drmwatch.com/legal/article.php/11578_3421731_2.

284. Zittrain, *supra* note 44, at 255.

in which mass distribution of copies of works required a significant capital investment."[285] Even if the initial invention of a physical world distribution technology is achieved cheaply—and history is filled with examples of hobbyist inventors on shoestring budgets making amazing breakthroughs—getting it to market inevitably still requires significant capital injections to finance further refinement of the technology, construction of a working prototype, mass-manufacturing, packaging, compliance with regulatory requirements (such as electrical safety standards) and marketing and distribution of the resulting devices in each market.[286] Such costs presented significant barriers to market entry, and led to secondary liability laws evolving on the assumption that there would be relatively few manufacturers of technologies that were capable of vast amounts of infringement.

But we have seen throughout this Article that this assumption does not always hold true in the software context. The brief history of P2P has demonstrated time after time that code-based distribution technologies can be unleashed from the minutest financial investments. Napster was created by a teenager in response to an idle comment from his roommate; Gnutella was "developed in just fourteen days by two guys without college degrees" and BitTorrent was invented by an unemployed programmer working from his dining room table.[287] Indeed, the costs associated with creating file sharing programs are so low that some universities routinely require students to create them as part of their undergraduate computer science studies.[288]

The cheapness and ease of P2P file sharing software development can be further illustrated by a sequence of events that began with Professor Edward Felten uploading what he claimed to be the world's smallest P2P file sharing application to his website in 2004.[289] Utilizing just fifteen lines of software code, the purpose of the exercise was to illustrate the ease of creation and thus "the difficulty of regulating peer-to-peer applications."[290] But that point was made even more emphatically than Felten had intended: as news of his feat spread, so too did an implied challenge to create one that was even smaller. Within just 24 hours, the source code for a number of even tinier alternatives began to mushroom online, with the effort eventually culminating in at least one challenger writing a P2P file sharing application using just six lines of code.[291]

Not only is it possible for the initial development costs of software-based

285. Litman, *supra* note 43, at 253.

286. WU, THE MASTER SWITCH, *supra* note 45 (discussing many hobbyist inventors).

287. *See* Kan, *supra* note 160, at 95; Daniel Roth, *Torrential Reign*, 152 FORTUNE 68, 69 (2005).

288. *See e.g.*, *Programming Assignment 4*, UNIV. OF NOTRE DAME – DEP'T OF COMPUTER SCIENCE & ENG'G, http://www.cse.nd.edu/~cpoellab/teaching/cse354/ project4.html (last visited Nov. 11, 2011); *Programming Assignment 5*, UNIV. OF NOTRE DAME – DEP'T OF COMPUTER SCIENCE & ENG'G , http://www.cse.nd.edu/~cpoellab/teaching/ cse354/project5.html (last visited Nov. 11, 2011).

289. *See* Edward Felten, *P2P in 15 Lines of Code*, FREEDOM TO TINKER (Dec. 15, 2004, 1:25 AM), http://www.freedom-to-tinker.com/?p=738; Edward Felten, *TinyP2P*, TINYP2P, http://ww7.be/ neofutur/tools/sharing/tinyp2p.html (last visited Nov. 11, 2011).

290. *See* Felten, *P2P in 15 Lines of Code*, *supra* note 289; Felten, *TinyP2P*, *supra* note 289.

291. *See* Felten, *P2P in 15 Lines of Code*, *supra* note 289.

distribution technologies to be low, but the manufacture and distribution of software-based distribution technologies can also be virtually costless. The marginal cost of creating additional copies of the prototype software approximates zero.[292] While there can be costs associated with hosting a website to distribute software, these can be easily avoided since a number of sites (such as SourceForge) will host and distribute software free of charge.[293] Alternatively, a developer could outsource its distribution costs to users by disseminating its software using a P2P protocol such as BitTorrent. Any of these virtually cost-free online distribution methods allows the finished product to hit the global market within minutes, and if the software is useful and fills a niche, there is no need for expensive marketing. Word of mouth across the online file sharing community can do the rest.

2. Developers Aren't Necessarily Motivated by Profit

The second physical world assumption follows closely from the first. If developing a distribution technology capable of facilitating vast amounts of infringement requires a substantial investment, it follows that its provider will want to extract a profit or at least recoup its costs. The resulting link between financial benefit and liability for the copyright infringements of third parties is strong. The most obvious manifestation of this assumption is in the financial element of vicarious infringement, but it has sometimes even influenced contributory infringement analyses.[294] Likewise, the Supreme Court's inducement analysis was heavily influenced by the defendants' infringement-reliant business model.[295]

In the physical world context, using actual or intended infringement related profit-making as an indicia of liability makes a lot of sense. As Ganley explains, in that paradigm:

> The normal phases of R&D, product design, manufacture, unit testing and distribution all help to constrain the wilder excesses of copyright infringing potential. The inherent checks and balances in the structure of legitimate businesses help to ensure that companies will shy away from such costly and time consuming exercises if they believe there is no legitimate avenue for them to recoup their substantial investment.[296]

This assumption that distribution technology providers will want to profit from their inventions can certainly be supported in the software context, as was amply

292. *See, e.g.*, Richard Stallman, *Why Software Should Be Free*, MIKROPOLIS (Apr. 24, 1992), http://www.mikropolis.org/wp-content/uploads/2009/08/why-software-should-be-free1.pdf.

293. *See, e.g.*, SOURCEFORGE.NET, http://sourceforge.net/create/ (last visited Nov. 7, 2011).

294. *See* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (developing the modern contributory infringement framework and finding liability while seemingly influenced by the fact that the defendant had significantly profited from infringement, although profit was not, strictly speaking, an element of the tort). *See also* Fonovisa Inc. v. Cherry Auction Inc., 76 F.3d 259, 259 (9th Cir. 1996) (indicating that the Court was influenced by the fact that Cherry Auction was profiting from the increased revenue that resulted from the infringement).

295. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005).

296. Ganley, *supra* note 49, at 22.

demonstrated by the providers of Napster, Aimster, Grokster, Morpheus and Kazaa. However, the fact that a code-based distribution technology can be created, refined, marketed and distributed globally with relatively little investment of time or money means that development projects do not necessarily have to be driven by the prospect of financial advantage. As Zittrain explains, "[b]efore the advent of modems and networks, major physical-world infringers typically needed a business model because mass-scale copyright infringements required substantial investment in copying and distribution infrastructure. With the advent of the Net, large scale infringements became possible through the sum of minor favors among friends and strangers."[297]

While this is not to say that the developers of such projects would not be happy to turn a profit, it means that they have unprecedented scope to create projects that are not primarily driven by the need or the desire to do so. When Felten's disciples spent a frenzied week working to better his fifteen line P2P app, it is doubtful that they had any thought or expectation that financial reward would flow from that work. No prize or reward was offered by Felten. Instead the challengers appear to have been motivated by less tangible rewards, such as the satisfaction of solving a tricky intellectual puzzle, the enjoyment that comes from publicly one-upping a celebrated Princeton professor and perhaps even the expectation of some brief worship from the online peanut gallery. Those individuals only worked on their projects for a few days, but this willingness to work on hobby projects without the motivation of financial gain can extend indefinitely.

