RUTGERS LAW JOURNAL

VOLUME 40

SPRING 2009

NUMBER 3

WHY PIRATES (STILL) WON'T BEHAVE: REGULATING P2P IN THE DECADE AFTER NAPSTER

*Annemarie Bridy**

Governing people, in the broad meaning of the word, governing people is not a way to force people to do what the governor wants; it is always a versatile equilibrium, with complementarity and conflicts between techniques which assure coercion and processes through which the self is constructed or modified by himself.
– Michel Foucault¹

INTRODUCTION

Napster went legit years ago. Grokster and Aimster are fading memories. And the once ubiquitous media coverage of peer to peer (“P2P”) file sharing has dwindled to occasional updates on legal and tech blogs. But hundreds of lawsuits, thousands of takedown notices, and millions of dollars later, victory

* Associate Professor, University of Idaho College of Law. The author would like to thank David Post and Clint Jeffery for comments on earlier drafts of this article and the Institute for Intellectual Property and Information Law at the University of Houston Law Center, which funded the project through its Sponsored Scholarship Grant Program. Thanks also to Axel Krings and participants in the University of Idaho CS (Computer Science) Colloquium, where portions of this article were presented.

1. Michel Foucault, *About the Beginning of the Hermeneutics of the Self: Two Lectures at Dartmouth*, 21 POL. THEORY 198, 203-204 (1993) (footnote omitted).

for the entertainment industry in the war on P2P remains elusive. Illegal music file sharing, notwithstanding the popularity of legal download services like iTunes, continues by all accounts at a robust rate, with *The Economist* reporting that for every one song that is legally purchased, about twenty are illegally downloaded.² For organizations like the Recording Industry Association of America (“RIAA”), this is a devastating statistic not only because it signifies a wealth of lost revenue, but also because it signifies a long-running failure of both public and private regulation. The news is not much better for movie distributors, whose hottest properties—including movies not yet released in theaters—are trafficked freely on P2P networks, thanks to warez traders.³ It seems that no matter what the entertainment industry does to try to stop them, pirates just won’t behave.

Among college students, who have historically embraced the culture of P2P with a level of enthusiasm and technical acumen surpassing that of any other demographic group, the latest P2P trend is swapping textbooks online.⁴ The controversies surrounding MP3 and DVD have accustomed most people to thinking of piracy strictly as a digital goods problem, but the rise of sites

2. Internet Piracy, *Thanks, Me Hearties: Media Firms Find That Statistics On Internet Piracy Can Be Rather Useful*, THE ECONOMIST, July 17, 2008, http://www.economist.com/business/displaystory.cfm?story_id=11751035. BigChampagne, a firm that monitors P2P traffic for major record labels and music industry magazines like *Billboard*, reported that the average number of simultaneous users on P2P networks was 9.35 million in 2007. ELECTRONIC FRONTIER FOUNDATION, *RIAA v. THE PEOPLE: FIVE YEARS LATER* 10 (Sept. 2008), <http://www.eff.org/files/eff-riaa-whitepaper.pdf>. The International Federation of the Phonographic Industry, a trade group, estimates that a staggering 95% of the music downloaded globally is downloaded illegally. See Eric Pfanner, *Global Music Sales Fell 7% in '08 as CDs Lost Favor*, NY TIMES, Jan. 17, 2009, <http://www.nytimes.com/2009/01/17/business/media/17music.html>.

Reliable estimates of P2P traffic are hard to come by, however, and there is reason to suspect the accuracy of estimates that emanate from the content industries themselves. See, e.g., Majid Yar, *The Global ‘Epidemic’ of Movie ‘Piracy’: Crime-wave or Social Construction?*, 27 MEDIA, CULTURE & SOC’Y 677, 690 (2005) (critiquing “official reliance on partial industry sources for ‘piracy’ figures,” and arguing that “[i]ndustry bodies have a vested interest in maximizing the figures” for lobbying purposes).

3. See, e.g., Eric Goldman, *The Challenges of Regulating Warez Trading*, 23 SOC. SCI. COMPUTER REV. 24, 26 (2005) (describing a prerelease copy of a movie as a “juicy trophy” for warez traders).

4. In the summer of 2008, web sites such as The Pirate Bay and Textbook Torrents began making college textbooks available in large numbers for free download, prompting fears among publishers that a new wave of online piracy had begun. See, e.g., Randall Stross, *First It Was Song Downloads. Now It’s Organic Chemistry.*, N.Y. TIMES, July 27, 2008 at BU4; Jeffrey R. Young, *On the Web, a Textbook Proliferation of Piracy*, CHRON. OF HIGHER ED., July 11, 2008 at IT1, available at <http://chronicle.com/free/v54/i44/44a00103.htm>.

like Textbook Torrents makes it clear that traditional print publishers are not being spared.⁵ In the summer of 2008, the site boasted 64,000 registered users and offered more than 5,000 scanned textbooks in PDF format.⁶ Its operator, a college student known only pseudonymously as “Geekman,” said in an interview that he considered his actions a form of “civil disobedience” in protest of “the monopolistic business practices of textbook publishers.”⁷ As print publishers in greater and greater numbers follow music and movie distributors into the world of digital distribution, the problem will become even more pressing.

What corporate rights owners might initially have conceived as an unwelcome but surmountable challenge to a viable business model has so radically altered the landscape of content distribution over the last decade that it now seems impossible to imagine a world without online file sharing. Since the birth of Napster in 1999, corporate rights owners have attempted to “govern” file sharing aggressively at three discrete points of intervention: the content level, the network level, and the user level. Their efforts have failed at each of these points, however, because they have failed to grasp Foucault’s insight, quoted above, that coercion alone cannot ensure compliance.

Sections I and II of this Article focus on content- and network-directed regulation, respectively, arguing that the coercive interventions undertaken at these levels have given rise to a variety of complications that militate against their long-term efficacy. Section III discusses user-directed regulation, arguing that the endurance of online piracy proves the inutility of industry efforts to reshape file sharing norms through educational programs that have been both punitive and propagandistic in character. The Article concludes by arguing that the effective solution to the problem of online piracy does not lie in *making* pirates behave—though some element of coercion will surely always be necessary to ensure compliance. Rather, the effective solution lies in addressing the underlying causes of noncompliance and the legitimate sources of consumer discontent. This entails an interrogation by rights owners of the extreme will-to-control that has permeated their responses to

5. See Young, *supra* note 4. Textbook Torrents was shut down shortly after it started, and it has since been taken over by a new administrator who provides access to free and cheaper textbooks, but not to torrents of pirated textbooks. There are, however, plenty of other torrent trackers that continue to provide access to pirated textbooks and other unauthorized book downloads. See, e.g., Alive Torrents, http://www.alivetorrents.com/cat/2/Books_torrents.html (last visited Dec. 7, 2009).

6. Young, *supra* note 4.

7. *Id.*

piracy at every level of intervention. It requires an approach to regulating piracy that takes for its goal the development and maintenance of a versatile equilibrium between *making* pirates behave and making them *want* to behave.

I. THE TROUBLE WITH REGULATING CONTENT: DRM'S BAD MAGIC

In 2003, Jack Valenti, then-president of the Motion Picture Association of America ("MPAA"), predicted that technology (i.e., digital rights management ("DRM")) would be the solution to a problem (i.e., P2P file sharing) that technology had created.⁸ "I'm trying," Valenti said, "to put in place technological magic that can combat the technological magic that allows thievery."⁹ The intuitive appeal of Valenti's isopathic logic, echoed in James Grimmelmann's observation that "digital media are at least the right sort of thing to be regulated with software, because they are themselves creatures of software,"¹⁰ has proven irresistible to corporate rights owners, who have made huge investments over the last ten years in regulating piracy at the level of content by means of "code."¹¹ The practical appeal of using bits to regulate bits is that regulation by code can be accomplished by rights owners, for rights owners, in precisely the way that rights owners want, without the need for recourse to a legal regime that most commentators agree has adapted less than nimbly to the challenge of protecting copyrights in the digital age.¹² The ultimate regulatory goal of DRM from the point of view of corporate rights owners is total control over the reproduction of digital content—a complete substitution of reliable computational rules for fuzzy legal standards like fair use.¹³

8. Interview by J.D. Lasica, with Jack Valenti, President, MPAA (Nov. 14, 2003), available at http://www.darknet.com/2005/06/interview_jack_.html.

9. *Id.*

10. James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1757 (2005).

11. In *Code Version 2.0*, Lawrence Lessig identified two types of "code" that serve a regulatory function in cyberspace: East Coast Code is "the 'code' that Congress enacts (as in the tax code or 'the U.S. Code')." . . . [West Coast Code] is the code that code writers 'enact'—the instructions imbedded in the software and hardware that make cyberspace work." LAWRENCE LESSIG, *CODE VERSION 2.0* 72 (Basic Books 2006).

12. See Julie E. Cohen, Lochner in *Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 471-73 (discussing the many ways in which DRM allows copyright owners an unprecedented level of control over content).

13. See Grimmelmann, *supra* note 10, at 1723 ("Along the traditional continuum between rules and standards, software lies at the extreme rule-bound end. Because a computer, rather than a person, makes a program's decisions, rules encoded in software are free from ambiguity, discretion, and subversion."); see also Yuval Feldman and Alon Harel, *Social*

Despite the entertainment industry's conviction that technology can fix what technology has broken, DRM has not solved the problem of piracy. Instead, content controls have been received by ordinary consumers as a frustrating impediment to lawful use (see Figure 1 below) and by hackers as both an affront to digital freedom and an opportunity to prove their mettle.

Figure 1: The DRM Dilemma¹⁴

Code, as it turns out, can break what code fixes.¹⁵ So when the entertainment industry chose to take on P2P file sharing at the level of code, it provoked an

Norms: Self-Interest and Ambiguity of Legal Norms: An Experimental Analysis of the Rule vs. Standard Dilemma, 4 REV. LAW & ECON. 81, 82 (2008) ("Legal norms may be divided into rules and standards. Rules are characterized by great specificity, as they define legal outcomes ex ante. Legal standards, on the other hand, are less specific, articulating open-ended tests whose precise content is only revealed ex post.").

14. XKCD: A Webcomic of Romance, Sarcasm, Math, and Language, *Steal This Comic*, <http://xkcd.com/488/>.

15. See, e.g., Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 682 (2003) (arguing that code functions not only as a regulatory mechanism, but as an anti-regulatory mechanism that can be used as a means of avoiding laws and "exploiting the internal dynamics of regulated groups"); Grimmelmann, *supra* note 10, at 1757 ("DRM systems encourage their own circumvention and hold up poorly in response to attack. . . . The plasticity of software

arms race with hackers that continues to escalate with every new iteration of content protection introduced into the marketplace.¹⁶ As the arms race has played out, a casual alliance has developed between hackers, many of whom openly disdain copyright laws, and ordinary consumers, who generally comply with copyright laws, but don't scruple at using software for circumventing DRM to enable what they believe to be legitimate personal uses of lawfully acquired content.¹⁷ Content distributors have fostered this alliance between the Lawless and the Merely Frustrated by placing the most draconian access and copy restrictions on seemingly everything they market in digital form, including public domain works.¹⁸

As a regulatory tool, DRM has proven to be a blunt instrument. The cartoon in Figure 1, above, illustrates the bind created by DRM for purchasers of music online who value the ability to build a music library over time and to access it across different operating systems, computers, and portable devices. The cartoon appeared on the Internet in the fall of 2008, around the time Wal-Mart announced that it would be taking its DRM servers off-line as part of a planned transition to a completely DRM-free music store.¹⁹ Wal-Mart's decision to power down its DRM servers, a decision the company promptly reversed after a consumer backlash, would have left those who had downloaded DRM-protected music from its store unable to transfer song files to an MP3 player or another computer without circumventing the DRM.²⁰ The moral of the cartoon is that consumers can't

makes it all too possible to write more software that handles the regulated media in a way the system regulating them cannot stop.”).

16. See, e.g., Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393, 402 (1999) (“The warfare analogy of a race between offense and defense comes readily to mind. For those who sympathize with content providers, one can view the copier as the attacker, with the content provider responding to copying by using ‘defensive’ self-help systems. Then offensive techniques will arise to overcome the defenses to copying (or to alteration) not authorized by the content provider, and so on ad infinitum.”).

17. See Mark F. Schultz, *Copynorms: Copyright Law and Social Norms*, in INTELLECTUAL PROPERTY AND INFORMATION WEALTH, 212-13 (2007) (Peter Yu, ed.) (discussing the effect of “hacker norms” and practices on people outside the hacker subculture).

18. See, e.g., Lessig 2.0, *This Is the Constitution on DRM*, available at <http://lessig.org/blog/> (Sept. 24, 2004, 13:23 EST) (describing copy controls applied to a digital version of the United States Constitution).

19. See Greg Sandoval, *How Long Before Wal-Mart Reverses Its DRM Decision?*, CNET NEWS.COM, Sept. 29, 2008, http://news.cnet.com/8301-1023_3-10053857-93.html.

20. See Posting of Scott Nichols to Today @ PC World, <http://blogs.pcworld.com/staffblog/> (Sept. 29, 2008, 12:25 EST). Wal-Mart notified customers of the plan via e-mail:

win for losing when it comes to DRM: you're damned if you pirate, and damned if you buy. Insofar as DRM locks digital content to specific devices and operating systems, and insofar as it requires sustained communication with remote servers beyond users' control, users risk losing access to legally purchased content if their systems crash, their device preferences shift, or market conditions change.²¹

Users have protected themselves from this risk by downloading backup programs like SharePod²² and CopyTrans,²³ which enable copying of DRM-protected files from an MP3 player to an unauthorized computer.²⁴ Such programs also enable file sharing, however, and their availability is legally

Beginning October 9, we will no longer be able to assist with digital rights management issues for protected WMA files purchased from Walmart.com. If you do not back up your files before this date, you will no longer be able to transfer your songs to other computers or access your songs after changing or reinstalling your operating system or in the event of a system crash. Your music and video collections will still play on the originally authorized computer.

Posting of Cory Doctorow to Boing Boing, <http://www.boingboing.net/> (Sept. 26, 2008, 20:34 EST).

Wal-Mart has since reversed the decision and now plans to keep its DRM servers online indefinitely. *See* Posting of Cory Doctorow to Boing Boing, <http://www.boingboing.net/> (Oct. 10, 2008, 2:41 EST) (discussing Wal-Mart's decision to keep its DRM servers online and quoting an email communication sent from Wal-Mart to its digital music customers).

21. Jonathan Zittrain sees the rise of "tethered appliances," playback devices that vendors can modify through software updates indefinitely and from afar, as a threat to the existing culture of consumer control over home-based technologies like PCs, DVRs, and DVD players. *See* JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* 106-07 (2008).