An inkling of the extent to which this development model exists can be gleaned from the SourceForge open source software repository, which hosts a vast number of P2P projects that apparently have no revenue model at all, including a number which have been under continuing development for a number of years. Some of these projects include ANts P2P, a single-developer project that creates an anonymous P2P network; MUTE, which creates a file sharing network designed to protect end user privacy, and Gtk-Gnutella, a Gnutella client intended for use on Unix operating systems.[298] This willingness to create innovative and sophisticated distribution technologies purely for the challenge, satisfaction and reputation that come from creating something really cool has been replicated many times over. The secrecy with which Frankel and Pepper developed Gnutella suggests they knew AOL would never sanction its continued development once the cat was out of the bag, but they created it anyway.[299] Even Bram Cohen, creator of the revolutionary BitTorrent distribution technology, never actually intended to

297. Zittrain, *supra* note 44, at 255.

298. *See ANts P2P*, SOURCEFORGE, http://sourceforge.net/projects/antsp2p/ (last visited Nov. 11, 2011); *GTK-GNUTELLA*, SOURCEFORGE, http://gtk-gnutella.sourceforge.net/ (last visited Nov. 11, 2011); *MUTE: Simple, Anonymous File Sharing*, SOURCEFORGE, http://mute-net.sourceforge.net (last visited Nov. 11, 2011).

299. David Kushner, *The World's Most Dangerous Geek*, DAVID KUSHNER (Jan. 13, 2004), http://74.220.215.94/~davidkus/index.php?option=com_content&view=article&id=82:the-worlds-most-dangerous-geek-&catid=35:articles&Itemid=54.

commercialize it.[300] Once it was finished "he was ready to move on to something new," and only built it into a company because of some arm-twisting by his father.[301]

Of course, as Wu has pointed out in a different context, "the human urge to speak, create, build things, and otherwise express oneself for its own sake, without expectation of financial reward, is hardly new."[302] After all, there have been hobbyists and inventors throughout history who have made amazing breakthroughs without any financial incentive at all.[303] There is however a vital difference between this willingness of physical world inventors and that of their software world equivalents. An inventor of a physical world distribution technology might be able to make the technological breakthrough on a shoestring budget, but as described above there are significant and unavoidable costs associated with the development of any physical world distribution technology to bring it to the point where it's capable of facilitating any large amount of infringement that exist regardless of the inventor's willingness to work for free. By contrast, a P2P programmer can potentially create a distribution technology, get it to market and distribute it globally for an unprecedentedly small amount of cash.

3. Tell Everyone How it Works—Maybe They Can Help Improve It

The third assumption relevant to explaining the explosion in post-*Grokster* P2P development follows naturally from those discussed above. Assume that researching, developing, manufacturing and distributing a technology that is capable of widespread infringement will be expensive, and thus there is a need to make some profit or recoup those costs. From that perspective, it is unthinkable that someone might create a new kind of technology capable of revolutionizing the way content is distributed, and then freely give away that idea (and detailed instructions for implementing it) to others.

It is not unusual for software developers to similarly lock away their secrets.[304] But there are also strong norms in the software development community that promote sharing them with the world.[305] Software's secrets are contained in something known as source code, the human-readable instructions written by the programmer in a particular programming language.[306] In order to operate on a

300. Roth, *supra* note 287, at 73.

301. *Id.*

302. WU, THE MASTER SWITCH, *supra* note 45, at 37.

303. *Id.*

304. For example, the FastTrack protocol stack and Kazaa Media Desktop software were closed source, and the source code kept secret. In fact the secret was held so tightly that even by the end of a fully argued bench trial regarding its owners' secondary liability in Australia, the court was still not entirely persuaded that it had been provided with the software's true source code. *See Universal Music Austl. Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289, 339–44 (Austl.).

305. *See, e.g.*, GLYN MOODY, REBEL CODE: THE INSIDE STORY OF LINUX AND THE OPEN SOURCE REVOLUTION (2002); RICHARD M. STALLMAN, FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN (Joshua Gay ed., 2009).

306. Jacqueline D. Lipton, *IP's Problem Child: Shifting the Paradigms for Software Protection*,

computer, source code must be compiled into machine-readable object code.[307] Once this conversion takes place, it is almost always no longer comprehensible to humans.[308] This means that, unless a separate copy of the original source code is provided with the software, it is possible to ascertain what a software program does (for example, by observing network outputs and outcomes), but not precisely how it does it. Where the source code is provided, the program is referred to as being "open source," otherwise it is known as "closed source" or "proprietary" code.[309] However, being truly "open source" means more than just making the source code available. The most widely accepted definition of the concept, coined by the Open Source Initiative organization, also requires, among other things, that the terms of the software's license allow for that software to be freely redistributed, for "modifications and derived works" to be developed and for those modified versions to be able to be distributed under the same terms as the original.[310]

The P2P secondary liability cases decided to date have almost exclusively involved large scale commercial P2P operators, which overwhelmingly favored closed source code. Napster, Kazaa, Grokster and Morpheus (until it was locked out of the FastTrack network) were all closed source.[311] Gnutella was the earliest open source pioneer to achieve widespread popularity. Those in control of its code willingly released it for free to the general public, permitting it to be altered by strangers as they saw fit.[312] This willingness to give away a technology's secrets is far from being an isolated case.

58 HASTINGS L.J. 205, 219 (2006) [hereinafter Lipton, *IP's Problem Child*].

307. *Id.*

308. *Id.* at 219–22 (describing source code as "human-readable" and object code as "machine-readable").

309. *See generally* James Gibson, *Once and Future Copyright*, 81 NOTRE DAME L. REV. 167, 173–75 (2005) (providing a more detailed explanation of source codes); Josh Lerner & Jean Tirole, *Some Simple Economics of Open Source*, 50(2) J. INDUS. ECON. 197, 200 (2002) (providing, particularly in footnote 5, more detailed information regarding source codes). *See also* Lipton, *IP's Problem Child*, *supra* note 306.

310. Ken Coar, *The Open Source Definition*, OPEN SOURCE INITIATIVE, http://opensource.org/docs/osd (last visited Sept. 25, 2011). *See generally* MOODY, *supra* note 305 (providing a comprehensive examination of the history and explanation of open source and "free" software); JOSEPH FELLER, BRIAN FITZGERALD & ERIC S. RAYMOND, UNDERSTANDING OPEN SOURCE SOFTWARE DEVELOPMENT (2001) (providing comprehensive examination as well). Where a program's source code is made available for viewing but cannot freely be further developed, this more limited concept is generally referred to as "shared source." *See, e.g.*, *Shared Source Initiative*, MICROSOFT, http://www.microsoft.com/resources/sharedsource/default.mspx (last visited Nov. 11, 2011).

311. For a discussion of Napster being closed source, *see, e.g.*, RAMESH SUBRAMANIAN & BRIAN D. GOODMAN, PEER-TO-PEER COMPUTING: THE EVOLUTION OF A DISRUPTIVE TECHNOLOGY 43 (2005). For a discussion of Kazaa, *see, e.g.*, Peter Backx et al., *A Comparison of Peer-to-Peer Architectures* (2002), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.151.9453&rep=rep1&type=pdf; *Universal Music Austl. Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289, 339–44 (Austl.). For a discussion of Grokster, *see, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1039 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005). For a discussion of Morpheus, *see, e.g.*, Borland, *Morpheus Looks to Gnutella for Help*, *supra* note 184.

312. Source code replicating the Gnutella protocol was released into the public domain days after the release by Pepper and Frankel. *See* Kan, *supra* note 160, at 96.

As noted in Section A above, software repository SourceForge was hosting literally thousands of open source file sharing projects two years after Grokster was handed down.[313] For a long time BitTorrent was also open source. When Cohen released his technology, he made its underlying source code widely available and provided a general license allowing third parties to further develop and distribute the software.[314] The protocol documentation, specifying the requirements necessary to creating a compatible client, was also made available online.[315] While each of the official BitTorrent clients released after August 2007 was closed source, the source code of all previous iterations and the protocol itself remain fully documented and "publicly accessible without the need for a license."[316] As a result, any person with the requisite programming skill can code his or her own BitTorrent client, and thousands of individuals and organizations have done so to date.[317] Such independently created BitTorrent clients can be of excellent quality—indeed, BitTorrent Inc. found the µTorrent client to be such a beautifully executed implementation of the protocol that it ended up purchasing it, then adopting a rebranded version as its official client in 2006.[318] This occasional willingness of programmers to freely share the secrets that underlie their inventions is yet another vital and under-recognized distinction between the development of code-based and physical distribution technologies.

C. BITTORRENT & THE SIGNIFICANCE OF THE MISMATCH

With reference to the BitTorrent distribution system, the following pages explain the practical significance of the mismatch between the post *Grokster* law's physical world assumptions and the software world's realities, and why it led directly to the abandonment of the secondary liability campaign against P2P software providers.[319]

313. *See supra* note 274 and accompanying text.

314. *BitTorrent Open Source License*, BITTORRENT, http://www2.bittorrent.com/legal/bittorrent-open-source-license (last visited Nov. 11, 2011) (showing license in its current form).

315. *See BitTorrent Protocol Specification v1.0*, THEORY.ORG (Sep. 13, 2006), http://wiki.theory.org/BitTorrentSpecification; *For Developers*, BITTORRENT.ORG, http://bittorrent.org/beps/bep_0000.html (last visited Nov. 11, 2011).

316. *See* Ryan Paul, *BitTorrent's Closed Protocol: Fact or Fiction? (Updated)*, ARS TECHNICA (Aug. 10, 2007), http://arstechnica.com/news.ars/post/20070810-will-bittorrent-protocol-documentation-be-publicly-available-bittorrent-inc-president-says-no-company-web-site-says-yes.html. *See also* Thomas Mennecke, *BitTorrent Addresses Closed Source Issues*, SLYCK (Aug. 8, 2007), http://www.slyck.com/story1566.html.

317. See *BitTorrent client*, WIKIPEDIA, http://en.wikipedia.org/wiki/BitTorrent_client (last visited Nov. 11, 2011) (listing BitTorrent clients currently available). Original research was also performed on SOURCEFORGE, http://sourceforge.net/ (last visited Nov. 11, 2011) (On Oct. 24, 2007, author performed a search for "BitTorrent" projects, which yielded 206 results. Since that time, the number of BitTorrent projects on record has changed. Original documentation of this research is on file with the author.).

318. George Ou, *BitTorrent Buys uTorrent, Reaction Mixed*, ZDNET (Dec. 7, 2006), http://blogs.zdnet.com/Ou/?p=389.

319. *See generally* Rebecca Giblin, *A Bit Liable? A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 7 (2008) (providing more detailed analyses of the potential liability of BitTorrent, Inc. and Bram Cohen under United States and Australian

1. How BitTorrent Works

"BitTorrent" refers to a number of distinct concepts. The BitTorrent protocol dictates the technology's operation. BitTorrent clients implement that protocol. Since the technology was open source for the first years of its existence, there are a huge number of such clients.[320] Several have been provided by BitTorrent Inc. (the company created by its inventor to commercialize the technology), but mostly they've been made available by independent third parties. It has even entered the vernacular as a verb—to the dismay of content interests—individuals who miss episodes of their favorite TV shows may well announce an intention to "BitTorrent" them.[321]

The BitTorrent distribution process is a lot like a jigsaw puzzle. Users seek to obtain parts of the puzzle from any number of others, and then they piece it together into a coherent whole once they're all gathered. The process begins when the holder of a piece of content uses a BitTorrent client to divide it into a number of much smaller pieces and to create an associated "torrent" file.[322] The torrent file contains metadata about the piece of content (such as the number of pieces into which it was divided, and the order in which they should be pieced back together), but not the content itself.[323] Torrent files are then commonly made available via the World Wide Web.[324] Any Web server is sufficient, but hosts commonly upload their torrents to one of a number of specialized torrent hosting websites in order to make them more easily locatable.[325] Some such sites, most notably Sweden's infamous Pirate Bay, are clearly designed to facilitate access to infringing content.[326] Unlike Napster, Kazaa, Morpheus and so on, BitTorrent clients typically have no integrated search functionality.[327] Instead, individuals must

law); Rebecca Giblin, *The Uncertainties, Baby: Hidden Perils of Australia's Authorisation Law*, 20 AUSTL. INTELL. PROP. J. 148 (2009) (providing analyses as well).

320. *See supra* note 317.

321. A recent Google search for "bittorrent the episode" returned over 1,400 results. GOOGLE, http://www.google.com (last visited Nov. 11, 2011).

322. Bram Cohen, *The BitTorrent Protocol Specification*, BITTORRENT.ORG (Jan. 10, 2008, 4:43 PM), http:// www.bittorrent.org/beps/bep_0003.html. *See also BitTorrent Protocol Specification v1.0*, *supra* note 315.

323. J.A. Pouwelse et. al., *A Measurement Study of the BitTorrent Peer-to-Peer File-Sharing System*, DELFT U. OF TECHNOLOGY (May 15, 2004), http://www.citeulike.org/user/twleung/article/71746.

324. Bram Cohen, *Incentives Build Robustness in BitTorrent* (May 22, 2003), http:// citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.1911.

325. *See supra* note 279 for some of the main hosting sites.

326. For example, The Pirate Bay's website does not just contain a neutral search engine. It also provides direct links to categories, such as "TV shows," "music" and "Top 100" (which, in turn, leads to further subcategories, such as "applications," "games" and so on, allowing users to easily browse what appears to be almost entirely copyright-protected content, and then to simply and easily download the corresponding torrent files that would allow infringing copies to be downloaded. *See* THE PIRATE BAY, http://www.thepiratebay.org (last visited Nov. 11, 2011).