22. SharePod is described by its publisher as "a free program which allows you to easily and quickly share your iPod music collection with friends." With SharePod, users can back up and restore the entire contents of an iPod or copy individual tracks to and from the device. Jeff Harris, SharePod 3.9.3: Publisher's Description, SharePod – CNET download.com, http://www.download.com/SharePod/3000-2141_4-10794489.html?tag=mncol (last visited Nov. 29, 2009).

23. CopyTrans is described by its publisher as "the ultimate backup & recovery tool for your iPod & iPhone songs and videos." CopyTrans, <http://www.copytrans.net/> (last visited Dec. 7, 2009).

24. Since July 7, 2009, 63,727 copies of SharePod have been downloaded from CNET. *See* SharePod 3.9.3: Quick Specs, SharePod – CNET download.com, http://www.download.com/SharePod/3000-2141_4-10794489.html?tag=mncol (last visited Nov. 29, 2009). Since September 24, 2009, 299,311 copies of CopyTrans have been downloaded. *See* CopyTrans 3.29 Quick Specs, CopyTrans – CNET Download Statistics, http://www.download.com/CopyTrans/3000-2141_4-10426173.html?tag=mncol (last visited Nov. 29, 2009).

questionable under the Digital Millennium Copyright Act ("DMCA").²⁵ Section 1201 of the DMCA, which functions as a statutory buttress for DRM, divides DRM into two categories: measures that prevent unauthorized access to a copyrighted work ("access protection measures")²⁶ and measures that prevent the unauthorized exercise of one or more of an author's exclusive rights ("rights protection measures").²⁷ The provision also implicitly divides circumvention into two categories: individual acts of circumvention and the manufacture and distribution of tools that enable circumvention.²⁸ Under section 1201(a), both the individual circumvention of access protection measures and the distribution of tools for circumventing such measures are expressly prohibited.²⁹ Under section 1201(b), by contrast, the individual circumvention of rights protection measures is implicitly permitted, while the distribution of tools for circumventing such measures is expressly banned.³⁰

The differential treatment of the two categories of DRM with respect to individual acts of circumvention was intended by Congress to protect the public's fair use rights against potentially overzealous rights owners, who could use DRM not only on the front end to require lawful access to copyrighted works but also on the back end to abrogate fair use copying.³¹

25. See 17 U.S.C. § 1201 (2006) (establishing a legal framework for the regulation of DRM circumvention).

26. See *id.* § 1201(a)(1)(A) (governing the circumvention of "a technological measure that effectively controls access to a [copyrighted] work").

27. See *id.* § 1201(b)(1)(A) (governing the circumvention of "a technological measure that effectively protects a right of a copyright owner").

28. Section 1201(a) expressly bans individual acts of circumvention of access protection measures. See *id.* § 1201(a)(1)(A) (providing that "[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work"). It also bans the distribution of technologies designed to circumvent access protection measures. See *id.* § 1201(a)(2)(A) (providing that "[n]o person shall . . . traffic in any technology . . . that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted] work"). Section 1201(b) is silent as to individual acts of circumvention of rights protection measures, but it bans the distribution of technologies that may be used to circumvent rights protection measures. See *id.* § 1201(b)(1)(A) (providing that "[n]o person shall . . . traffic in any technology . . . that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner").

29. See *supra* note 28 and accompanying text.

30. See *supra* note 28 and accompanying text.

31. See 17 U.S.C. § 1201(c)(1) (expressly preserving "defenses to copyright infringement, including fair use"); see also U.S. COPYRIGHT OFFICE, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S. COPYRIGHT OFFICE SUMMARY (December 1998), <http://www.copyright.gov/legislation/dmca.pdf> (explaining that section 1201's distinction

The practical glitch with section 1201(b)'s apparent solicitude for fair use is that the provision protects the right of fair use at the same time as it effectively deprives the public of the tools it needs to exercise the right.³² Confronted with this anomaly, courts have interpreted section 1201(b) as a blanket ban on the distribution of DRM circumvention tools, no matter if the tools are put to "legal downstream uses" by individual consumers.³³ So, while the DMCA theoretically permits an individual to circumvent DRM to make fair use of a lawfully accessed copyrighted work, it has been held to simultaneously forbid the distribution of software that would enable such permissible circumvention.³⁴ The bottom line for users? They are permitted to circumvent DRM to engage in fair use of digital goods for access to which they have paid, but no one who actually knows *how* to circumvent DRM is permitted to give them the wherewithal to do it.

This seemingly paradoxical statutory framework has been applied by courts in cases involving DRM circumvention tools for eBooks³⁵ and DVDs.³⁶ In *United States v. Elcom*, a 2002 case that takes on renewed relevance in light of the growing popularity of Amazon's Kindle and other portable eBook readers, the defendant was the distributor of a DRM-stripping program known as the Advanced eBook Processor ("AEBPR").³⁷ The DRM that the AEBPR was designed to circumvent enabled the publisher of an eBook to prevent the book or any portion of it from being copied, printed, "lent" to one user by another on the same network, or viewed on any computer other than the one to which it was originally downloaded.³⁸ The court recognized that the defendant's software "enable[d] a purchaser of an

between access controls and copy controls "was employed to assure that the public will have the continued ability to make fair use of copyrighted works").

32. See *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085, 1097-98 (N.D. Cal. 2004) (holding that "legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)"); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1124 (N.D. Cal. 2002) (holding that "[s]ection 1201(b) imposes a blanket ban on trafficking in or the marketing of any device that circumvents use restrictions").

33. See *321 Studios*, 307 F. Supp. 2d at 1097-1098; *Elcom*, 203 F. Supp. 2d at 1124.

34. See *Elcom*, 203 F. Supp. 2d at 1120 (explaining that, in section 1201(b), "Congress did *not* ban the act of circumventing the use restrictions. . . , [but] banned only the trafficking in and marketing of devices primarily designed to circumvent the use restriction protective technologies").

35. *Elcom*, 203 F. Supp. 2d 1111.

36. *Universal City Studios v. Corley*, 273 F.3d 429, 439-440 (2d Cir. N.Y. 2001); *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

37. 203 F. Supp. 2d at 1118-19.

38. See *id.* at 1117-18.

ebook to engage in 'fair use' of an ebook without infringing the copyright laws, for example, by allowing the lawful owner of an ebook to read it on another computer, to make a back-up copy, or to print the ebook in paper form."³⁹ The court pointed out, however, that the AEBPR "allow[ed] a user to engage in copyright infringement by making and distributing unlawful copies of the ebook."⁴⁰ When the eBook DRM was *on*, it prevented fair use; when it was *off*, there was no preventing infringement. There was no middle ground. Faced with a choice between enabling fair use and preventing infringement, the courts interpreted the DMCA to prefer the latter. Even though eBook owners were within their rights under the DMCA to do many of the things that the AEBPR enabled and the DRM blocked, the defendant's attempt to aid eBook owners in the exercise of their rights was held to violate the statute.⁴¹

The story of DRM for DVDs—the Content Scrambling System ("CSS")—is another example of what happens when the "extreme ruleishness"⁴² of DRM collides with consumers' preference for flexibility in the personal use of digital content. CSS encrypts the content on DVDs to keep them from being played in non-licensed machines.⁴³ In early 2000, a 16-year-old Norwegian programmer named Jon Lech Johansen was indicted in Norway for posting code on the Internet that could be used to crack CSS.⁴⁴ He had developed the program, which he called "DeCSS," in late 1999 by reverse engineering a licensed DVD player.⁴⁵ DeCSS allowed users to unlock CSS encryption so that DVDs could be played using unlicensed

39. *Id.*

40. *Id.* at 1119.

41. *Id.* at 1140-41.

42. Grimmelmann, *supra* note 10, at 1724.

43. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 309-10 (S.D.N.Y. 2000). CSS involves encrypting, according to an encryption algorithm, the digital sound and graphics files on a DVD that together constitute a motion picture. A CSS-protected DVD can be decrypted by an appropriate decryption algorithm that employs a series of keys stored on the DVD and the DVD player. In consequence, only players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs.

Id.

44. See J.S. Kelly, *Meet the Kid Behind the DVD Hack*, CNN.COM, Jan. 31, 2000, <http://archives.cnn.com/2000/TECH/computing/01/31/johansen.interview.idg/>; Steve Stecklow, *Repro Man – Meet the 21-Yr-Old Norwegian Who Defied Hollywood to Help the World Copy DVDs – And Beat the Studios in Court; Now He's Liberating your iPod*, WALL ST. J., Oct. 15, 2005, at A1.

45. Stecklow, *supra* note 44.

hardware.⁴⁶ More problematically for the movie industry, it also allowed viral distribution of decrypted copies of motion pictures.⁴⁷

Johansen wrote the code, he said, not to promote piracy or even to enable copying, but because he wanted to be able to play DVDs on a computer running the Linux operating system.⁴⁸ There was no way for him to do so without cracking CSS.⁴⁹ What Johansen wanted to do probably wouldn't strike most people as legally or morally questionable: he wanted to play—not copy, just play—a lawfully acquired DVD on a lawfully acquired machine (his computer) that happened not to be licensed by the DVD Copy Control Association (“CCA”), which administers the CSS system on behalf of the entertainment industry.⁵⁰ He also wanted to help other, less technologically savvy people do the same thing, which he did by posting DeCSS on the Internet.⁵¹

Beyond the reach of the DMCA in Norway, Johansen was acquitted of the charges brought against him under Norwegian law.⁵² Two U.S.-based

46. See Kelly, *supra* note 44.

47. See DAVID NIMMER, COPYRIGHT ILLUMINATED: REFOCUSING THE DIFFUSE U.S. STATUTE 341 (2008).

48. See Kelly, *supra* note 44. Johansen testified in the *Reimerdes* case concerning his motives for creating DeCSS, but the court was not persuaded:

Moreover, the Court does not credit Mr. Johansen's testimony that he created DeCSS solely for the purpose of building a Linux player. Mr. Johansen is a very talented young man and a member of a well known hacker group who viewed “cracking” CSS as an end in itself and a means of demonstrating his talent and who fully expected that the use of DeCSS would not be confined to Linux machines. Hence, the Court finds that Mr. Johansen and the others who actually did develop DeCSS did not do so solely for the purpose of making a Linux DVD player if, indeed, developing a Linux-based DVD player was among their purposes.

Reimerdes, 111 F. Supp. 2d at 320.

49. See *Reimerdes*, 111 F. Supp. 2d at 309-10 (explaining how CSS works).

50. See DVD CCA, Frequently Asked Questions, <http://www.dvdcca.org/faq.html> (last visited Dec. 7, 2009):

The DVD Copy Control Association (DVD CCA) is a not-for-profit corporation with responsibility for licensing CSS . . . to manufacturers of DVD hardware, discs and related products. Licensees include the owners and manufacturers of the content of DVD discs; creators of encryption engines, hardware and software decrypters; and manufacturers of DVD Players and DVD-ROM drives.

Id.

51. See Kelly, *supra* note 44. The DVD CCA has since licensed the distribution of a Linux-based DVD player. See DVD CCA, Frequently Asked Questions, <http://www.dvdcca.org/faq.html> (last visited Dec. 7, 2009) (stating that Sigma Designs is now marketing a DVD player for Linux under its license to manufacture products using CSS).

52. Jillian Law, *Defendant Acquitted in DVD Hacking Case*, PC WORLD, Jan. 7, 2003, http://www.pcworld.com/article/108462/defendant_acquitted_in_dvd_hacking_case.html.

distributors of DeCSS fared less well, having run afoul of the interpretation of section 1201 that proscribes trafficking in code that circumvents DRM, even for fair use purposes.⁵³ In 2000, eight film studios sued and won injunctions against Eric Corley and Shawn Reimerdes, programmers who had posted the code on their own web site.⁵⁴ In the same year, the Copyright Office considered in a round of rulemaking⁵⁵ whether DeCSS software should be exempted from the DMCA's prohibition on circumvention to allow consumers to play DVDs on Linux machines.⁵⁶ It denied the exemption, reasoning that "there is no unqualified right to access works on any particular machine or device of the user's choosing. . . . [Thus,] an exemption to benefit individuals who wish to play their DVDs on computers using the Linux operating system does not appear to be warranted."⁵⁷ Tough luck for Linux users—or maybe not: Even though the exemption was denied, programs allowing users to circumvent CSS remained freely available on the Internet,⁵⁸ to be supplemented only belatedly by a CCA-authorized player for Linux.⁵⁹ Where content providers and government regulators have failed to respond promptly to consumer demand for flexibility with respect to how, when, and on what devices copyrighted content is viewed, consumers have turned again and again to the Internet for a little help from their hacker friends. And court orders notwithstanding, they keep finding it.

After distributing DeCSS in 1999, Johansen went on to hack Apple's iTunes Fair Play DRM system and to distribute a free desktop client called DoubleTwist that allows digital files to be freely ported to online social

53. See 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1097-1098 (N.D. Cal. 2004) (hold

ing that "legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)").

54. See Universal City Studios v. Corley, 273 F.3d 429, 436 (2d Cir. N.Y. 2001); Reimerdes, 111 F. Supp. 2d at 303-04, n.2.

55. See 17 U.S.C. § 1201(a)(1)(C). Under the DMCA, the Librarian of Congress is required every three years to consider the necessity for exemptions to the anti-circumvention provisions in section 1201. *Id.*

56. See Supplementary Information, 65 Fed. Reg. 64,568-69 (Oct. 27, 2000).

57. *Id.* at 64,569.

58. See, e.g., DVD Decrypter, <http://www.mrbass.org/dvdrrip/> (last visited Nov. 29, 2009); Freez DVD Ripper, <http://www.smallvideosoft.com/dvd-ripper/> (last visited Nov. 29, 2009); HandBrake, <http://handbrake.fr/> (last visited Nov. 29, 2009).

59. See DVD CCA, Frequently Asked Questions, <http://www.dvdcca.org/faq.html> (last visited Dec. 7, 2009) (stating that Sigma Designs is now marketing a DVD player for Linux under its license to manufacture products using CSS).

networking sites and a wide range of media and playback devices.⁶⁰ To his lawyer's dismay, Johansen was already at work cracking Fair Play when the retrial of his criminal case involving DeCSS began in Norway in 2003.⁶¹ And in a development that might have caused even an optimist like Valenti to doubt the invincibility of DRM, Hollywood's Advance Access Content System ("AACs"), the next generation of DRM for HD DVDs and Blu-Ray discs, was compromised within a year of its introduction—using an Xbox 360, a computer, and a copy of *King Kong*.⁶²

DRM systems have become supplier since the DeCSS debacle. Manufacturers of licensed playback devices can now periodically push software updates to devices already in the hands of consumers.⁶³ These updates revoke cracked keys and replace them with new, secure ones.⁶⁴ Although this two-way communication between user-owned devices and their manufacturers has slowed hackers in their efforts to crack AACs, most commentators believe that it is only a matter of time until AACs, like its predecessor, is definitively cracked.⁶⁵ The fact that every "next generation" DRM system deployed so far has been cracked exposes Valenti's thinking about technological magic for the magical thinking that it is.⁶⁶

60. Posting of Erica Ogg to CNET News Blog, <http://news.cnet.com/> (Feb. 18, 2008, 21:00 PST).

61. See Stecklow, *supra* note 44.

62. Bobbie Johnson, *Hollywood faces up to DRM flop*, THE GUARDIAN, Feb. 22, 2007, at Tech. 1; Posting of Ken Fisher to Ars Technica, <http://arstechnica.com/> (Jan. 26, 2007, 9:23 EST). Reports that the standard had been hacked began circulating on the Internet just before the end of the year in which it was introduced. See Johnson, *supra*; see also Press Release, AACs, Response to Reports of Attacks on AACs Technology (February 21, 2006), available at <http://www.aacsla.com/press/> (stating that the consortium of manufacturers that developed the AACs standard introduced it in a press release in February 2006).