327. Note, however, that some clients now include a link to search engines enabling users to search for torrents from within the client. *See, e.g.*, *Xtorrent: Mac BitTorrent Client with Integrated Search*, WEBMONKEY, http://www.webmonkey.com/2006/09/xtorrent_mac_bittorrent_client_with_integrated_

independently find a torrent associated with desired content, which they may do via dedicated torrent search engines, by browsing torrent hosting sites, or simply by adding "filetype:torrent" to any Google search.[328] They might also use BitTorrent Inc.'s own torrent search engine, which was added to its website in May 2005.[329] That facility, which is completely independent of the BitTorrent software and protocol, "crawls" the World Wide Web for torrent files to create an index, from which it provides users with responses to their search queries.[330]

Once a torrent file has been obtained, BitTorrent client software uses the information within it to facilitate the distribution of the desired content amongst users.[331] Users transferring content via BitTorrent are categorized as either "seeds" or "leechers."[332] Seeds are users who continue uploading pieces of a resource to others, despite themselves already having a complete copy.[333] The first seed will often be the host user who originally created and published the torrent file, but it can be any user who has a complete copy of the resource that matches the metadata in the torrent file. Leechers are users that are attempting to obtain all or part of the file.[334] Collectively, a group of seeds and leechers is known as a "swarm."[335]

It is important to understand that unlike Napster, Gnutella and FastTrack, BitTorrent does not facilitate the creation of a single vast network to which every BitTorrent user connects. Instead, each swarm effectively comprises a discrete peer network devoted exclusively to distributing a resource associated with a particular torrent.[336] Communications within the swarm are traditionally facilitated by a tracker or trackers, which are BitTorrent's equivalent to Napster's central servers and FastTrack's supernodes.[337] Their role is to maintain information about the users distributing a particular resource, including their IP addresses and a record of those pieces they already have and those they are yet to obtain.[338] Using that information, trackers effectively act as a "rendezvous point" for those involved in distributing the resource associated with a particular torrent.[339]

When the BitTorrent protocol was first formulated, trackers represented the

search/ (last visited Nov. 11, 2011).

328. Poulwelse, *supra* note 323, at 2.

329. Kevin Poulsen, *Next for BitTorrent: Search*, WIRED NEWS (May 23, 2005), http://www.wired.com/techbiz/media/news/2005/05/67596.

330. *Id.*

331. Cohen, *Incentives Build Robustness in BitTorrent*, *supra* note 324.

332. M. Izal et. al., *Dissecting BitTorrent: Five Months in a Torrent's Lifetime*, *in* Proc. Passive & Active Measurement 1, 2 (Chadi Barakat & Ian Pratt eds., 2004), *available at* http://www.eurecom.fr/~btroup/BPublished/bittorrent.pdf.

333. *Id.*

334. *Id.*

335. *See, e.g.*, Spencer Kelly, *BitTorrent Battles Over Bandwidth*, BBC NEWS (Apr. 13, 2006), http://news.bbc.co.uk/2/hi/programmes/click_online/4905660.stm.

336. Izal, *supra* note 332, at 2.

337. *Id.*

338. *See, e.g.*, Pouwelse, *supra* note 323; Bob Rietjens, *Give and Ye Shall Receive! The Copyright Implications of BitTorrent*, SCRIPT-ED: A J. OF LAW, TECH. & SOC'Y (2005), http://www.law.ed.ac.uk/ahrc/script-ed/vol2-3/torrent.asp.

339. Izal, *supra* note 332, at 2.

most vulnerable point in the distribution process.[340] Their failure due to technical or legal difficulties had been observed to cause severe interruptions to the downloading of infringing torrents.[341] However, an extension to the protocol was subsequently developed that now enables files to be distributed without the assistance of a tracker, using Distributed Hash Tables or DHT.[342] Commonly referred to as "trackerless torrenting," DHT enlists peers to perform the tracker's traditional functions through the creation of a separate decentralized P2P network to which most modern BitTorrent clients now connect by default.[343] An additional technology known as Peer Exchange or PEX can be used to further reduce the load on the tracker or DHT system by allowing for individual peers to subsequently share the locations of others amongst themselves.[344] These technologies have been so successful in reducing reliance on centralized trackers that the Pirate Bay switched its tracking server off in 2009, explaining that the maturation of DHT and PEX meant that there was no longer any need for it.[345] "This is what we consider to be the future. Faster and more stability for the users because there is no central point to rely upon."[346]

Unlike most distribution systems, BitTorrent's performance actually improves as more users try to simultaneously download a particular piece of content.[347] That's because once a leecher has obtained a piece of the resource from one source, it begins uploading or sending it to other users while it simultaneously downloads new ones.[348] By spreading the distribution across all users, rather than concentrating it on the few that have the entire copy, popular content can be distributed very widely, very fast. When highly popular files are released via BitTorrent, thousands or even tens of thousands of peers have been known to join swarms within hours.[349] The system is also extremely efficient. Cohen designed it with a "tit-for-tat" algorithm to encourage peers to put their upload allocation to

340. *See* Pouwelse, *supra* note 323 (discussing that the failure that a tracker can have).

341. *Id.*

342. *See* Thomas Mennecke, *Official BitTorrent Developer Releases Trackerless Client*, SLYCK NEWS (May 19, 2005), http://www.slyck.com/news.php?story=795 (providing more information).

343. *Id.*

344. *See, e.g.*, *Peer Exchange*, VUZE, http://wiki.vuze.com/w/Peer_Exchange (last visited Nov. 11, 2011).

345. *World's Most Resilient* [sic] *Tracking*, THE PIRATE BAY (Nov. 17, 2009), http://thepiratebay.org/blog/175.

346. *Id.*

347. Rietjens, *supra* note 338.

348. *Id.*

349. *See Heroes: Run! Episode Summary*, TV.COM, http://www.tv.com/heroes/run!/episode/924072/summary.html?om_act=convert&om_clk=episodessh&tag=episodes;title;1 (last visited Oct. 14, 2011) (an example of a popular file). Torrent indexing website EZTVefnet.org quickly posted links to a torrent file for the episode. Less than three days after the original airdate, statistics displayed on that site showed that the swarm currently downloading that file comprised 16,450 seeds and 12,528 leechers, and that the episode had been downloaded in its entirety 168,139 times. These statistics reflect only the particular torrent to which ETVefnet.org had linked. It is likely that more than one torrent for that episode had been created and distributed around the Internet, potentially resulting in an even higher number of infringements.

best use, and thus to achieve Pareto efficiency.[350] In the event that a particular peer does not reciprocate by sending data upstream in exchange for downloaded pieces, they can find themselves at the bottom of the priority list for the next piece of the file.[351] Another clever element of the BitTorrent distribution process is the protocol's policy of "rarest first."[352] If pieces of the resource were distributed randomly, it is more likely that a situation will arise where nobody in the swarm has one or more necessary pieces. However, the protocol enables peers to automatically request the rarest pieces first, thereby maximizing the life of the swarm.[353] Still, swarms inevitably die out as peers stop sharing a particular resource or simply go offline. Leechers who are stranded with only part of the file when this occurs may never be able to complete their download.

2. Contributory and Vicarious Liability Ruled Out by BitTorrent's Design

If BitTorrent Inc. or any other BitTorrent client provider were sued for the infringements of their users, it is unlikely they would be liable under existing formulations of contributory or vicarious infringement. Although the BitTorrent distribution process has two points of centralization—the trackers and torrent hosting websites—the system is designed in such a way that providers of BitTorrent software need not have control over either. That is, the trackers and torrent hosting websites can be (and usually are) completely independent of the software providers.[354] Additionally, the system incorporates no internal search functionality, and creates no single network like that of Napster, Grokster and Sharman's technologies.[355] These design features combine to ensure that no BitTorrent software provider could be liable for its users' infringements under the existing contributory or vicarious liability law. Here's why.

To start, any contributory liability analysis would be partly shaped by whether the technology was accepted as being capable of substantial noninfringing uses. This is likely to be controversial because its legitimate usages are significantly outweighed by those that are infringing—making it fall into a category of products for which the Supreme Court was unable to agree on the proper treatment.[356] It would, however, be relevant to the analysis that the technology's current legitimate uses are varied and growing, and include the distribution of the enormously popular World of Warcraft computer game, independent films, Linux operating systems and even data published by NASA.[357]

350. Cohen, *Incentives Build Robustness in BitTorrent*, *supra* note 324.

351. *Id.*

352. *BitTorrent Protocol Specification v1.0*, *supra* note 315.

353. Cohen, *Incentives Build Robustness in BitTorrent*, *supra* note 324.

354. Edward Felten, *BitTorrent Search*, FREEDOM TO TINKER (May 26, 2005, 6:27 AM), https://freedom-to-tinker.com/blog/felten/bittorrent-search.

355. *See* John Borland, *BitTorrent File-Swapping Networks Face Crisis*, ZDNET NEWS (Dec. 20, 2004, 8:52 PM), http://www.zdnet.com/news/bittorrent-file-swapping-networks-face-crisis/140385.

356. *See generally* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

357. *See, e.g.*, Schultz, supra note 276, at 687; *FAQ*, VODO, http://vo.do/faq (last visited Nov. 11, 2011); *Frequently Asked Questions*, BLIZZARD ENTERTAINMENT, http://us.blizzard.com/en-us/company/

Increasingly, it is also used to streamline data distribution within enterprise. For example, after adopting BitTorrent technology for rolling out software to its thousands of servers, Facebook became able to send updates hundreds of megabytes in size to tens of thousands of machines in a single minute—a process that could take hours via more traditional distribution technologies.[358] Engineers at Twitter similarly managed to use BitTorrent to reduce the time it took to deploy code across its servers from forty minutes to a mere twelve seconds.[359] Its efficiencies are such that even high profile content owners like Warner Brothers, Twentieth Century Fox and MTV have at various times gotten onboard the BitTorrent bandwagon.[360] If *Sony* does apply, the consequence is that contributory liability can only be made out if BitTorrent Inc. has sufficient actual knowledge of third party infringement. The Ninth Circuit in *Grokster* held that, to satisfy this element, actual knowledge must be held at a time that the defendant was contributing to the third party infringement or could do something to stop it.[361] This is something that no BitTorrent software provider could satisfy, since the design of their software means that third party infringement is always outside their control.

However, the issue of whether *Sony* applies is something of a red herring. That is because, even if the knowledge element could be satisfied, BitTorrent providers do not appear to have relevantly contributed to the third party infringement. In accordance with the Ninth Circuit's reasoning in *Grokster* (which was undisturbed by the Supreme Court on appeal), the creation of software that facilitates connection to independent networks without any need for assistance or intervention from the defendants is not a sufficiently "material" contribution to any resulting infringement.[362] Vicarious liability is also ruled out by the technology's design. Even if the defendants were found to have the requisite financial interest in the third party infringement, they nonetheless have no right and ability to supervise that infringement within the meaning of the existing law, and thus could not be held vicariously liable for it.

One of the most interesting aspects of BitTorrent's design is the way in which it disproves the belief that efficiency and liability resistance are mutually exclusive.

about/legal-faq.html (last visited Nov. 11, 2011) (explaining how Blizzard can distribute large files to the public). *See also* Cory Doctorow, *U.S. Govt Uses BitTorrent*, BOING BOING (Apr. 6, 2005, 3:34 PM), http://www.boingboing.net/2005/04/06/us_govt_uses_bittorr.html.

358. Ernesto, *Facebook Uses BitTorrent, and They Love It*, TORRENTFREAK (June 25, 2010), http://torrentfreak.com/facebook-uses-bittorrent-and-they-love-it-100625/.

359. Larry Gadea, *Murder: Fast Datacenter Code Deploys Using BitTorrent*, TWITTER ENGINEERING (July 15, 2010), http://engineering.twitter.com/2010/07/murder-fast-datacenter-code-deploys.html.

360. *See, e.g.*, Peter Bowes, *Warner to Start Movie Downloads*, BBC NEWS (May 9, 2006), http://news.bbc.co.uk/1/hi/business/4753435.stm; Sunshine Mugrabi, *BitTorrent Hooks Big Studios*, RED HERRING (Nov. 29, 2006), http://www.redherring.com/Article.aspx?a=19936&hed=BitTorrent+Hooks+Big+Studios.

361. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 380 F.3d 1154, 1162–63 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

362. *Id.* at 1163–64.

The evolution of Gnutella and Kazaa suggested that departing from Napster's centralized P2P model to eliminate liability-attracting control would result in less efficient ways of distributing content. As Wu stated in 2003:

> The design of P2P applications to avoid copyright presents a technical challenge with implications not fully appreciated by legal scholarship. The technical study of P2P design shows that designing a P2P filesharing network to avoid copyright requires important deviations from the optimal design for speed, control, and usability. The programmers of a copyright-resistant P2P network must balance an interest in avoiding legal liability against the competing interests of ensuring performance on a mass scale, maintaining system stability, and fostering network trust. These matters all require control over the network, while a pure peer design eliminates control as much as possible.[363]

Thus, it was assumed that a P2P software provider could not design an optimally efficient distribution system without having a liability-attracting degree of control over it. If it did have control, it could be liable under the doctrines of contributory or vicarious infringement. With BitTorrent, however, which was actually released before Wu's article even made it to print, Cohen proved that it was possible to code a P2P distribution technology that achieves a high degree of efficiency even though the software provider has no control whatsoever over any of the networks formed when individuals attempt to distribute a piece of content. BitTorrent certainly has centralized points—in the form of trackers and torrent hosting and indexing sites—which help achieve these aims, but (by design) they can and do exist completely independently of BitTorrent software providers.[364] The result is a technology that, contrary to all accepted wisdom, facilitates the fast, efficient and effortless transfer of data, and does so in a way that is powerfully protective of its provider's liability.