63. See Posting of Jeremy Reimer to Ars Technica, <http://arstechnica.com/> (Apr. 7, 2007, 20:06 EST) (reporting on the release of a mandatory update for users of the InterVideo DVD player).

64. See John Leyden, *Latest AACs Crack 'Beyond Revocation'*, THE REGISTER, May 4, 2007, http://www.theregister.co.uk/2007/05/04/aacs_crack/ ("The technology includes a system for revoking keys, making it impossible to play newly released high-definition movies via versions of playback software known to be weak or flawed."). Undeterred, hackers have taken a brute force approach to getting around AACs that involves removing and reading firmware chips from Xboxes and resoldering the chips onto the motherboards from which they were removed. *Id.* Although this approach voids hardware warranties and is technically difficult, "it takes hackers one step closer to using software to achieve the same ends." *Id.*

65. See *id.*

66. See SIR JAMES FRAZER, THE GOLDEN BOUGH: A STUDY IN MAGIC AND RELIGION 44 (1922):

The fundamental technical problem with DRM as a regulatory mechanism is that its “magic” relies, at base, on a cryptographically sophisticated but conceptually primitive system of locks and hidden keys. Apple’s Steve Jobs, who has argued consistently that DRM will ultimately prove futile to prevent piracy, has explained this flaw:

There is no theory of protecting content other than keeping secrets. In other words, even if one uses the most sophisticated cryptographic locks to protect the actual music, one must still “hide” the keys which unlock the music on the user’s computer or portable music player. No one has ever implemented a DRM system that does not depend on such secrets for its operation.⁶⁷

The fundamental normative problem with DRM as a regulatory mechanism is that it prevents users from doing what they *should* be able to do in order to keep them from doing what they *shouldn’t*. The court in *Reimerdes* recognized that DRM has “the capacity to prevent fair uses of copyrighted works as well as foul.”⁶⁸ This failure to discriminate is countenanced by the DMCA, but it fundamentally delegitimizes DRM in the eyes of many consumers, who take little comfort in judicial conclusions that “[f]air use is still *possible* under the DMCA, although such copying will not be as easy, as exact, or as digitally manipulable”⁶⁹ as they might wish.

For it must always be remembered that every single profession and claim put forward by the magician as such is false; not one of them can be maintained without deception, conscious or unconscious. Accordingly the sorcerer who sincerely believes in his own extravagant pretensions is in far greater peril and is much more likely to be cut short in his career than the deliberate impostor. The honest wizard always expects that his charms and incantations will produce their supposed effect; and when they fail, not only really, as they always do, but conspicuously and disastrously, as they often do, he is taken aback.

Id.

67. Steve Jobs, *Thoughts on Music* (Feb. 6, 2007), <http://www.apple.com/hotnews/thoughtsonmusic/>; see also Posting of Jeremy Reimer to Ars Technica, <http://arstechnica.com/> (Apr. 15, 2007, 00:30 EST) (“The real problem with trying to create an ‘uncrackable’ copy protection is that the media must come with the keys used to decrypt it somewhere on the device and the media itself. Hiding these keys in different places—security by obscurity—merely delays the inevitable.”).

68. *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 304 (S.D.N.Y. 2000). The court went on to explain that Congress made a policy choice when it enacted the DMCA “to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so.” *Id.* at 324.

69. *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085, 1102 (N.D. Cal. 2004) (emphasis added).

Even as the Copyright Office denied the exemption sought for DeCSS in 2000, it acknowledged that Congress probably didn't anticipate when it enacted the DMCA "that persons who legitimately acquired copies of works should be denied the ability to access these works."⁷⁰ Short of a wholesale denial of access, however, consumers have been held not to deserve relief from DRM, and the facilitation of fair use has been held not to be a defense for distributors of software that circumvents it.⁷¹ Although the anti-circumvention provisions of the DMCA have been aggressively enforced by corporate rights owners and repeatedly upheld by courts,⁷² proponents of DRM have been learning the hard way that wrapping vulnerable "west coast code"⁷³ in a protective shell of "east coast code"⁷⁴ has done little to either protect or legitimate it.

DRM for protecting music has proven no more effective or palatable to consumers than DRM for protecting movies. It can be stripped from protected music files sold online using publicly available software tools such as SoundTaxi.⁷⁵ As for prerecorded CDs, they are sold through retail channels without any DRM at all. It's not that rights owners didn't try to deploy DRM to protect prerecorded music CDs; they did, but with very poor results. The most infamous industry mishap concerning DRM for prerecorded music CDs has come to be known as the Sony BMG Rootkit Incident.⁷⁶

In 2005, computer security expert Mark Russinovich discovered that DRM-protected CDs distributed by Sony BMG Music Entertainment surreptitiously installed software known as a rootkit on the hard drives of

70. Supplementary Information, 65 Fed. Reg. 64,569 (Oct. 27, 2000).

71. *Macrovision v. Sima Prods. Corp.*, 2006 WL 1063284 at 3 (S.D.N.Y. Apr. 20, 2006) (stating that "Sima's defense that it only intends to enable 'fair use' copying of copyrighted works is no defense at all," because "the DMCA provides no exception to its prohibition of the manufacture of these devices").

72. *Universal City Studios v. Corley*, 273 F.3d 429, 434-35 (2d Cir. 2001); *Paramount Pictures Corp. v. 321 Studios*, 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004) ("[M]anufacturing and distributing DeCSS software for sale violates the anti-trafficking provisions of the DMCA"); *321 Studios*, 307 F. Supp. 2d at 1098; *Reimerdes*, 111 F. Supp. 2d at 325.

73. LESSIG, *supra* note 11, at 72.

74. *Id.*

75. See SoundTaxi, How to Strip DRM Off From iTunes MP4, <http://www.soundtaxi.us/how-to-strip-drm-off-from-itunes-m4p.html> (last visited Nov. 29, 2009).

76. See Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157 (2007) (discussing in detail the technical and legal ramifications of Sony's deployment of a rootkit in connection with DRM for prerecorded audio CDs).

consumers who played the CDs in their computers.⁷⁷ When Russinovich attempted to remove the rootkit from his own system, it disabled his CD-ROM drive.⁷⁸ The rootkit was designed to secretly communicate information to Sony BMG about the computer users playing the CDs.⁷⁹ In doing so, it compromised the security of the computers on which it was installed, making them vulnerable to malicious attacks by third parties.⁸⁰ Attorneys for the Electronic Frontier Foundation (“EFF”) characterized the rootkit as spyware.⁸¹ News that Sony CDs were being shipped with rootkits that installed automatically and masked their own presence spread quickly over the Internet, and the incident came under investigation by the Federal Trade Commission (“FTC”) and law enforcement officials in forty-two states.⁸²

In addition to the government investigations, numerous class action lawsuits were filed on behalf of consumers from New York to California.⁸³ The incident was a public relations disaster for Sony BMG.⁸⁴ Under the terms of the agreement hastily adopted to settle the civil suits, the company promised to stop manufacturing CDs with the DRM software, to recall all affected CDs already in the supply chain, to provide an uninstaller for consumers whose computers were affected, and to provide “clean” replacement CDs to consumers who had bought CDs containing the DRM.⁸⁵

77. See John Bowman, *Sony and the Rootkit*, CBC NEWS, Nov. 10, 2005, <http://www.cbc.ca/news/background/tech/rootkit.html>.

78. *Id.*

79. See Mulligan & Perzanowski, *supra* note 76, at 1167 (explaining that “[t]he ‘phone home’ feature of Sony BMG’s DRM undermined customer privacy by collecting and transmitting information about users’ interactions with protected CDs, including users’ IP addresses”).

80. *Id.* at 1166 (pointing out that “[p]ractically any malicious code authored by a hacker could take advantage of [the] general purpose security holes” created by the rootkit).

81. Complaint at 11, *Hull v. Sony BMG Music Entertainment Corp.*, No. BC343385 (Cal. Super. Ct. Nov. 21, 2005), available at <http://www.sonysuit.com/classactions/eff/complaint.pdf>.

82. See Robert McMillan, *Sony Rootkit Settlement Reaches \$5.75M*, PC WORLD, Dec. 22, 2006, <http://pcworld.about.com/gi/dynamic/offsite.htm?site=http://www.pcworld.com/article/id,128310/article.html>.

83. See, e.g., Complaint, *Michaelson v. Sony BMG Music, Inc.*, No. 05-CV-09575 (S.D.N.Y. Nov. 14, 2005), available at <http://www.sonysuit.com/classactions/michaelson/complaint.pdf>; Hull Complaint, *supra* note 81.

84. See, e.g., Bowman, *supra* note 77 (describing how widely and quickly the story unfolded on tech blogs).

85. See Motion and Memorandum of Law in Support of Plaintiff’s Application for Preliminary Approval of Class Action Settlement at 1-2, *In re Sony BMG CD Technologies Litigation*, No. 1:05-cv-09575-NRB (S.D.N.Y. Nov. 14, 2005), available at http://www.eff.org/files/filenode/Sony-BMG/sony_prelim_approval_motion.pdf.

In addition to costs associated with the class action and FTC settlements, Sony agreed to pay the states \$5.75 million to end their investigations.⁸⁶ Thus ended efforts by corporate rights owners to protect prerecorded music CDs with DRM.⁸⁷

DRM for music downloads has suffered the same fate.⁸⁸ Online music distributors, including Amazon, Wal-Mart, and most recently and significantly Apple, have shifted to an entirely DRM-free distribution model.⁸⁹ This development is hard to interpret as anything but a concession by corporate rights owners that DRM for protecting music has been a regulatory failure. As Jonathan Zittrain has pointed out, most trusted systems have failed, either because sophisticated users have found a way to crack them, or because the market has rejected them.⁹⁰ If consumers remain willing to accept regulation by DRM at all, and there is good reason to doubt that they do, future forms will have to be less intrusive and less coercive in their operation than past forms have been.⁹¹ The way DRM systems are currently structured, “[users] can enjoy the content [they buy] within the software-regulated space created by the DRM system but cannot remove the content from that space.”⁹² DRM’s rigid prohibition on portability is at the core of the dilemma it presents for device users who aren’t satisfied to enjoy content for which they have paid within the narrow parameters dictated by a computer algorithm.

86. See McMillan, *supra* note 82.

87. See Bowman, *supra* note 77 (reporting that “[i]n response to all of the negative publicity it received over the copy-protection scheme, Sony BMG suspended its use as a ‘precautionary measure.’”).

88. See RONALD S. ROSEN, MUSIC AND COPYRIGHT 570-71 (2008) (tracing the music industry’s incremental retreat from DRM).

89. After having reached an agreement with the three major music distributors—Sony BMG, Universal Music Group, and Warner Music Group—Apple announced in January 2009 that it would no longer sell DRM-protected music through iTunes. See Brad Stone, *Copy an iTunes Song? Go Ahead Apple Says*, NY TIMES, Jan. 7, 2009 at B1. Steve Jobs, Apple’s CEO, had argued publicly that selling DRM-protected music online is futile in a world where most music is still purchased on DRM-free CDs. See Jobs, *supra* note 67.

90. ZITTRAIN, *supra* note 21, at 10.

91. David Hughes, head of the RIAA’s technology unit, said during a panel discussion at the Digital Hollywood conference in Spring 2008 that “[he] made a list of the 22 ways to sell music, and 20 of them still require DRM.” Posting of Greg Sandoval to CNET News Blog, <http://news.cnet.com/> (May 8, 2008, 09:06 PDT). At the same time, however, he acknowledged that consumers would prefer a less obtrusive form of DRM than currently exists. *Id.*

92. Grimmelmann, *supra* note 10, at 1752.

To the extent that DRM can function only by cabining the enjoyment of digital content in a “software-regulated space,” it will continue to clash—to its detriment—with the public’s desire for portability and mobility. People don’t want to watch movies only on their TVs at home; they also want to watch them on laptops, iPods, and other mobile devices in airports, hotels, and everywhere else. They don’t want their ability to watch a movie or hear a song to be limited to particular devices and operating systems approved by rights owners. DRM has failed as a regulatory mechanism in large part because it makes no allowance for the multiplicity of ways in which people now want to enjoy digital content. It makes no accommodation for fair use. It’s not coded to balance the interests of those who consume digital goods with the interests of those who produce them. Rather, it’s the product of a regulatory fantasy of perfect control by corporate copyright owners. As such, it has been rejected not only by scofflaw hackers, who supply many of the Internet’s free circumvention tools, but also by law-abiding consumers, who use those tools without scruple to decouple lawfully acquired content from the “authorized” file formats, machines, and operating systems to which DRM locks it. Consumers who prefer to be self-authorizing with respect to where and how they enjoy the digital goods they buy justifiably resent—and will continue to resist—the blindness of DRM to their legitimate interests.

II. THE TROUBLE WITH REGULATING NETWORKS: OUT OF THE COURTS & INTO THE CLOUD

In the years since Napster folded as a free service,⁹³ attempts by the recording industry to regulate P2P file sharing at the network level have ultimately been frustrated from both a legal and a technical standpoint. This section explores the difficulties of confronting the problem of piracy at the level of the network. It begins with a discussion of the high-profile court

93. A coalition of music industry plaintiffs sued Napster in December 1999. *See* A&M Records v. Napster, 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000). A preliminary injunction was entered against Napster in August 2000. *Id.* at 927 (enjoining Napster from “engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs’ copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of the rights owner”). In October 2000, with the litigation still pending, Napster and the German entertainment conglomerate Bertelsmann announced a “strategic alliance” under which Napster would offer a paid membership-based service. *See* Amy Doan, *Napster, Bertelsmann Deal Gives Labels a Fright*, FORBES.COM, Oct. 31, 2000, <http://www.forbes.com/2000/10/31/1031napster.html>.

cases, beginning in 2000 with *A&M Records v. Napster*,⁹⁴ that were brought by the recording industry against P2P software distributors in an effort to shut down P2P networks at their source. It goes on to consider two technical measures the entertainment industry has pursued to curb music and movie piracy at the network level: third-party traffic surveillance and traffic management by broadband operators.