3. Inducement

Since the technology's design seemingly rules out BitTorrent software providers from being liable under existing control-based formulations of contributory and vicarious liability, rights holders would be obliged to rely on inducement. Inducement focuses on the individual defendant's conduct and intent, and is not automatically ruled out by a defendant's lack of immediate control over the third party infringement.[365]

Has BitTorrent Inc. "distributed a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement?"[366] In large part, the answer to this question depends on the interpretation given to this newly-minted doctrine. If an interpretation is adopted that requires some active step being taken to promote infringement, it is unlikely that BitTorrent Inc. would be liable. The public record does not disclose any

363. Wu, *When Code Isn't Law, supra* note 4, at 717 (internal note omitted).
364. *See* Felten, *BitTorrent Search*, *supra* note 354.
365. *See Grokster*, 545 U.S. at 934–41.
366. *Id.* at 918.

evidence of bad intent similar to that which justified the finding of liability against the providers of the Grokster, Morpheus or LimeWire technologies. To the contrary, BitTorrent Inc has consistently promoted its software as a useful tool for efficient legitimate content distribution, and has gone to some lengths to ensure that its own search engine does not return links to torrents associated with infringing content.[367] Ginsburg has argued that "the most probative Grokster element" is the promotion of the availability of infringing content—something that is certainly absent on these facts.[368] Furthermore, the technology is actually designed in a way that makes it easy for rights holders to identify direct infringers, a fact that led Cohen to describe those who put it to infringing use as "patently stupid."[369] As Felten puts it, BitTorrent's creator "seems interested only in noninfringing uses, and has said all the right things about infringement—so consistently that one can only conclude he is sincere."[370]

But that is not to say that BitTorrent Inc. could not be found liable for inducement. The doctrine's real life application would be largely dependent on information that could only come to light after an exhaustive discovery process. It is quite possible that some smoking gun would be discovered supporting a finding of liability. Even in its absence, BitTorrent Inc. could still be held liable if rights holders were able to persuade courts to adopt a broad interpretation of inducement. For example, Ginsburg and Ricketson have suggested that the very prevalence of infringement facilitated by a particular technology may itself be evidence of intent.[371] If such a standard were to be adopted, a court may indeed find that BitTorrent Inc. has the requisite intent to induce infringement by virtue of its overwhelming number of infringing uses. In that case some other circumstances might be relevant in supporting that finding. For example, a technology called FurthurNet was launched a year before BitTorrent, and was also designed to facilitate sharing of jamband music.[372] Despite the unusually strong anti-infringement norms predominant in the jamband community, copyright infringement remains an ongoing problem. With that in mind, FurthurNet was designed to implement strict filtering protocols that limit distribution to those recordings and musicians who have agreed to permit it.[373]

The fact that such technology was released to a similar market at an earlier time may suggest that, by failing to include similar filtering technology in BitTorrent, Cohen intended it to be used for infringement. It may also be relevant that Cohen

367. *See P-to-P Goes Hollywood*, INFOWORLD (Jan. 1, 2007), http://www.infoworld.com/d/developer-world/p-p-goes-hollywood-620.

368. Jane C. Ginsburg, *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 586 (2008).

369. Seth Schiesel, *File Sharing's New Face*, N.Y. TIMES, Feb. 12, 2004, at G1.

370. Edward Felten, *BitTorrent: The Next Main Event*, FREEDOM TO TINKER (June 28, 2005, 5:26 AM), http://www.freedom-to-tinker.com/?p=859.

371. Ginsburg & Ricketson, *supra* note 63, at 7.

372. *See* Schultz, *supra* note 276, at 679, 685–86; *History of the Furthur Network and FurthurNet Software*, http://www.furthurnet.org/about/history.html (last visited Nov. 11, 2011).

373. Schultz, *supra* note 276, at 686.

created his software in a post-Napster, post-Kazaa world. Having experienced the phenomenon of those distribution technologies attracting millions of users and publicly facilitating billions of infringements, it must have been clear to him that it was that infringement that truly drove the "success" of the companies behind these technologies. These circumstances suggest that if Cohen wanted his technology to be a success, he wanted people to use it for infringement, and that might potentially be seen as evidence of intent. Thus, it's certainly possible that BitTorrent Inc. and its founder might be held liable for inducement.

4. So Why Haven't Content Interests Sued?

The above sketch demonstrates that, whilst the design of the BitTorrent technology appears to automatically rule out contributory and vicarious liability, it is at least arguable that a BitTorrent software provider such as BitTorrent Inc. could have been held liable for inducement. Even though liability is not clear cut, in light of the amount of infringement facilitated by BitTorrent and the past pattern of success against P2P providers in similar circumstances, content interests might have been expected to pursue an expansionist litigation strategy, hopeful of finding some smoking gun that might persuade a court to find liability. But they have not done so. Not a single BitTorrent software provider has ever been sued for the infringements of its users. The underlying reasons for that omission are the key to the industry's abandonment of the secondary liability campaign against P2P software providers, and this is where the mismatch between physical world assumptions and software world realities again comes into play.

All three of the physical world assumptions identified above are premised on the idea that that not just anyone could or would be able to create a technology capable of widespread copying or distribution. As discussed throughout this Article, for a long time it was universally true that it was expensive to develop a distribution technology capable of facilitating widespread infringement from inception to market, that the individuals involved were thus looking to make a profit or at least recoup their costs and that they were not keen to give away their technology's secrets. Each of these realities of physical world manufacturing contributed to keeping the number of market entrants relatively few. Combined, as noted above, they made the gatekeeper enforcement model an effective means of controlling large scale infringement. The universality of these assumptions may have been reinforced by the fact that they can and indeed often do hold in the software context—just think of the business models of Microsoft, Adobe and Apple. But, as BitTorrent demonstrates, they can and have been dramatically diverted from, with significant, though under-recognized, consequences.

It is now well recognized that existing secondary liability doctrines are premised on the idea that there is a limited number of gatekeepers that can be utilized to deter end user infringement, and that gatekeeper liability regimes work less well in the era of code-based distribution technologies where tens of millions of individuals

have the ability to quickly and cheaply make perfect copies.[374] Wu has compellingly argued that developers of code-based P2P file sharing technologies have exploited this weakness of the gatekeeper structure by eliminating intermediaries in order to avoid copyright's traditional enforcement measures.[375] However, there is an additional nuance that needs to be recognized: the difference in the efficacy of gatekeeper enforcement regimes when applied to open source versus closed source technologies. Gatekeeper enforcement regimes undeniably work less well in circumstances where the ability to make perfect copies is in the hands of many. But they work considerably less well still when the ability to create the *tools* necessary to make those copies becomes widely dispersed.

Consider a proprietary P2P protocol like FastTrack, as implemented by Kazaa and other licensed clients. That technology's source code was always very tightly guarded by its various owners.[376] Although at one point it was licensed to Grokster Ltd. and StreamCast Networks Inc., Sharman retained the ability to lock them out of its network, and they did not have access to its source code.[377] The decentralized nature of the technology meant that existing FastTrack clients could not be forced out of circulation. However, a finding of liability can have some impact even in a situation involving a technology that cannot be "switched off." For example, its owners could certainly take measures to make it a less attractive tool for committing infringement, by effectively forcing upgrades upon its users (and incorporating filtering technologies into the new versions), and by ceasing development and support of the software.[378] Even if the technical design of the software prevents forced upgrades, the cessation of development would soon result in its becoming outdated and incompatible with the latest operating systems, resulting in abandonment by some and then most of its users, and inevitably reducing the amount of infringement facilitated by that software. Indeed that is effectively what transpired after FastTrack's operators settled with content interests in 2006.[379] A study of P2P traffic conducted by a German Internet traffic management and analysis organization in late 2006 found that FastTrack had "all but ceased to exist" in that market, with its share of the P2P market estimated at just 0.06%.[380]

Contrast this with an open source technology like BitTorrent. By releasing the

374. *See, e.g.*, Wu, *When Code Isn't Law*, *supra* note 4, at 709–16.

375. *Id.* at 716–17.

376. *See Universal Music Austl. Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289, 339–44 (Austl.) (regarding the secrecy with which the source code was guarded).

377. *Id.*

378. *See. id.* at 361–64 (regarding the ability of Sharman to force upgrades upon its users, and concluding that Sharman could "drive its users mad" through the repetitive use of messages requesting them to upgrade, and in that way "persuade" them to do so).

379. *See, e.g.*, Ted Bridis, *Makers of 'Kazaa' Settle Piracy Suits*, THE SEATTLE TIMES (July 27, 2006), http://community.seattletimes.nwsource.com/archive/?date=20060727&slug=webkazaaa27; *Record Industry, Kazaa Settle Music Case*, THE AGE (July 27, 2006), http://www.theage.com.au/news/National/Record-industry-Kazaa-settle-music-case/2006/07/27/1153816326356.html.

380. *P2P Survey 2006*, IPOQUE, http://www.ipoque.com/userfiles/file/p2p_survey_2006.pdf (last visited Nov. 11, 2011).

protocol document and source code of his original client, Cohen put the power to create programs capable of facilitating vast amounts of infringement into the hands of an unlimited number of developers. Because of the negligible investment needed to follow those instructions and create a compatible client, many have taken up the implied invitation and done so—SourceForge alone typically hosts well over a hundred BitTorrent clients on its site, and almost four hundred BitTorrent related software projects in total, and there are scores more to be found elsewhere on the Internet.[381] Those clients are invulnerable to threats of vicarious and contributory liability because the technology does not give them the control over third party infringement that various physical world assumptions led the law to require. The potential liability of their providers is further limited by the fact that they have a relatively sophisticated understanding of the kind of behavior that will render them liable under other doctrines, and because the low development costs and intangible rewards from creating their own application mean they do not necessarily have the infringing business model that was so crucial to liability in *Grokster*.[382] As a result, they are unlikely to be liable for inducement or authorization.

To tease out the implications of a finding of liability, however, assume that some incriminating evidence led to a BitTorrent software provider being held liable for inducement or authorization. When a similar finding was made against the closed source FastTrack technology, it rapidly brought about its virtual disappearance from the marketplace.[383] But even if such evidence of intent against one BitTorrent developer led to its being held liable for inducement or authorization, it does not follow that BitTorrent technology generally would be similarly removed. Although a court might order a specific developer to stop distributing, developing and supporting its own particular client, it could and would do nothing to prevent new implementations of precisely the same technology from appearing and filling the gap. And since authorization and inducement attach to culpable behavior rather than anything inherent to the technology itself, a finding of liability would do nothing to prevent other BitTorrent developers from continuing support and development of their own virtually identical implementations of the same technology.[384]

This is ultimately why content interests abandoned their litigation campaign against P2P software providers. It was not because there were no providers left, or because P2P file sharing had stopped being of great concern to rights holders. It was because they realized that, even if they managed to successfully sue a company such as BitTorrent Inc., it would have had no real impact on the amount of third

381. *See, e.g.*, *Software Search*, SOURCE FORGE, http://sourceforge.net/softwaremap/?&fq[]=trove:251&fq[]=trove:622 (follow "Communications" hyperlink; then follow "file sharing" hyperlink; then follow "BitTorrent" hyperlink).

382. Fred von Lohmann, *What Peer-to-Peer Developers Need to Know About Copyright Law*, ELECTRONIC FRONTIER FOUNDATION (Jan. 2006), http://w2.eff.org/IP/P2P/p2p_copyright_wp_v5.pdf.

383. *See Universal Music Austl. Pty Ltd. v Sharman License Holdings Ltd.* [2005] 65 IPR 289 (Austl.). *See also* discussion *infra* at 113.

384. Giblin, Code Wars, *supra* note 18, at 159–61 (discussing the potential liability of torrent trackers and hosts).

party infringement facilitated by the BitTorrent file sharing technology in general. This was an inevitable consequence of a combination of a number of software world realities, particularly Cohen's willingness to share the technology's secrets in the first place, but also the low development costs and associated lack of imperative to profit from resulting infringement enjoyed by later comers. In those circumstances, the gatekeeper enforcement regimes of the U.S. and Australian copyright laws were of little utility, and further litigation was clearly useless. This might have been the type of situation that Lessig was hinting at, albeit in a slightly different context, when he argued that open code is harder to regulate than closed.[385] After all, gatekeepers aren't much help when they're the one punching the holes in the wall.

V. CONCLUSIONS: SERIOUS AND UNINTENDED CONSEQUENCES

The P2P cases decided over the last decade have had three main outcomes. Firstly, they resulted in large scale commercial P2P operators being almost entirely forced out of the market, although in the case of some—like Kazaa and LimeWire—this occurred so slowly that their technologies had already been superseded and most profits extracted before the death knell sounded. Secondly, they brought about the corresponding proliferation of independent, legally sophisticated operators whose software facilitates precisely the same result, but in a manner that is unlikely to render them liable under existing law. Finally, they led to the quiet abandonment of the litigation campaign against P2P providers in favor of targets higher up the food chain, including the ISPs who control access to the Internet and even the fabric of the Internet itself.

In the U.S., these measures have included negotiating partnerships with individual ISPs to assist with enforcement against end users, lobbying for increased legal obligations to filter for infringing content, and seeking the introduction of controversial government powers that would allow the Federal Attorney General to seize and block domain names associated with infringing content.[386] In Australia,

385. Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 764–67 (1999) (arguing that "[w]hether government can regulate code depends in part upon who controls that code. If the code is closed—controlled by private for-profit organizations—then government's power is assured. But if the code is open—outside of the control of any particular private for-profit organization—then the government's power is threatened. The more application space code is open code, the less government can regulate that code.").