A. Regulation by Preliminary Injunction: Fighting P2P Networks in the Courts

When a collection of recording industry plaintiffs sued Napster in 2000 to enjoin the distribution of the MusicShare software on which Napster's P2P network ran,⁹⁵ the entertainment industry was falling back on a familiar regulatory strategy: stop unauthorized copying by stopping the distribution of the technology that facilitates it.⁹⁶ This strategy, predicated on intermediary liability for gatekeepers who provide the means of reproducing copyrighted works on a large scale, was the primary mechanism for copyright enforcement in the pre-Internet era.⁹⁷ It was the strategy Hollywood famously pursued in an earlier generation, albeit without success, to stop home videotaping of over-the-air television broadcasts.⁹⁸ Because targeting gatekeepers is both more efficient and more palatable from a public relations

94. 239 F.3d 1004 (9th Cir. 2001) (affirming district court's grant of a preliminary injunction against Napster on A&M's claims of contributory and vicarious copyright infringement).

95. Here is how the MusicShare program worked:

[T]he software was distributed to users for free over the Internet, and it allowed online users to make the MP3 (and other) files stored on their hard drives available in real time to other online users. Napster stored the names of available MP3 files on its servers in a massive collective index that was updated continuously as users logged on and off the system; the files themselves remained stored on users' hard drives. Thus, the file transfers enabled by the MusicShare software were direct from user-to-user, or, in network parlance, peer-to-peer.

David Post et al., *Nice Questions Unanswered: Grokster, Sony's Staple Article of Commerce Doctrine, and the Deferred Verdict on Internet File Sharing*, 2004-05 CATO SUP. CT. REV. 235, 247 (2005).

96. See *Napster*, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

97. Wu, *supra* note 15, at 712 (arguing that "[c]opyright law's long dependence on a gatekeeping regime is under-recognized").

98. See *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 456 (1984).

standpoint than targeting end users,⁹⁹ suing software distributors was the logical first step for the music industry to take when it found itself in the grip of a new and radically disruptive technology over which it had no control. And it seemed, at first anyway, that suing providers of P2P software might be the most efficient way of eliminating the networks over which music files were being illegally shared.

The famous test case was, of course, *Napster*,¹⁰⁰ in which the recording industry sought and won a preliminary injunction to keep Napster from “engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs’ copyrighted musical compositions and sound recordings.”¹⁰¹ The court’s order further required Napster to “insure that no work owned by plaintiffs . . . is uploaded or downloaded on Napster.”¹⁰² Given the fact that the Napster system at its peak serviced fifty-eight million users with access to a dynamic catalog of as many as one billion MP3 files, the vast majority of them protected by copyright, the court’s order was an unworkably tall one.¹⁰³ On appeal, the Ninth Circuit ordered the injunction modified to shift some of the burden of policing the system onto A&M and to acknowledge technical limits on Napster’s ability to eliminate infringing files, but the panel found no fault with the district court’s conclusion that A&M had a substantial likelihood of succeeding on the merits of its copyright claims.¹⁰⁴

The Ninth Circuit’s decision to let stand a modified version of the district court’s injunction was a symbolically important win for the recording industry, but it hardly put the nail in the coffin of P2P. With respect to the file sharing technology underlying the Napster system, the court emphasized that the Supreme Court’s decision in *Sony Corp. of America v. Universal City Studios*,¹⁰⁵ the Betamax case, compelled the conclusion that “a computer

99. See Jane Ginsburg, *Putting Cars On “The Information Superhighway”: Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1488 (1995) (explaining the reasons for which copyright owners target intermediaries).

100. *Napster*, 114 F. Supp. 2d at 927.

101. *Id.*

102. *Id.*

103. See Post et al., *supra* note 95, at 247-48 (describing the Napster system).

104. See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1029 (9th Cir. 2001) (requiring modification of the district court’s injunction but noting that “appellees have substantially and primarily prevailed on appeal” notwithstanding the necessity for modification).

105. 464 U.S. 417, 489-91 (1984) (declining to impute knowledge of infringement to Sony when the challenged technology, Sony’s VCR, was capable of both infringing and “substantial noninfringing uses”).

system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material.”¹⁰⁶ Under the rule in *Sony*, where the technology in question is “capable of substantial noninfringing uses,” the fact that it is being used to infringe is an insufficient basis for barring its distribution.¹⁰⁷ Citing the need to strike a “balance between a copyright holder’s legitimate demand for effective . . . protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce,”¹⁰⁸ the *Sony* court refused to give copyright owners dominion over new technologies in the name of preventing infringement. Relying on *Sony*, the Ninth Circuit enjoined Napster from knowingly facilitating infringement by its users, but it did not enjoin the distribution of P2P software or the operation of P2P networks.¹⁰⁹

The next big legal showdown involving P2P came in the Seventh Circuit with *In re Aimster Copyright Litigation*.¹¹⁰ Aimster was a P2P program that used the AOL Instant Messenger (“AIM”) service as a platform for file sharing.¹¹¹ Aside from the fact that it relied on AIM, Aimster’s software differed from Napster’s in that it encrypted the contents of shared files—an ultimately fruitless attempt by the system’s operators to shield themselves from secondary liability by “seeing no evil” when it came to the unauthorized flow of copyrighted files.¹¹² The music industry again argued the inherent culpability of P2P technology and urged the court to hold that *Sony* could not shield an alleged contributory infringer if “there is anything more than a mere showing that a product may be used for infringing purposes.”¹¹³ Moving in step with the Ninth Circuit’s decision in *Napster*, the Seventh Circuit affirmed the preliminary injunction entered by the district court against Aimster but declined to narrow *Sony*’s safe harbor to

106. *Napster*, 239 F.3d at 1021.

107. *Sony*, 464 U.S. at 442. The court in *Sony*, however, declined to “give precise content to the question of how much [noninfringing] use is commercially significant.” *Id.*

108. *Id.*

109. *Napster*, 239 F.3d at 1021-22.

110. 334 F.3d 643 (7th Cir. 2003).

111. *See id.* at 646 (explaining the workings of the Aimster software).

112. *See id.* (explaining that “[a]ll communications back and forth are encrypted by the sender by means of encryption software furnished by Aimster as part of the software package downloadable at no charge from the Web site”).

113. *Id.* at 649 (internal quotation marks omitted).

exclude P2P software and the networks it creates.¹¹⁴ In an opinion revisiting both *Sony* and *Napster*, Judge Posner critiqued the Ninth Circuit for interpreting *Sony*'s safe harbor too narrowly by suggesting that "actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributory infringer."¹¹⁵ If knowledge of infringement alone were sufficient, Judge Posner asserted, Sony would have been held liable for merely distributing VCRs, because "it was apparent that the Betamax was being used for infringing as well as noninfringing purposes."¹¹⁶

In Judge Posner's view, the basis for Aimster's liability wasn't Aimster's knowledge of its customers' infringements, which could not be strategically negated by the system's "willful blindness"¹¹⁷ to the contents of encrypted files. The basis for Aimster's liability was, instead, its "invitation to infringement" in the form of, among other things, a tutorial giving examples of how to share copyrighted music.¹¹⁸ Also decisive was the fact that Aimster produced no evidence that its system was actually being used for any noninfringing purpose.¹¹⁹ The problem with Aimster, in other words, wasn't with the file sharing technology itself but with the manner in which Aimster promoted and facilitated its use.¹²⁰ As for the technology itself, Judge Posner interpreted *Sony* to eschew "allow[ing] copyright holders to prevent infringement . . . at the price of possibly denying noninfringing consumers the benefit of the technology."¹²¹ At the same time, however, he emphasized that such uses must be more than purely hypothetical to shield a distributor of new technology from liability.¹²² As an honest broker in the new P2P

114. See *id.* at 656 ("[T]he judge was right to grant the injunction."); *id.* at 649 ("[T]he recording industry's hostility to the *Sony* decision . . . is being articulated in the wrong forum.").

115. *Id.* at 649.

116. *Id.*

117. *Id.* at 650.

118. *Id.* at 651 ("The tutorial is the invitation to infringement that the Supreme Court found was missing in *Sony*.").

119. *Id.* at 653 (pointing out that "Aimster has failed to produce any evidence that its service has ever been used for a noninfringing use, let alone evidence concerning the frequency of such uses").

120. *Id.* (discussing the various ways in which Aimster's business model both invited and depended on infringement). The court found that Aimster "invited" its customers to infringe, "showed them how they could do so with ease using its system," and "disabled itself from doing anything to prevent infringement" by encouraging the encryption of unlawfully traded files. *Id.* at 655.

121. *Id.* at 649.

122. *Id.* at 653 ("It is not enough, as we have said, that a product or service be physically capable, as it were, of a noninfringing use.").

economy, Aimster came up fatally short, as had Napster, but the underlying technology was not to blame.

Following the decisions in the Seventh and Ninth Circuits, the Napster and Aimster services were effectively shut down before trials on the merits.¹²³ While these were undeniably positive legal outcomes for rights owners, they were not the game changers they might have been if the appellate courts had been more receptive to what Judge Posner characterized in *Aimster* as “[t]he recording industry’s [manifest] hostility to the *Sony* decision.”¹²⁴ *Sony*’s resilience in the file sharing context prevented the recording industry from getting what it really wanted out of the Napster and Aimster litigation, which was control over the distribution of P2P software and, by extension, the culture of free-riding that it created.

When the last of the big file sharing cases, *MGM v. Grokster*,¹²⁵ made its way to the Supreme Court in 2005, the recording industry was hoping for the *coup de grace* it had been denied in *Napster* and *Aimster*: a definitive narrowing of the *Sony* safe harbor to effectively preclude distribution of P2P software.¹²⁶ What the industry got instead was the much less gratifying holding that Grokster could be held liable because it had encouraged others to infringe—a refrain familiar from *Aimster*.¹²⁷ Citing “the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful . . . potential,”¹²⁸ the Court in *Grokster* affirmed its earlier decision in *Sony* and announced the “inducement rule,” imported from patent law, under which secondary liability for copyright infringement may be predicated on the culpable conduct of a technology distributor.¹²⁹ By focusing on inducement of infringement as the rationale for Grokster’s liability, the Court was able to avoid grappling with some very troublesome

123. See *supra* note 93 and accompanying text (discussing Napster’s purchase by Bertelsmann); *Aimster*, 334 F. 3d at 655 (“[T]he preliminary injunction has put [Aimster] out of business.”).

124. *Aimster*, 334 F.3d at 649.

125. 545 U.S. 913 (2005).

126. MGM urged the Court to “quantify *Sony* to the extent of holding that a product used ‘principally’ for infringement does not qualify.” *Id.* at 933 (citing MGM’s brief).

127. *Id.* at 941 (holding Grokster liable on the basis of “substantial evidence in MGM’s favor on all elements of inducement”); see also *supra* note 120 and accompanying text.

128. *Id.* at 937.

129. *Id.* at 936-37 (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”).

questions concerning the precise contours of *Sony's* safe harbor: What, exactly, does it mean for a product to be "capable of substantial noninfringing uses"? Exactly what, and how much, does an alleged contributory infringer have to know about the infringements for which its product is being used in order to be held liable?¹³⁰ Insofar as the Court held these questions at bay, *Grokster* was, as *Aimster* and *Napster* had been before it, only half a loaf for the recording industry. On the upside, it led to the demise of *Grokster* as a service, but on the downside, it permitted the continued distribution of P2P software as an "innovation having lawful promise."¹³¹

In terms of wins and losses in major litigation against operators of file sharing networks, the recording industry has a perfect record, and it has continued with some success in the aftermath of *Grokster* to target network operators with lawsuits. In 2006, Arista Records and other distributors sued MetaMachine, operator of the eDonkey P2P service.¹³² The case reportedly settled for \$30 million, and eDonkey was subsequently shut down.¹³³ In the same year, the industry sued LimeWire¹³⁴ in an action that is still pending.¹³⁵ During the pendency of the litigation, LimeWire has taken an affirmative step to curb infringement by adopting a content filtering system to which

130. See 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, 584 (2008) (pointing out that "the Court declined to analyze what the standard for contributory infringement would be when intent to foster infringement cannot be shown" and "assiduously declined to offer further guidance on the meaning of 'substantial non-infringing use'").

131. *Grokster*, 545 U.S. at 937.

132. See Complaint at 1, *Arista Records LLC v. MetaMachine, Inc.*, No. 06-cv-06991, 2006 U.S. Dist. Ct. Pleadings 6991 (S.D.N.Y. September 11, 2006) (alleging inducement of copyright infringement, contributory copyright infringement, and vicarious copyright infringement). P2P usage statistics from 2004 put eDonkey's share of total P2P traffic at 24%. See RAMON CASADESUS-MASANELL, ET AL., HARVARD BUSINESS SCHOOL CASE N2-706-479: PEER-TO-PEER FILE SHARING AND THE MARKET FOR DIGITAL INFORMATION GOODS 21 exhibit 5 (March 7, 2006), available at <http://www.smith.umd.edu/seminars/pdfs/masanell.pdf>.

133. See Caroline McCarthy, *File-sharing Site eDonkey Kicks It*, CNET NEWS.COM, Sept. 13, 2006, http://international.com.com/File-sharing-site-eDonkey-kicks-it/2100-1030_3-6115353.html?tag=txt.5.

134. LimeWire provides access to the Gnutella P2P network. See LimeWire, The Company, <http://www.limewire.com/about/company.php> (last visited Nov. 29, 2009).

135. See *Arista Records v. Lime Wire LLC*, No. 06-cv-5936, 2006 U.S. Dist. Ct. Pleadings 5936 (S.D.N.Y. Aug. 4, 2006) (bringing counts for inducement of copyright infringement, contributory copyright infringement, vicarious copyright infringement, and related state law claims).

rights owners and users can opt in.¹³⁶ It remains to be seen, however, whether LimeWire users in search of unfiltered material will simply migrate to other services that are less accommodating of rights owners. The operators of Sweden's Pirate Bay,¹³⁷ which bills itself as the world's largest torrent tracker,¹³⁸ are openly hostile to copyright owners and have vowed to continue operation notwithstanding a 2009 Swedish court order requiring them to pay the equivalent of \$3.6 million in copyright damages and sentencing them to a year each in prison.¹³⁹

In the final analysis, the industry's high-profile legal victories against P2P network operators have not amounted to a durable or comprehensive network-level solution to the problem of P2P piracy. For every network

136. See LimeWire, The Lime Wire Beta Filtering System, <http://register.limewire.com/filter/> (last visited Dec. 7, 2009) ("To address the security issues inherent to open information sharing networks, Lime Wire is launching an experimental Beta Filtering System. . . . The Filtering System prevents users from downloading, uploading and querying files flagged by copyright owners for filtering.").

137. The Pirate Bay was founded in 2003 by a Swedish national living in Mexico. See Quinn Norton, *Secrets of the Pirate Bay*, WIRED, Aug. 16, 2006, <http://www.wired.com/print/science/discoveries/news/2006/08/71543>. Its servers were moved later that year to Sweden and were seized by Swedish law enforcement in a raid in 2006. *Id.* Within days, the site was resurrected on a host based in the Netherlands. *Id.* It has since returned to Sweden, evading law enforcement through a system architecture consisting of redundant servers distributed across three countries. *Id.* If a single server is shut down, the site will be offline for only a matter of minutes—as long as it takes for fail-over scripts to execute. *Id.* The locations of the scattered servers are "obscured behind a load balancer configured to lie." *Id.* The "About" section of the Pirate Bay's web site contains the following statement concerning copyrights: "Any complaints from copyright and/or lobby organizations will be ridiculed and published at the site." Pirate Bay, About, <http://thepiratebay.org/about> (last visited Nov. 29, 2009).

138. BitTorrent is a protocol that allows users to download a file quickly by automatically having those who download the file upload parts of it to other peers as the download is occurring. See BitTorrent, What Is BitTorrent?, <http://www.bittorrent.com/btusers/what-is-bittorrent/> (last visited Nov. 29, 2009). BitTorrent is often used for distribution of very large files, like movie files, because it is faster and more efficient than other file sharing protocols. *Id.* A torrent tracker is a server that mediates between peers who are using the BitTorrent protocol to exchange files. See Nikitas Liogkas, et al., *Exploring the Robustness of Peer-to-Peer Content Distribution Systems*, 20 CONCURRENT COMPUTAT.: PRACT. EXPER. 179, 180 (2008) (describing a tracker as a "centralized component that is not involved in data exchange, but rather keeps track of all peers participating in the download").

139. See Eric Pfanner, *File-Sharing Site Violated Copyright, Court Says*, NY TIMES, Apr. 17, 2009, <http://www.nytimes.com/2009/04/18/world/europe/18copy.html>. After the verdict, the site's operators vowed in a blog post that "[t]he site will live on! We are more determined than ever that what we do is right. Millions of users are a good proof of that." Anonymous Posting to The Pirate Bay, <http://thepiratebay.org/blog> (Apr. 19, 2009, 22:42 EST).

operator that has been sued out of existence, another has come along: exit Napster, Aimster, and Grokster; enter Azureus, LimeWire, and Shareaza. Hydra-like, they just keep coming back. And for some, as sites like Pirate Bay demonstrate, flouting copyright law is the point.

B. Watch and Throttle: Fighting P2P Networks in the Cloud

If you visit the URL at which users were once able to find the Grokster file sharing service, you will see the following message:

The United States Supreme Court unanimously confirmed
that using this service to trade copyrighted material is illegal.

Copying copyrighted motion picture and music files
using unauthorized peer-to-peer services is illegal and is
prosecuted by copyright owners.

There are legal services for downloading music and movies.
This service is not one of them.

YOUR IP ADDRESS IS [insert IP address here] AND HAS BEEN
LOGGED.

Don't think you can't get caught. You are not anonymous.¹⁴⁰

The last two lines are obviously calculated to make the reader feel caught in the act of doing something wrong, even though there is certainly nothing inherently illegal in visiting the Grokster web site or, for that matter, using an extant file sharing service. The message, whose authors remain strategically nameless, asserts a power to punish that operates through what Foucault described as “the instrument of permanent, exhaustive, omnipresent surveillance, capable of making all visible,” a “faceless gaze” that cannot be

140. Grokster Home Page, <http://www.grokster.com> (last visited Nov. 29, 2009). A similar message greets visitors to the former site of eDonkey:

The eDonkey2000 Network is no longer available. If you steal music or movies, you are breaking the law. Courts around the world—including the United States Supreme Court—have ruled that businesses and individuals can be prosecuted for illegal downloading. You are not anonymous when you illegally download copyrighted material. Your IP address is [insert IP address here] and has been logged. Respect the music, download legally.

eDonkey Home Page, <http://www.edonkey.com> (last visited Aug. 31, 2009).

seen, but that “reports and registers” all wrongdoing.¹⁴¹ The message, in other words, is a warning that the authorities are watching you and know exactly where to find you if you don’t behave.¹⁴²

Even as the *Grokster* case was making its way to the Supreme Court, the entertainment industry had opened an alternate front—a technical one—in the network-level war on file sharing. It hired the information forensics firm MediaSentry to monitor traffic on popular P2P networks by acting as what one court called “an undercover user.”¹⁴³ The task of MediaSentry’s investigators was to provide proof of individual infringements in the form of incident reports documenting the IP addresses of computers offering to share copyrighted files.¹⁴⁴ They accomplished this by using special software to check the hash, a unique digital identifier, of each suspected file to verify that it was identical to the hash of a copyrighted song file in the RIAA’s database.¹⁴⁵ If the hashes didn’t match, the investigators would download the file, which they would then test using Audible Magic, a software program that compares the sound waves of the allegedly infringing file to those of the copyrighted song of which it is believed to be a copy.¹⁴⁶ If Audible Magic didn’t turn up a match, then a live person would actually listen to the song.¹⁴⁷ If a match was made at any of these junctures, MediaSentry investigators would engage in an electronic handshake with the computer offering the file to verify that the computer was online and ready to share the song.¹⁴⁸ The

141. MICHEL FOUCAULT, *DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON* 214 (1977).

142. The message is one that the RIAA and the MPAA have pushed in the media since they began filing suits against individual file sharers in 2003. See, e.g., *Watching the Detectives: You Think the Net Provides Anonymous Access to Free Music? Look Out for the Trackers*, FINANCIAL POST, Sept. 18, 2003 (quoting Tom Temple, the MPAA’s director of worldwide Internet enforcement, who cautioned that “it is an unfortunate myth for those people who think they can’t get caught . . . [because] they are easy to find and track down”).

143. *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 160 (D. Mass. 2008) (“MediaSentry essentially functions as an undercover user of the peer-to-peer networks.”).

144. See, e.g., *Arista Records, LLC v. Does 1-27*, No. 07-162-B-W, 2008 U.S. Dist. LEXIS 6241, at *9-11 (D. Me. Jan. 25, 2008) (explaining the process by which MediaSentry goes about identifying the IP addresses and other information associated with specific instances of alleged infringement); *Universal City Studios Prods. v. Martinez*, No. 06-01128, 2007 U.S. Dist. LEXIS 13426, at *11 (E.D. Cal. Feb. 22, 2007) (explaining that the plaintiff’s allegations of infringement are “based on data received by MediaSentry, a provider of anti-piracy services”).

145. Catherine Rampell, *How It Does It: The RIAA Explains How It Catches Alleged Music Pirates*, CHRON. OF HIGHER EDUC., May 13, 2008, <http://chronicle.com/article/How-It-Does-It-The-RIAA-Ex/786/>.

146. *Id.*

147. *Id.*

148. *Id.*

handshake was the “gotcha” moment: the inculpatory act on which the industry’s lawyers could later rely to “out” the alleged infringer behind the IP address. As MediaSentry’s investigators trawled LimeWire and other P2P networks for infringing files, the Orwellian prospect of an omniscient enforcer became all too real for the many John Does who unwittingly shared, or merely offered to share, copyrighted files with them. These users found themselves on the receiving end of DMCA takedown notices or, worse, legal complaints.

The entertainment industry’s traffic surveillance program has succeeded in making discoverable, in the technical and the legal sense, the identities of a slew of individual infringers, but it has operated with a margin of error wide enough to prove embarrassing. First, there were the news stories about RIAA lawsuits against innocent grandmothers, at least one of whom turned out to be dead.¹⁴⁹ Later, there was the study by computer scientists at the University of Washington, who became curious about the entertainment industry’s surveillance practices only after their own research-driven monitoring of BitTorrent traffic triggered unexpected takedown notices.¹⁵⁰ With little effort, they were able to attract hundreds of mistaken DMCA takedown notices for machines, including a networked printer, that were not sharing any content at all.¹⁵¹ Based on these false positives, the researchers concluded that agents hired by the entertainment industry to monitor P2P traffic were identifying alleged BitTorrent infringers by means of indirect and inconclusive methods.¹⁵² They also concluded that “it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials.”¹⁵³

149. See Chris Gaither, *Mistaken Identity Raises Questions on Legal Strategy*, BOSTON GLOBE, Sept. 24, 2003, at C1 (reporting on the RIAA’s suit against 66-year old Sarah Seabury Ward); Andrew Orłowski, *RIAA Sues the Dead*, THE REGISTER, Feb. 5, 2005, http://www.theregister.co.uk/2005/02/05/riaa_sues_the_dead/ (reporting on the RIAA’s suit against deceased 83-year old Gertrude Walton).

150. See Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks—or—Why My Printer Received a DMCA Takedown Notice 2* (Univ. of Wash. Technical Report No. UW-CSE-08-06-01,2008), available at http://dmca.cs.washington.edu/dmca_hotsec08.pdf (stating that the authors initially viewed unjustified DMCA complaints as “an annoyance to be avoided”).

151. *Id.* at 1.

152. *Id.*

153. See *id.* In a press release describing the study, the RIAA stated that the University of Washington researchers “commended the RIAA’s transparency and technological practices used to detect . . . those engaged in online music theft.” Press Release, RIAA, New Report Examines RIAA Methodology for Detecting Illegal Activity Over Peer-To-Peer Networks (June 11, 2008), available at http://riaa.com/newsitem.php?news_month_filter=&

To be truly effective as a regulatory strategy, network surveillance must be both reliable and invisible. The monitor must see all, as Foucault asserted, without being seen. Disembodied omniscience is *the* salient attribute of the enforcer's "faceless gaze." In practice, however, the entertainment industry's methods for monitoring BitTorrent networks in particular have proven to be neither reliable nor invisible. In addition to exposing the problem of false positives, the University of Washington study cast doubt on the ability of undercover monitoring agents to roam BitTorrent networks untraceably.¹⁵⁴ The researchers observed that monitoring agents behave online in ways that make them "highly distinguishable" from regular BitTorrent users.¹⁵⁵ It more or less follows from this, they concluded, that "automatic and fine-grained detection of monitoring agents is feasible."¹⁵⁶ Such detection will inevitably lead to the development of on-the-fly blacklisting techniques, by means of which network access can be blocked for IP addresses associated with suspected monitoring agents.¹⁵⁷

In the meantime, some users have found another way to transform the watchers into the watched when it comes to the investigative tactics of monitoring agents. John Doe file sharing defendants have argued in court motions that evidence provided by MediaSentry should be excluded because the company is operating as an unlicensed private investigator in contravention of applicable state laws.¹⁵⁸ Other users have formally

news_year_filter=&resultpage=2&id=9A412FB1-0D41-5C90-7C70-3674F3FDE752. The study does not exactly "commend the RIAA's transparency," but it does characterize the RIAA's method of direct monitoring of the Gnutella network as a "more conclusive" means of enforcement than the indirect monitoring used (presumably by the MPAA) to monitor BitTorrent.

154. See Piatek, et al., *supra* note 150, at 1, 6 (observing that monitoring agents stand out because they "share no data whatsoever, occur frequently in swarms, and are drawn from a small number of prefixes").

155. See *id.* at 1.

156. *Id.*

157. See *id.* at 6 (predicting that "[f]uture P2P networks may employ . . . mechanisms to identify monitoring agents, gossiping this information among peers" to enable the creation and maintenance of "[b]lacklists on-the-fly").

158. See, e.g., *Arista Records LLC v. Doe*, 584 F. Supp. 2d 240, 256-57 (D. Me. 2008) (addressing the defendant's argument that MediaSentry gathered information in violation of a Maine statute requiring licensure of private investigators); *Sony BMG Music Entm't v. Doe*, No. 5:08-CV-109-H, 2008 U.S. Dist. LEXIS 106088, at 17 (E.D.N.C. Oct. 21, 2008) (addressing defendant's argument that a declaration offered by plaintiff should be stricken because "MediaSentry unlawfully investigated defendant without a license"); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 175-76 n.30 (D. Mass 2008) (addressing the defendant's argument that "the Linares affidavit, which forms the basis of some of the plaintiffs' prima facie case, should be stricken [because MediaSentry] does not have the

complained about MediaSentry to state regulatory agencies responsible for oversight of private investigative services.¹⁵⁹ As a result of a complaint filed in Massachusetts, the Department of State Police issued a cease and desist letter ordering MediaSentry to cease operations in the Commonwealth until it obtained a license.¹⁶⁰ Central Michigan University, whose students were targets of RIAA subpoenas, petitioned the Michigan Department of Labor and Economic Growth for an order requiring MediaSentry to stop all operations in Michigan until properly licensed as a private investigator.¹⁶¹ Such complaints represent little more than temporary impediments when it comes to the overall project of surveillance for which MediaSentry was retained. They are remarkable, however, as highly visible gestures of resistance to the RIAA's putatively invisible network monitoring methods. Not surprisingly, once MediaSentry "became the story," it was quietly fired.¹⁶²

More problematic for the industry's hired monitors than their own increasing visibility has been the increasing *invisibility* of their quarry. As surely as users have migrated over time from one P2P network to another, they have also migrated in ever-larger numbers from open networks like LimeWire to closed networks known as friend-to-friend ("F2F") networks or

license to undertake private investigations required by Massachusetts General Laws ch. 147, §§ 23-25").

159. See Jaikumar Vijayan, *Mediasentry Defends Work for RIAA in Music Piracy Cases*, COMPUTERWORLD, Sept. 9, 2008, <http://www.computerworld.com/action/article.do?command=printArticleBasic&taxonomyName=Security&articleId=9114371&taxonomyId=17> (reporting on complaints against MediaSentry filed with various state agencies).

160. See *Arista Records*, 584 F. Supp. 2d at 256 (citing the docket entry for the "cease and desist order, dated January 2, 2008, directing MediaSentry to stop conducting investigatory activities until licensed by the Commonwealth").

161. Ass't Gen. Counsel, Cent. Mich. Univ., Statement of Complaint to Michigan Department of Labor and Economic Growth by Central Michigan University (July 11, 2008), available at http://beckermanlegal.com/Documents/centralmichigan_mediasentry_080805Complaint.pdf (last visited Sept. 8, 2009) (pointing out that MediaSentry's unlicensed activities have been challenged in John Doe copyright infringement cases pending in federal courts in eight states).

162. The RIAA ended its relationship with MediaSentry sometime in 2008, replacing it with a Copenhagen-based company called DTecNet. Sarah McBride, *Changing Tack, RIAA Ditches MediaSentry*, WALL ST. J., Jan. 5, 2009 at B2. It offered no explanation for the switch. *Id.* Automated online media monitoring is a growth market, with new entrants joining all the time. See, e.g., CyberAlert, Inc., Media Monitoring for Intellectual Property Infringement, http://www.cyberalert.com/app_intellectual_property_infringement.html (last visited Dec. 10, 2009); Ultima Thule Technology, Brand and Copyright Monitoring, <http://www.ultimathule.net/software/brand-copyright.php> (last visited Dec. 10, 2009).