386. *See, e.g.*, Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1; Nate Anderson, *RIAA Graduated Response Plan: Q&A with Cary Sherman*, ARS TECHNICA (Dec. 21, 2008, 5:54 PM), http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars; Steve Knopper, *RIAA's Gaze Turns from Users to ISPs in Piracy Fight*, ROLLING STONE (Dec. 19, 2008), http://www.rollingstone.com/music/news/14844/94542. *See also* Nate Anderson, *MPAA Head Wants Deeper Relationship (Read: Content Filtering) with ISPs*, ARS TECHNICA (Sep. 19, 2007), http://arstechnica.com/news.ars/post/20070919-mpaa-head-wants-deeper-relationship-read-content-filtering-with-isps.html. The government powers were originally intended to be enacted via the Combating Online Infringement and Counterfeits Act, which Govtrack reports was supported by content interests including the Motion Picture Association of America, Screen Actors Guild and Property Rights Alliance. *See S. 3804: Combating Online Infringement and*

rights holders took advantage of the broad scope of the authorization doctrine (and the narrowness of the complementary safe harbor) by suing an ISP for authorizing its users' infringements, possibly with the aim of pressuring Australian ISPs to agree to a general code of conduct addressing responses to copyright infringement.[387] That matter is still making its way through the appeal process.[388] Globally they have included lobbying for the introduction of "graduated response" or "three strikes" laws in a number of jurisdictions, as well as (unsuccessfully) seeking their inclusion in the recently finalized international Anti-Counterfeiting Trade Agreement (ACTA).[389]

These outcomes have all been driven by the secondary liability law's susceptibility to exploitation of the physical world/software world divide, and its continued inability to recognize and respond to the ways in which P2P file sharing software differs from predecessor distribution technologies. That inability is not altogether surprising given that the P2P cases decided to date have involved litigants that, thanks to their largely closed source code and infringement reliant business models, positively reinforced those assumptions. As has been seen, however, the realities of P2P software development can be very different from those of their physical world counterparts, and the failure to take those realities into account in determining legal responses has had serious and unintended consequences.

In response to *Grokster*, Zittrain predicted in 2006 that the existence "of software authors willing to code and release file sharing software without any business model at all" would mean that P2P distribution software "w[ould] continue to exist even if it c[ould not] be marketed formally, much less marketed as a pirate's tool."[390] That is precisely what has occurred. The shakeout of commercially oriented P2P software providers demonstrated the success of the Supreme Court's inducement framework in removing commercial enterprises whose business models relied on infringement. At the same time, however, there has been exponential growth of small noncommercial providers that have no infringing business model (or indeed any business model at all), but that have put

Counterfeits Act, GOVTRACK, http://www.govtrack.us/congress/bill.xpd?bill=s111-3804 (last visited Sept. 26, 2011). However, it never became law. A second attempt is currently wending its way through the legislative process in the form of the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act. Govtrack records its supporters as including Microsoft, the MPAA, the RIAA, the Independent Film & Television Alliance and the National Association of Theater Owners. *See S. 968: Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*, GOVTRACK, (Sept. 24, 2011, 6:20 AM), http://www.govtrack.us/congress/bill.xpd?bill=s112-968.

387. The decision of the trial judge largely rejected the claims of the applicants. *See Roadshow Films Pty Ltd. v iiNet Ltd. (No 3)* 2010 FCA 24 (Austl.).

388. On appeal, the full Federal Court also found in favor of the ISP, but gave considerable comfort to the applicants regarding their prospects in future claims, in the event that ISPs did not do more to respond to infringement claims in future. *See Roadshow Films Pty Ltd. v iiNet Ltd.* 2011 FCAFC 23 (Austl.). The matter is currently awaiting ultimate appeal to the High Court of Australia.

389. *See infra* note 10; *see also* David Kravets, *ACTA Backs Away from 3 Strikes*, WIRED (Apr. 21, 2010), http://www.wired.com/threatlevel/2010/04/acta-treaty/.

390. Zittrain, *supra* note 44, at 292.

out software that is just as capable of facilitating infringement as that of their predecessors.[391] Since there is no need for substantial investment, there is no need to recoup that investment, and as a consequence, those "checks and balances" inherent to physical world development can be almost entirely absent.[392] This is the reality of current P2P software development, which is simply not recognized by the existing law—even by those principles that were specifically crafted in response to P2P technologies.

Legal scholarship has touched upon the distinctions between software worlds and physical worlds in several different contexts, particularly in considering whether and how computer software should be provided with patent and copyright law protection, and while considering the jurisdictional and choice of law difficulties associated with enforcing laws in cyberspace.[393] However, their implications remain poorly understood. It is not surprising that we are slow to acknowledge the revolutionary properties of code. As Katsh explains, new technologies have historically been "perceived not as something with unique characteristics that will create new institutions and change old ones, but rather as something that simply extends the capabilities of . . . existing technolog[ies]."[394] Thus "early films were labeled 'moving pictures' and were not immediately understood to be a new art form," "the first cars were called 'horseless carriages' and looked as though they were designed to be pulled by a horse," and early personal computers "were called 'typewriters with memory.'"[395] As Katsh explains, the danger of equating unlike technologies is that it may "mask the revolutionary character of the new technology."[396] In turn, this can lead to legal standards that miss their targets because they fail to take into account the properties of the new innovation that make them unique. As this Article has demonstrated, that is exactly what has occurred with regard to P2P file sharing software.

This Article has told the story of the beginning of the P2P file sharing era,

391. *See supra* note 9 (showing huge growth in the number of open source file sharing applications between 2007 and 2008); pp. 101–102 (discussing the lack of business model adopted by the providers of many such technologies).

392. *See* Ganley, *supra* note 49, at 22.

393. *See, e.g.*, Jane C. Ginsburg, *Four Reasons and a Paradox: The Manifest Superiority of Copyright over Sui Generis Protection of Computer Software*, 94 COLUM. L. REV. 2559 (1994); Greubel, *supra* note 33; Robert Plotkin, *Computer Programming and the Automation of Invention: A Case for Software Patent Reform*, 2003 UCLA J.L. & TECH. 7 (2003); Pamela Samuelson, *Contu Revisited: The Case Against Copyright Protection for Computer Programs in Machine-Readable Form*, 1984 DUKE L.J. 663 (1984); John Swinson, *Copyright or Patent or Both: An Algorithmic Approach to Computer Software Protection*, 5 HARV. J.L. & TECH. 145 (1991). *See also* Lipton, *IP's Problem Child*, *supra* note 306 (canvassing more recently some of the practical realities of software development that she argues makes it "unsuitable" to provide copyright protection to the underlying source code). *See, e.g.*, BIEGEL, *supra* note 38, at 25–49; David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

394. M. ETHAN KATSH, LAW IN A DIGITAL WORLD 135 (1995).

395. *Id.* at 24, 135 (citing JAMES MARTIN, HYPERDOCUMENTS AND HOW TO CREATE THEM 9 (1990)).

396. *Id.* at 136.

tracing the way in which the law and technology evolved in response to efforts by rights holders to end the resulting infringement, and explaining how, after a decade of ostensibly successful litigation, there came to be more P2P file sharing software providers than ever before. It unmasked the revolutionary nature of software code, and highlighted how the physical world assumptions on which the existing law is based cripple its ability to respond to the P2P phenomenon. My recently published book, *Code Wars: 10 Years of P2P Software Litigation*, more completely chronicles the history of the P2P file sharing litigation era, and goes on to ask whether the secondary liability law can be reformulated in a way that better responds to the challenges posed by code-based distribution technologies.[397] If you're interested in continuing the story, please refer to the book.

397. REBECCA GIBLIN, CODE WARS: 10 YEARS OF P2P SOFTWARE LITIGATION (2011).