“darknets,” over which the flow of traffic is often encrypted.¹⁶³ The increasing popularity of F2F networks has been driven in large part by well-publicized, third party monitoring of public P2P networks.¹⁶⁴ The rate of migration from P2P to F2F is likely to accelerate in the near future, given that the popular LimeWire P2P client now includes support for F2F file sharing.¹⁶⁵

F2F networks may represent the end of the road for industry monitoring for a couple of reasons. First, they’re hard to penetrate, because they’re not open to the general public.¹⁶⁶ Second, files shared using F2F clients that support encryption are not only invisible to human monitors, they’re not susceptible to deep packet inspection (“DPI”), which is the automated surveillance technology on which the entertainment industry has pinned its hopes.¹⁶⁷ This means that even if rights owners can convince internet service

163. See, e.g., Posting of Ken Fisher to Ars Technica, <http://arstechnica.com/> (May 9, 2007, 13:29 EST) (defining darknets as “private networks, usually requiring authentication through ‘insider’ contacts, loaded with digital content”). But see Peter Biddle, et al., *The Darknet and the Future of Content Distribution*, in PROCEEDINGS OF THE 2002 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 1 (2002) (defining “darknet” more loosely as “a collection of networks and technologies used to share digital content”).

164. As an example, researchers at the University of Washington recently released a friend-to-friend BitTorrent client called OneSwarm that “provides privacy against the systematic monitoring of user behavior common in today’s P2P networks.” Thomas Isdal, et al., *Friend-to-Friend Data Sharing with OneSwarm* 11 (Univ. of Wash. Technical Report, UW-CSE, Feb. 2009), available at <http://oneswarm.cs.washington.edu/papers.html>.

165. See Posting of Nate Anderson to Ars Technica, <http://arstechnica.com/> (Mar. 5, 2009, 21:35 EST) (reporting on the addition of darknet support to LimeWire 5.1.1 and observing that “LimeWire’s massive install base means that millions of users now have a secure and simple way to share files with each other and no one else”).

166. See John Markoff, *New File-Sharing Techniques Are Likely To Test Court Decision*, N.Y. TIMES, Aug. 1, 2005, at C1, (explaining that darknets “grow as part of a ‘web of trust,’ and are far more restricted than open systems”).

167. Files traveling over the Internet are broken into smaller “packets” of data at their point of departure and are reassembled at their point of destination. Following is a description of how DPI works and an explanation for why it is ineffective for monitoring encrypted traffic:

A packet is often conceptualized as having two parts: a “header” (analogous to an envelope) and a data or payload portion (analogous to what is contained in the envelope). In the normal course of simply routing packets over its network, a broadband service provider need only look at the “header” portion of the packet, which includes information such as the sender’s and recipient’s IP addresses and protocol and other formatting information. In the case of DPI, however, the service provider can “inspect” the entire packet, including the data portion. Notably, deep packet inspection is not a technique for breaking encryption, so data sent in encrypted form remains secure.

providers ("ISPs") to partner with them in policing P2P traffic, as they have lately been trying very hard to do, the ISPs will have no effective means of examining encrypted file contents.¹⁶⁸ It is likely, too, that migration to F2F networks that use encryption will increase among users as DPI is more widely deployed by network intermediaries.¹⁶⁹

Putting aside the challenges posed by darknets that support encryption, which are for now the refuge primarily of sophisticated users, the attraction for the entertainment industry of deputizing ISPs in the network-level fight against online piracy is obvious. Unlike MediaSentry and its brethren, whose monitoring is scattershot and whose agents behave in ways that make them

Of course, given the volume of packets at issue, DPI must as a practical matter be done in automated form, at least in the first instance (depending on the purpose of for which the service provider is using DPI, certain packets might be blocked or held for further analysis and a person might then become aware of the contents of such packets). Thus, for example, a provider could install hardware and software at various points on its network and place an incoming packet in a buffer as it passed through one of those checkpoints. The packet could then be analyzed to determine whatever information was needed to carry out the purpose of the DPI (e.g., whether the complete URL contained in the packet matched a blacklist of URLs known to display child pornography). Then, depending on the results of that analysis, the packet would continue on its route—perhaps with some information about its contents or other attributes being recorded—or be blocked or diverted.

Samir Jain, *The Promise and Perils of Deep Packet Inspection*, 8 PRIVACY & SEC. L. REP. 217, 218 (2009), available at <http://www.wilmerhale.com/files/Publication/0f1fbf30-bfcd-49ba-bc64-610d2362389a/Presentation/PublicationAttachment/a64a1796-08db-48ec-9ab2-64700d18eace/PDFArtic.pdf>.

168. See, e.g., Anne Broache, *MPAA Wants ISP Help in Online Piracy Fight*, CNET NEWS.COM, Sept. 18, 2007, http://international.com.com/8301-10784_3-9780401-7.html?tag=mncol;txt (quoting a statement by MPAA CEO Dan Glickman concerning the entertainment industry's desire to "deepen our relationship" with telephone, cable, and Internet companies "because we're all in this together").

169. The inclusion of support for darknets in the LimeWire P2P client may be the first step in a mass migration of mainstream P2P users to darknets. According to the company's promotional materials, the LimeWire software has been downloaded "hundreds of thousands of times per day." See LimeWire, About, <http://www.limewire.com/about/> (last visited Dec. 1, 2009). Support for file encryption in mainstream clients like LimeWire may not be far behind the recent addition of support for closed networks. The Freenet client, whose distributors report two million downloads since 2000, supports encryption:

Communications by Freenet nodes are encrypted and are routed-through other nodes to make it extremely difficult to determine who is requesting the information and what its content is. . . . Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it.

The Free Network Project, What is Freenet?, <http://freenetproject.org/whatis.html> (last visited Dec. 1, 2009).

vulnerable to exposure and blacklisting, ISPs—through which all traffic flows—are truly in a position to be the industry's invisible eye.¹⁷⁰ Moreover, ISPs themselves have a vested interest in managing P2P traffic, because applications like BitTorrent consume large amounts of bandwidth. Asserting a direct link between congestion and illegal P2P file sharing, the RIAA has attempted to make common cause with ISPs, but it has also publicly threatened that “government action may be necessary” if voluntary anti-piracy agreements with broadband providers are not reached.¹⁷¹

Such action has already been taken at the federal level with respect to colleges and universities in their roles as ISPs. As a condition of continued participation in federal student aid programs, institutions of higher education are required under the Higher Education Opportunity Act of 2008 (“HEOA”)¹⁷² to certify that they have “developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents.”¹⁷³ Although the HEOA doesn't require specific deterrents, the legislative history mentions “bandwidth shaping, traffic monitoring to identify the largest bandwidth users, a vigorous program of accepting and responding to Digital Millennium Copyright Act (“DMCA”) notices, and a variety of commercial products designed to reduce or block illegal file sharing.”¹⁷⁴ The RIAA has also

170. See Declan McCullagh, *Music, Movie Lobbyists Push to Spy on Your Net Traffic*, CNET NEWS.COM, Aug. 18, 2008, http://international.com.com/8301-13578_3-10019622-38.html?tag=mncol (quoting a statement by Shira Perlmutter, a vice president for global legal policy at the International Federation of the Phonographic Industry, urging ISPs to help curb piracy because “[t]hey have the technical ability to manage the flow over their pipes”).

171. Press Release, RIAA, *RIAA CEO Encourages ISPs to Work with Music Industry to Address Digital Theft*, (May 6, 2008), available at <http://www.riaa.com/newsitem.php?id=445DBB88-3C46-F2B7-784F-8B1B1B7F5FAA> (asserting that P2P traffic “is causing significant congestion over our broadband networks” and advocating “private market discussions” between ISPs and the RIAA as the preferred solution to the problem). Some researchers have cast doubt on the RIAA's assertions about the severity of the congestion caused by file sharing applications. See, e.g., KIMBERLY CLAFFY, COOP. ASS'N FOR INTERNET DATA ANALYSIS, TEN THINGS LAWYERS SHOULD KNOW ABOUT THE INTERNET 7 (2008), http://www.caida.org/publications/papers/2008/lawyers_top_ten/lawyers_top_ten.pdf (“Although the little data that researchers can scrape together . . . do not support the ‘p2p is causing a bandwidth problem’ claim, the press releases we see as a popular substitute for real data in the U.S. do support the claim that the Internet transit business model is broken.”).

172. Pub. L. No. 110-315, 122 Stat. 3078.

173. *Id.* § 493, 20 U.S.C. § 1094(a)(29)(A).

174. H.R. REP. NO. 4137, at 116 (2008), available at http://help.senate.gov/Hearings/2008_07_29_E/Statement_of_Managers.pdf. In comments published with the rules implementing the HEOA, the Department of Education stated that the inclusion of one or more technology-based deterrents in an institution's plan is statutory, but “no particular

aggressively pursued state legislation that imposes direct enforcement requirements on college and university information technology departments.¹⁷⁵

Using DPI or other intrusive methods to monitor, filter, or block the contents of files on behalf of rights owners is a significant functional departure for ISPs, which have historically acted merely as conduits for information.¹⁷⁶ It also represents a controversial burden shift in the enforcement of copyright laws from rights owners to network operators, a shift that may be especially hard to bear for cash-strapped public colleges and universities.¹⁷⁷ In addition, traffic surveillance by ISPs raises important questions concerning user privacy and net neutrality. With respect to the latter, Comcast found itself on the defensive in October 2007 after the Associated Press conducted tests which revealed that the ISP was secretly blocking P2P traffic and sending bogus error messages to affected users.¹⁷⁸ Comcast at first denied that it was targeting P2P traffic for differential

technology measures are favored or required.” Supplementary Information, 74 Fed. Reg. 55,910, 55,925 (Oct. 29, 2009).

175. See, e.g., TENN. CODE ANN. § 49-7-142(a)(3) (2008) (“Each public and private institution of higher education in the state that has student residential computer networks shall . . . reasonably attempt to prevent the infringement of copyrighted works over the institution’s computer and network resources”); 110 ILL. COMP. STAT. 205/9.33(a)(2) (2008) (proposing to amend the Board of Higher Education Act to require an “institution [that] receives 10 or more legally valid notices of infringement within the preceding year, [to] undertake reasonable efforts to install and implement a technology-based deterrent system to attempt to prevent the infringement of copyrighted works over the institution’s computer and network resources”).

176. This hands-off posture is a condition under the DMCA for ISP immunity from third-party liability for copyright infringement. See 17 U.S.C. §§ 512(a)(2), (5) (2006) (providing that “[a] service provider shall not be liable . . . if . . . the transmission, routing, provision of connections, or storage [of material] is carried out through an automatic technical process without selection of the material by the service provider . . . [and] without modification of its content”).

177. A representative of the Campus Computing Project, an advocacy group for information technology officers in higher education, refers to the HEOA’s anti-piracy provisions as “pro bono compliance enforcement for the entertainment industry.” Sara Lipka, *New Rules Will Push Colleges to Rethink Tactics Against Student Pirates*, CHRON. OF HIGHER ED., Feb. 13, 2009, at A19.

178. See *In re Free Press & Pub. Knowledge*, 23 F.C.C.R. 13028, 13031 (2008) (describing the AP study). Comcast argued that it was merely slowing and not actually blocking P2P traffic, but the Federal Communications Commission found otherwise. See *id.* at 13053-54 (finding that “whether or not blocking was Comcast’s intent, Comcast’s actions certainly had that effect in some circumstances”).

treatment.¹⁷⁹ When it finally admitted to the conduct, which it accomplished by means of DPI, it argued that it was engaged in legitimate network management designed to ease traffic congestion.¹⁸⁰

A Federal Communications Commission (“FCC”) investigation of the controversy concluded that Comcast’s discrimination against P2P protocols “poses a substantial threat to both the open character and efficient operation of the Internet, and is not reasonable” as a form of network management.¹⁸¹ As a means of reducing network congestion, the FCC found, Comcast’s targeting of P2P protocols was both over-inclusive and under-inclusive: it was over-inclusive insofar as it blocked low-bandwidth as well as high-bandwidth P2P transfers; and it was under-inclusive insofar as it failed to block high-bandwidth transfers made using non-P2P protocols.¹⁸² To remedy the poor fit between the reduction of congestion and protocol-specific blocking or “throttling,” the FCC ordered Comcast to “institute a protocol-agnostic network management technique.”¹⁸³ Under the FCC’s decision, Comcast may slow or meter transmissions on the basis of bandwidth consumption, but not on the basis of protocol.

As for Comcast’s use of DPI to inspect the contents of files, the FCC drew an analogy to reading someone else’s mail: “[I]n laymen’s terms, Comcast opens its customers’ mail because it wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein.”¹⁸⁴ Although the FCC’s rebuke of Comcast was couched in terms of protecting open access rather than privacy, the choice of analogy suggests an awareness on the FCC’s part that using DPI to accomplish content-based sorting of Internet traffic implicates *both* values. In the wake of revelations that Comcast has been using DPI to manage traffic, some have questioned whether DPI violates the Wiretap Act’s prohibition on the intentional interception of electronic communications.¹⁸⁵ The question is sure to be raised for adjudication, given the fact that the FCC in the Comcast decision expressly affirmed the right of ISPs to “block . . . transmissions that

179. See *id.* at 13030-31 (stating that Comcast “misleadingly disclaimed any responsibility for [its] customers’ problems” with P2P transfers).

180. See *id.* at 13031-32, 13056 (noting that “Comcast justifies its practice as a means of easing network congestion”).

181. *Id.* at 13058.

182. See *id.* at 13057-58.

183. *Id.* at 13057-58.

184. *Id.* at 13051.

185. See Jain, *supra* note 167, at 155 (arguing that “the complexity of the applicable Wiretap Act provisions and the various possible fact patterns make[] it difficult to definitively answer the question whether the use of DPI violates existing wiretapping laws”).

violate copyright law” in any manner that is “consistent with federal policy.”¹⁸⁶ This pronouncement gives the green light, at least in principle, to the anti-piracy collaboration between ISPs and rights owners that rights owners have been aggressively advocating.¹⁸⁷ It also acknowledges, however, that there are public law limits on any private ordering in which ISPs and rights owners may engage to regulate traffic in copyrighted content. These unspecified limits will inevitably be tested and defined in Congress and the courts over the coming years as the network-level regulatory strategies of content owners continue to evolve in response to developments in the nature and culture of P2P networks.

III. THE TROUBLE WITH REGULATING USERS: WHEN NORMS AND THE LAW PART WAYS

The solution to music piracy is not a technological one. No one can make the perfect safe to put things in. And it won't be a magic law that stops all piracy. In the end, the solution will be a behavioral one.

– Phil Shiller, Senior Vice President of Worldwide Product Marketing,
Apple Inc.¹⁸⁸

At the most basic level, there are two reasons why P2P file sharers won't behave: (1) they don't have to, and (2) they don't want to. They don't *have* to for reasons that are elaborated in the first two sections of this Article: The means for trafficking illegally in copyrighted files are readily available and,

186. *In re Free Press & Pub. Knowledge*, 23 F.C.C.R. at 13058.

187. The controversial collaborative model being promoted most aggressively by the RIAA and other industry groups, both in the United States and abroad, is known as “graduated response.” See, e.g., Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1 (describing the graduated response model favored by the RIAA); Leigh Phillips, *French Internet Law Clashes with EU Position*, EU OBSERVER, Oct. 31, 2008, <http://euobserver.com/871/27026> (reporting a conflict between European Union law concerning graduated response and proposed legislation in France). Under this “three strikes” model, the rights owner notifies the ISP of an alleged infringement and the associated IP address. See McBride & Smith, *supra*; Phillips, *supra*. The ISP, in turn, notifies the customer to whom the IP address is assigned and requests that the customer cease and desist sharing copyrighted files. See McBride & Smith, *supra*. After two or three such notices, the ISP summarily terminates the customer's Internet access. See *id.* This model represents an end run around the procedural protections afforded by the litigation process and gives rights owners unprecedented authority to act as the *de facto* judge and jury in all claims of copyright infringement that involve P2P file sharing.

188. J.D. LASICA, DARKNET: HOLLYWOOD'S WAR AGAINST THE DIGITAL GENERATION 198 (2005).

thanks to the continuing vitality of *Sony*, they remain perfectly legal. From a technical standpoint, illegal file sharers have always managed to stay a step ahead of rights owners: When content is locked, they pick the locks; the better the locks get, the better they get at lock-picking. When they're being watched, they hide; the better the surveillance gets, the better they get at hiding. To the extreme dismay of rights owners, over the last ten years illegal file sharers have adapted rather deftly to the succession of coercive tactics deployed to manage their behavior.

Why file sharers don't *want* to behave is a trickier question whose answer is largely to be found in the permissive social and cultural norms that have developed over the years around file sharing.¹⁸⁹ The answer is to be found, too, in Foucault's assertion, quoted at the beginning of this Article, that effective regulation is not simply a matter of coercion, but requires a degree of willing self-modification (i.e., "buy-in") on the part of the governed.¹⁹⁰ In the decade after Napster, the entertainment industry's user-directed anti-piracy interventions have presupposed that most illegal file sharers *can*, in fact, be reformed. The underlying premise is that permissive social norms—and the unruly behavior they motivate—can be strategically realigned, through punishment and education, to coincide with legal norms.¹⁹¹

189. In 2005, at the peak of the P2P controversy, Lawrence Solum described the war on file sharing as "a moral and ideological battle for the hearts and minds of . . . [the] public." Lawrence Solum, *The Future of Copyright*, 83 TEX. L. REV. 1137, 1139 (2005) (book review). David Operderbeck described it in very similar terms as "a titanic struggle to change public ambivalence." David Operderbeck, *Peer-to-Peer Networks, Technological Evolution, and Intellectual Property Private Attorney General Litigation*, 20 BERKELEY TECH. L.J. 1685, 1687 (2005).

190. See Foucault, *supra* note 1, at 203-04 and accompanying text.

191. This premise has been explored over the years by social scientists with mixed results. See, e.g., George E. Higgins et al., *Low Self-Control and Social Learning in Understanding Students' Intention to Pirate Movies in the United States*, 25 SOC. SCI. COMPUTER REV. 339, 353 (2007) (recommending "educational messages that emphasize the risks of movie piracy" and "training that emphasizes piracy as a crime"); Robert LaRose, et al., *Sharing or Piracy? An Exploration of Downloading Behavior*, 11 COMPUTER-MEDIATED COMMUN. 1, 15 (2006) (finding that "[i]n multivariate analyses, only the expectation of punishment remained as a factor supporting discontinuance" of illegal downloading); X. Li & N. Nergadze, *Deterrence Factors for Online Copyright Infringement*, International Communication Association Conference Papers 20 (October 2004) (concluding that "increas[ing] awareness of the law" and "increasing consensus with the rule" are "more viable" than punishment as deterrents to music piracy); but see Ram D. Gopal et al., *A Behavioral Model of Digital Music Piracy*, 14 J. ORG'L COMPUTING & ELEC. COMM. 89, 103 (2004) (finding that "legal and educational campaigns" have "no significant deterrent effect on music piracy").

Punishment and education have thus been the cornerstones of the industry's anti-piracy efforts when it comes to individual users. Punishment, which an RIAA press release characterized as "the enforcement phase of its education program," began in 2003 in the form of a widely publicized campaign of lawsuits against individual file sharers.¹⁹² By the time the campaign ended without fanfare in late 2008, it had targeted some 35,000 people.¹⁹³ Education has come in a variety of forms and through a variety of proxies, including the World Intellectual Property Organization ("WIPO"), the United States Copyright Office, and even the Boy Scouts of America, whose Los Angeles chapter now offers a "Respect Copyrights" merit badge—sponsored by the MPAA.¹⁹⁴ Have these user-directed regulatory strategies been effective at curbing online piracy? Predictably, the answer depends very much on who is being asked.

A. The RIAA v. John Does 1-35,000: Fighting P2P Users in the Courts

Although the RIAA's user-directed litigation campaign is widely regarded as having created a major public relations problem for music distributors, industry representatives maintain that the lawsuits were successful at "raising awareness" about the illegality of file sharing.¹⁹⁵ As of this writing, only two cases against individual file sharers have actually gone to trial. The first, *Capitol Records v. Thomas*,¹⁹⁶ resulted in an arguably Pyrrhic victory for the music industry plaintiffs. The RIAA won the case on the merits in two separate trials.¹⁹⁷ The jury in the first trial returned a verdict

192. Press Release, RIAA, *Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online* (Sept. 8, 2003), available at <http://www.riaa.org/newsitem.php?id=85183A9C-28F4-19CE-BDE6-F48E206CE8A1>. Justice Breyer, in his concurring opinion in the *Grokster* case, characterized the RIAA's lawsuit campaign as "a teaching tool." 545 U.S. at 963 (Breyer, J., concurring).

193. See McBride & Smith, *supra* note 187 at B19 (reporting on the end of the file sharing litigation).

194. See Press Release, MPAA, *Los Angeles Area Boy Scouts Collaborate with MPAA to Teach Young People about Respecting Copyrights* (Oct. 20, 2006), available at http://www.mpaa.org/press_releases/boy%20scouts%20press%20release.pdf.

195. See McBride & Smith, *supra* note 187 at B19 (reporting on the end of the RIAA's campaign of lawsuits).

196. 579 F. Supp. 2d 1210 (D. Minn. 2008).

197. *Id.*; Richard Koman, *Wow! Jury Verdict in Capitol v. Thomas-Rasset: \$ 2 Million*, ZDNET, June 18, 2009, <http://government.zdnet.com/?p=4990>. Thomas's motion for a retrial was granted based on an error in the judge's jury instructions concerning whether the "making available" of music for download qualifies as distribution within the meaning of the Copyright Act. See *Thomas*, 579 F. Supp. 2d at 1226-27. The case was subsequently retried.

against Thomas and awarded the plaintiffs statutory damages of \$222,000 to compensate for twenty-four downloaded songs.¹⁹⁸ In his decision granting Thomas's motion for a new trial based on an erroneous jury instruction, the judge himself said he thought the damages awarded were excessive, and he implored Congress to revisit the criteria for awarding large statutory damages in cases involving noncommercial infringement by individual consumers.¹⁹⁹ In the retrial, the jury found against Thomas again, this time awarding a breathtaking \$1.92 million, or \$80,000 per song, in damages.²⁰⁰ While it may be only arguable that the statutory damages awarded in the retrial were extreme enough to test the limits of due process,²⁰¹ it is certain that they were extreme enough to test the limits of decency.

Whereas the RIAA's lawyer after the first Thomas trial spoke triumphantly to the press of "sending a message" about the consequences of downloading,²⁰² the RIAA's communications staff after the second trial issued a succinct press release thanking the jury for taking the case seriously and expressing continued willingness to settle.²⁰³ This verdict-to-verdict shift in rhetoric from triumphalism to conciliation suggests that the RIAA recognized with the second Thomas verdict that it was in danger of becoming, from a public relations standpoint, a victim of its own success. In *Sony BMG Music Entertainment v. Tenenbaum*,²⁰⁴ a case against a Boston University graduate student that is likely to be the last prominent case against an individual file sharer, the RIAA's lawyers tried to keep a lower public profile. For example, they opposed Tenenbaum's motion to "narrowcast" oral arguments on the Internet. The irony of this stance was not lost on the judge, who found it "curious" that the plaintiffs should be so camera shy,

198. Thomas, 579 F. Supp. 2d at 1227.

199. *Id.*

200. See Koman, *supra* note 197.

201. See Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. (forthcoming 2009) (arguing that "Gore and its progeny have salience in copyright cases, and that statutory damage awards should be overturned or reduced when they are grossly excessive under the *Gore* guideposts").

202. See Posting of Eric Bangeman on Ars Technica, <http://arstechnica.com/> (Oct. 4, 2007, 17:30 EST) (quoting Richard Gabriel, RIAA lead counsel).

203. See Press Release, RIAA, *RIAA Comment on Verdict in Capitol Records v. Jammie Thomas-Rasset* (June 18, 2009), available at <http://www.riaa.com/newsitem.php?id=67AC2E75-E62A-1823-9604-FD0F15EF0F63>.

204. 593 F. Supp. 2d 319 (D. Mass. 2009).

given that the music industry's deterrence strategy "effectively relies on the publicity resulting from this litigation."²⁰⁵

As an empirical matter, the mass lawsuits appear to have had only a transitory deterrent effect. While surveys conducted at the end of 2003 and the beginning of 2004, just after the campaign began, showed a sharp decrease in illegal downloads, follow-on surveys showed that the percentage of music downloaders had rebounded by 2005.²⁰⁶ The rebound is consistent with a finding that fear among users of being prosecuted for illegally downloading content decreased from 2003 to 2005.²⁰⁷ After all, for the thousands of people who got sued, there were many millions who didn't. The warning on the RIAA's web site that "anyone—and everyone—engaged in music theft is at risk for a lawsuit,"²⁰⁸ reminiscent of the threat on Grokster's site that no one is anonymous in cyberspace, appears to have rung hollow for the millions of file sharers who continued to share copyrighted material without permission (or reprisal) during the five years the RIAA spent suing individual users. The more enterprising among them readily found refuge from surveillance and subpoenas in closed networks and encrypted file transfers.²⁰⁹ Providers of software that both encrypts and conceals the source of torrent traffic market their product to precisely this demographic.²¹⁰

205. *Id.* at 321. The case against Tenenbaum went to trial and ended in a \$675,000 judgment against him. See Posting of Ben Sheffner to Ars Technica, <http://arstechnica.com/> (July 31, 2009, 17:34 EST).

206. See LEE RAINIE, ET AL., PEW INTERNET PROJECT AND COMSCORE MEDIA METRIX DATA MEMO, THE STATE OF MUSIC DOWNLOADING AND FILE-SHARING ONLINE 1-2 (2004), http://www.pewinternet.org/~media/Files/Reports/2004/PIP_FilesSharing_April_04.pdf (reporting in early 2004 that a third of music downloaders surveyed said they had stopped because of the RIAA's lawsuits, and 60% of those surveyed who had never tried music downloading said the RIAA lawsuits would keep them from doing so); but see Michael Bachmann, *Lesson Spurned? Reactions of Online Music Pirates to Legal Prosecutions by the RIAA*, 1 INT'L J. CYBER CRIMINOLOGY 213, 220 (2007) (relying on Pew Internet & American Life Project data to conclude that an upward trend in downloading across all demographic groups between 2003 and 2005 suggests that the deterrent effect of the RIAA lawsuits was "wearing off" as the campaign wore on).

207. Bachmann, *supra* note 206, at 220.

208. RIAA, *FAQ For Students Doing Reports*, <http://www.riaa.com/faq.php> (last visited on Dec. 2, 2009).

209. The authors of a 2006 German study on file sharing behavior concluded that lawsuits against users produce a "negative effect" and operate to "intensify the open source development of anarchic p2p networks like Mute that encrypt the communication between the peers in such a way that the RIAA or MPAA will hardly be able to identify the user." Jan U. Becker & Michel Clement, *Dynamics of Illegal Participation in Peer-to-Peer Networks—Why Do People Illegally Share Media Files?*, 19 J. MEDIA ECON. 7, 25 (2006).

210. See, e.g., TorrentPrivacy, <https://torrentprivacy.com/> (last visited Dec. 7, 2009).

B. Teach Your Children Well: Fighting P2P Users in the Classroom

It has been an article of faith among corporate rights owners since the beginning of the file sharing “epidemic” that there is a pressing need for better education among children and teenagers about laws protecting intellectual property.²¹¹ A survey of teenagers sponsored by Microsoft in early 2008 revealed that 49% were not familiar with rules and guidelines for downloading copyrighted material from the Internet.²¹² Only 11% said they understood the rules very well.²¹³ The survey also showed that the more teenagers (say they) know about the rules, the more they (say they) believe downloading copyrighted content without permission should be punished.²¹⁴ Given the intuition that education and compliance vary together, there has been no shortage of educational material produced by corporate rights owners and affiliated organizations to fill the perceived void. Critics have charged, fairly, that much of this material is one-sided and fails to address adequately limitations on copyright like the public domain, fair use, and the first sale doctrine.²¹⁵ The range of materials available is wide, but examples from WIPO, the Copyright Society of the USA (“CSUSA”), and the RIAA are representative of their collective substance and tone.

WIPO offers a 75-page book aimed at “young students” called *Learn from the Past, Create the Future: The Arts and Copyright*.²¹⁶ In addition to

211. Cf. David McGuire, *Report: ‘Tweens’ Less Likely to Pirate*, WASHINGTONPOST.COM, May 26, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A58270-2004May26.html> (quoting an assertion by a representative of the Business Software alliance that “parents, businesses and the government should spend more time and money to teach children that illegal downloading and file-sharing is [sic] wrong”).

212. See Press Release, Microsoft, *Teens Less Likely to Download Illegally When They Know the Laws, Microsoft Survey Finds* (Feb. 13, 2008), available at <http://www.microsoft.com/presspass/press/2008/feb08/02-13MSIPSurveyResultsPR.msp>; Memorandum from KRC Research to Interested Parties, *Topline Results of Microsoft Survey of Teen Attitudes on Illegal Downloading 3* (Jan. 23, 2008), available at <http://www.microsoft.com/presspass/download/press/2008/02-13KRCStudy.pdf>. Of course, how closely what survey respondents say correlates with what they actually think is very hard to know.

213. Memorandum from KRC Research, *supra* note 212, at 3.

214. *Id.*

215. See, e.g., The Patry Copyright Blog, <http://williampatry.blogspot.com/> (Oct. 1, 2007, 11:26 EST) (criticizing materials produced by CSUSA for being “extreme” and “inaccurate”); Katie Dean, *Copyright Crusaders Hit Schools*, WIRED, Aug. 13, 2004, <http://www.wired.com/entertainment/music/news/2004/08/64543> (reporting on a program sponsored by the American Library Association designed to counteract perceived biases in educational materials provided to schools by corporate rights owners).

216. MARIA DE ACAIZO, WIPO, *LEARN FROM THE PAST, CREATE THE FUTURE: THE ARTS AND COPYRIGHT* (2007), http://www.wipo.int/freepublications/en/copyright/935/wipo_

providing basic information about copyrights, the publication focuses in particular on “the challenges that digital technology present[s] to the protection of copyrighted works.”²¹⁷ A section dedicated to P2P file sharing lists “reasons why we should not upload/download illegal copies of works.”²¹⁸ These include the risk of computer viruses and hacking, the risk of lawsuits, a reduced choice of music, and the ease of obtaining content from legal distributors.²¹⁹ WIPO’s general strategy is to engage children as actual and potential creators of artistic works, converting them from bystanders into stakeholders in the fight to protect intellectual property rights.²²⁰

In terms of balance, WIPO’s materials are predictably maximalist in their representation of the scope of intellectual property rights, asserting, for example, that “[i]ntellectual property refers to all creations of the human mind.”²²¹ One exercise encourages students to think of all the products they can that “can be protected by more than one type of intellectual property.”²²² The WIPO authors do, however, discuss the public domain at length and prominently acknowledge a need to balance the rights of authors with the rights of the public.²²³ They also discuss Creative Commons licensing as an alternative to the traditional “all rights reserved” approach to protecting creative work.²²⁴

WIPO’s balance is not matched in materials from CSUSA, which are available in a section of the group’s web site called *Copyright Kids!*.²²⁵ The rationale for the site, which is directed at kids in fifth through eighth grade, is that “anyone who creates and/or uses copyrightable materials—including kids—[should] understand what the U.S. copyright law permits, what it restricts, and why.”²²⁶ The appeal to kids as intellectual property stakeholders is a common element between the WIPO and CSUSA materials; CSUSA declaims that kids should “care about copyright,” because “[a]s the creator of

pub_935.pdf.

217. *Id.* at 4.

218. *Id.* at 52.

219. *Id.*

220. *See id.* at 57 (encouraging kids to “use [their] imagination to create new, original works” and to “[l]ook for inspiration in the works of other authors, and respect their rights”).

221. *Id.* at 16.

222. *Id.*

223. *See id.* at 40-47.

224. *See id.* at 30.

225. CSUSA, Welcome to Copyright Kids!, <http://www.copyrightkids.org/> (last visited Dec. 7, 2009).

226. CSUSA, Copyright Kids! Parent-Teacher Resource Page, <http://www.copyrightkids.org/teachrentframes.htm> (last visited Dec. 2, 2009).

your work, you should have the right to control what people can and cannot do with [it].”²²⁷ The statement, which portrays copyright as a mechanism for guaranteeing authorial control over existing work, distorts the utilitarian underpinnings of copyright law and the constitutional emphasis on creating incentives for future production. In doing so, it inculcates in children a fundamental misunderstanding about the reasons for which copyright exists. CSUSA does explain that copyright is limited by the doctrine of fair use, but it warns kids in the same breath always to seek permission to use copyrighted works “unless you are absolutely sure” that the use is fair.²²⁸ Given that one can seldom, if ever, be “absolutely sure” *ex ante* that a given use is fair, CSUSA’s ultimate advice for kids working on yearbooks and other projects is in the true spirit of the “permission culture” advocated by corporate rights owners:²²⁹ “The best course of action is simply to seek permission for all copied material that you intend to use.”²³⁰

The RIAA itself offers a curriculum called *Music Rules!*, which it markets to teachers and parents as “a free educational program designed to encourage respect for intellectual property and responsible use of the Internet among students in grades 3-8.”²³¹ The primary goal of the program is not really to educate kids about intellectual property so much as it is to foster in them an aversion to P2P file sharing: “To help students recognize that taking music without paying for it (‘songlifting’) is illegal and unfair to others.”²³² Among the recommended exercises is one that has students interview their families and friends to “find out if songlifting is a real problem in [their] community.”²³³ Another has students calculate how much money is lost to industry stakeholders if every child between the ages of 8-13—3.9 million by the last census, students are told in a footnote—“songlifts” two songs that cost ninety-nine cents each.²³⁴

227. CSUSA, Copyright Kids! Copyright Basics, <http://www.copyrightkids.org/cbasicsframes.htm> (last visited Dec. 2, 2009).

228. *Id.*

229. See LAWRENCE LESSIG, FREE CULTURE xiv (2004) (defining a “permission culture” as “a culture in which creators get to create only with the permission of the powerful, or of creators from the past”).

230. CSUSA, Parent-Teacher Resource Page, *supra* note 226.

231. RIAA, Music Rules, <http://www.music-rules.com> (last visited Dec. 2, 2009).

232. RIAA, MUSIC RULES! TEACHERS’ GUIDE 2 (2009), <http://www.music-rules.com/pdf/MusicRulesTeacherGuide.pdf>.

233. RIAA, MUSIC RULES! MIDDLE SCHOOL ACTIVITIES 1 (2009), <http://www.music-rules.com/pdf/MusicRulesMidSchActivities.pdf>.

234. *Id.*

Kids are instructed in *Music Rules!* handouts to “[d]elete any music that you receive by email and remind the person who sent it that sending copies of copyrighted music is illegal.”²³⁵ The elementary school component of the curriculum culminates in the signing of a “pledge” by each student that he or she will, among other things, “respect all forms of intellectual property,” “obey . . . copyright laws,” and “never accept illegal copies of songs online or on disc.”²³⁶ Unlike the materials offered by WIPO and CSUSA, the *Music Rules!* curriculum makes no effort, not even a perfunctory one, to educate kids about the public domain, fair use, or other limitations on copyright. It purports to be informative about copyright law, but the information it conveys is functionally propagandistic within established sociological definitions of the term.²³⁷

Whether these educational programs are being widely adopted in schools or will prove successful at inspiring compliance is difficult to gauge. Programs that appear to be motivated more by corporate self-interest than by a disinterested desire to help kids think critically about the ethics of computing have already been opposed by groups like the American Library Association, which has produced its own curriculum as an alternative to corporate-sponsored programs like *Music Rules!*.²³⁸ To the extent that trusted organizations like the ALA oppose corporate-sponsored copyright education in schools, parents and educators are likely to be skeptical of it.

It may ultimately prove effective for rights owners to target young children, whose computer literacy and ethics are just developing. The true test of any educational effort directed at today’s elementary school kids will come when they enter their teen years and begin to see the attraction of

235. *Id.* at 5.

236. RIAA, MUSIC RULES! ELEMENTARY ACTIVITIES 5 (2009), <http://www.music-rules.com/pdf/MusicRulesElemActivities.pdf>.

237. Propaganda theorist Jacques Ellul wrote of the impossibility of “distinguish[ing] exactly between propaganda and information,” because “information is an essential element of propaganda.” JACQUES ELLUL, PROPAGANDA: THE FORMATION OF MEN’S ATTITUDES 112 (Konrad Kellen & Jean Lerner trans. 1972). Garth Jowett and Victoria O’Donnell describe the propagandist’s strategy of skewing information:

Information communicated by the propagandist may appear to be indisputable and totally factual. The propagandist knows, however, that the purpose is not to promote mutual understanding but rather to promote his or her own objectives. Thus, the propagandist will attempt to control information flow and manage a certain public’s opinion by shaping perceptions through strategies of informative communication.

GARTH S. JOWETT & VICTORIA O’DONNELL, PROPAGANDA AND PERSUASION 41 (3rd ed. 1999).

238. See Dean, *supra* note 215 and accompanying text. The EFF has also recently developed and publicized a copyright education curriculum. See EFF, Teaching Copyright, <http://www.teachingcopyright.org> (last visited Dec. 2, 2009).

online social networks, including file sharing networks. For now, the continued popularity of P2P file sharing on college and university campuses is strong proof that the entertainment industry has not been winning the hearts and minds of the nation's young.²³⁹ Since the early days of P2P, surveys have consistently shown that the majority of young people who download music and movie files illegally are either unconcerned about copyrights or do not regard the practice as morally problematic.²⁴⁰ They know they're doing something illegal, but they do it anyway.²⁴¹ What they lack is not awareness of the law but the inclination to comply, which comes in part from a perception that the law is out of step with community norms.²⁴² Tech columnist David Pogue has called it "the generational divide

239. The MPAA claimed in 2008 that 15% of its global losses in 2007, nearly a quarter of a billion dollars, were attributable to piracy on college and university campuses. See Press Release, MPAA, MPAA Statement on Motion Picture Industry Losses Due to Piracy Among College Students (Jan. 22, 2008), available at http://mpaa.org/press_releases/lek%20college%20student%20data_f.pdf.

240. In 2000, the Pew Internet and American Life Project found that 61% of those who downloaded music "did not care much about [its] copyright status." MIKE GRAZIANO & LEE RAINIE, PEW RESEARCH CTR., THE MUSIC DOWNLOADING DELUGE 6 (2001), http://www.pewinternet.org/~media/Files/Reports/2001/PIP_More_Music_Report.pdf.pdf. In 2003, the percentage of users surveyed who didn't care about copyrights had actually increased to 67%. MARY MADDEN & AMANDA LENHART, PEW RESEARCH CTR., MUSIC DOWNLOADING, FILE-SHARING AND COPYRIGHT 1 (2003), http://www.pewinternet.org/~media/Files/Reports/2003/PIP_Copyright_Memo.pdf.pdf. By 2004, the percentage was down to 58%, still a majority of respondents. See Rainie, et al., *supra* note 203, at 5.

Studies published more recently reveal that lack of concern for the copyright status of downloaded files is persistent, particularly among teenagers and college students. In 2008, a survey of teenagers commissioned by Microsoft found that less than half believed that any punishment was appropriate for illegal downloading, although 90% believed that punishment was appropriate for stealing a bike. See Press Release, Microsoft, *supra* note 212. Another study published in 2008 found that college students "did not appear to view music piracy as a transgression." See Rajiv K. Sinha & Naomi Mandel, *Preventing Digital Music Piracy: The Carrot or the Stick?*, 72 JOURNAL OF MARKETING 1, 13 (2008) (interpreting data collected in 2002, 2005, and 2006).

241. See Jon Cooper & Daniel M. Harrison, *The Social Organization of Audio Piracy on the Internet*, 23 MEDIA, CULTURE & SOC'Y 71, 87 (2001) (providing an "ethnography" of audio pirates and asserting that "[f]or many pirates, the question of copyright is simply irrelevant"); Press Release, Univ. of Richmond, *One in Three College Students Illegally Downloads Music, National Survey Finds* (April 4, 2006), available at <http://oncampus.richmond.edu/news/april06/survey.html> (reporting a finding in a national survey of college students that one in three who download music think it's wrong, but do it anyway to save money).

242. See, e.g., Janice Nadler, *Flouting the Law*, 83 TEX. L. REV. 1399, 1431 (2005) (arguing for a causal relationship between compliance with the law and perceptions that the law is morally credible and consistent with community values).

in copyright morality.”²⁴³ While it is surely the case that some illegal file sharers know not what they do, to believe at this stage of the game that online piracy is primarily the result of an educational deficit is to ignore an important body of data suggesting that, for very many file sharers, the law just doesn’t matter.²⁴⁴

CONCLUSION: TOWARD A VERSATILE EQUILIBRIUM?

A decade after Napster, copynorms remain far out of alignment with copyrights. Coercive regulatory interventions—both public and private—at the content, network, and user levels have failed to close the distance between them. As the social dynamics of file sharing have evolved, it has become clear that fixating for regulatory purposes on the evils of P2P networks and the moral failings of the people who use them has distracted corporate rights owners from the hard work of interrogating their own commercial behavior and the role it has played in both inspiring and perpetuating noncompliance.

Lately, however, there have been some promising signs of a shift in focus. On the music side, the legal offensive against individual file sharers has ended,²⁴⁵ songs sold through authorized online distributors are no longer locked by DRM,²⁴⁶ and three of the four major labels are exploring the option of blanket licensing.²⁴⁷ Behavioral changes also appear to be underway on the movie side. In a public relations move that Jack Valenti could never have predicted, the MPAA’s “Respect Copyrights” web site now refers prominently to industry efforts to “increase consumer options in the digital space” and “give consumers the flexibility the modern marketplace

243. See Pogue’s Posts, <http://pogue.blogs.nytimes.com/> (Dec. 20, 2007, 12:30 EST) (marveling at how few members of an audience of informally polled college students (i.e., 2 out of 500) thought there was anything wrong with illegal downloading).

244. See *supra* notes 240 and 241 and accompanying text.

245. See McBride & Smith, *supra* note 187 (reporting on the RIAA’s decision to end its legal campaign against individual file sharers).

246. See *supra* note 89 and accompanying text.

247. See Posting of Eliot Van Buskirk to Epicenter, <http://www.wired.com/epicenter/> (Dec. 8, 2008, 08:55 EST) (describing a blanket licensing scheme being proposed to universities that would “eliminate[e] some of the most irksome and contentious issues dividing the music industry and its customers”). Consumer advocates like the EFF have long advocated a collective licensing model. See FRED VON LOHMANN, EFF, A BETTER WAY FORWARD: VOLUNTARY COLLECTIVE LICENSING OF MUSIC FILE SHARING 1-2 (2008), <http://www.eff.org/files/eff-a-better-way-forward.pdf> (extolling the benefits of blanket licensing, modeled on the regime for broadcast radio, as a solution to the problem of illegal file sharing).

demands.”²⁴⁸ This focus on consumer choice and flexibility is a radical departure from the threats and finger-wagging that have, until now, marked the approach of both industries to deterring piracy.

Could it be that corporate rights owners, after a thankless decade in the trenches, are moving away from the politics of coercion and toward the versatile equilibrium of regulatory forces that Foucault recognized as the key to shaping behavior? They do seem to be recognizing, however belatedly, that file sharers will be more inclined to comply with copyright law if they are presented with better opportunities to get what they want legally, on more flexible terms than they have yet been offered. The notion that the big players in the entertainment industry should learn to stop worrying and love the Internet is nothing new. The novelty lies entirely in the fact that they could finally be coming around. Whether their awakening has come too late remains to be seen.

248. MPAA, Respect Copyrights—Digital Hollywood, <http://www.respectcopyrights.org/digital.html> (last visited Dec. 2, 2009).