2008

Filtering, Piracy Surveillance and Disobedience

Sonia K. Katyal
Fordham University School of Law, skatyal@law.fordham.edu

Filtering, Piracy Surveillance and Disobedience

Sonia K. Katyal*

On January 6, 2009, Apple made a surprising announcement: it declared that it had decided to remove anti-copying restrictions from all of the songs in its iTunes store, and also to forego charging a single price for each song. Instead, Apple would price some songs at 69 cents (rather than the standard 99 cents), and others slightly higher, depending upon their popularity.[1] Almost immediately, the decision caused a firestorm of commentary on the potential effects of Apple's decision on the future of the market for music, piracy and content distribution. "I think the writing was on the wall, both for Apple and the labels, that basically consumers were not going to put up with D.R.M. [digital rights management] anymore," one consumer analyst explained to the *New York Times*.[2] Music industry insiders applauded the decision, predicting that it would help lift the sagging market for music by enabling more creative strategies to serve a consumer base that increasingly favored more interoperability with digital forms of content.[3]

The decision was a culmination of Apple's longstanding position, advanced over a couple of years, that was markedly critical of DRM. In February of 2007, Apple CEO Steve Jobs wrote an open letter to the public criticizing DRM for its rigorous limitations on consumers. "Imagine a world where every online store sells DRM-free music encoded in open licensable formats," Jobs wrote. "In such a world, any player can play music purchased from any store, and any store can sell music which is playable on all players. This is clearly the best alternative for consumers, and Apple would embrace it in a heartbeat," he promised, so long as the big four music companies would license their music to Apple without the requirement that it be DRM-protected.[4] The letter prompted one recording company, EMI, to reach a

* Professor of Law, Fordham University School of Law; Visiting Professor of Law, Hastings School of Law (Spring 2009). The author would like to thank Margreth Barrett, Genevieve Blake, Jana Checa Chong, Brett Frischmann, Robin Feldman, Jeanne Fromer, Gregg Macey, Eduardo Moises Peñalver, Joel Reidenberg, Paul Riley and Olivier Sylvain for helpful discussions, in addition to June Besek, Jane Ginsburg, Scott Hemphill, my co-panelists, Anthony Reese and Miguel Peguera and the staff of the Journal of Law and the Arts. Paul Riley provided exceptional research assistance, as always. The author also gratefully acknowledges Evan Lee, Shauna Marshall, and Nell Newton, in addition to the Traynor fund at University of California, Hastings College of Law, for their support.

1. *See* Brad Stone, *Want to Copy iTunes Music? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 7, 2009, at B1.

2. *See id.*

3. *Id.*

4. *See* Steve Jobs, *Thoughts on Music*, Feb. 6, 2007, http://www.apple.com/hotnews/thoughtsonmusic/ (last visited Feb. 20, 2009).

deal that offered DRM-free music on iTunes, but other recording companies remained recalcitrant until they finally agreed to Apple's request two years later.[5]

There is, however, an important and overlooked footnote to Apple's much-heralded decision. More than a year and a half before Apple's groundbreaking decision, a web site, Ars Technica, announced an important discovery: every consumer's identifying information, including the user's full name and email address, came embedded on each song that was purportedly DRM-free.[6] In fact, Apple embedded account information on every song purchased by a consumer. "Previously," the Ars Technica journalist explained, "it wasn't much of a big deal, since no one could imagine users sharing encrypted, DRMed content. But now that DRM-free music from Apple is on the loose, the hidden data is more significant since it could theoretically be used to trace shared tunes back to the original owner," raising implications for both privacy and, of course, piracy as well.[7]

This outcome, in many ways, highlights a unique shift in approaches to copyright enforcement. While civil liberties advocates previously warned about the aggressive nature of copyright protection initiatives, like litigation, we have also watched a number of major players in the music industry eventually cede to less direct forms of control over consumer behavior. In fact, just a few months before Apple's announcement, the recording industry offered a major concession of its own when it announced that it had opted to end its infamous lawsuit campaign against end users. Instead of filing suit, the industry announced that it would simply notify the Internet Service Provider, or ISP, if the RIAA detects infringement. The ISP, in turn, will notify the user, and if the infringement continues, terminate the user's access in lieu of a lawsuit.[8]

Notice, however, that while the RIAA's litigation campaign has waned, it still fully intends to rely on active surveillance and monitoring of the web to detect infringement. Thus, as more aggressive forms of consumer control, like litigation, have receded, we have also seen a rise in more passive forms of consumer surveillance, such as Apple's embedding of consumer information. Moreover, at the same time that DRM technologies have taken a slightly less prominent role in governing consumers, filtering has radically escalated, raising slightly different issues about the risks of error and preservation of fair use protections in a digital context.

Given this background, the importance of Apple's decision could not be overstated among those who had long expressed concern about the balance that had been struck between the protection of intellectual property and the preservation of civil liberties. Apple's DRM-free music, while a major win for consumer autonomy in enjoying content, also, to some extent carries implications for the

5. Stone, *supra* note 1.

6. *See* Ken Fisher, *Apple Hides Account Info in DRM-Free Music, Too*, May 30, 2007, http://arstechnica.com/apple/news/2007/05/apple-hides-account-info-in-drm-free-music-too.ars (last visited Feb. 20, 2009).

7. *See id.*

8. Sarah McBride and Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1.

user's informational privacy. Why would Apple try to collect such information, the Ars Technica report asked? The article opined that the information might be useful for Apple to collect in aggregate, perhaps in order to detect possible examples of what the entertainment industry has termed "casual piracy," or the occasional content shared between friends.[9] While consumers might *seem* free to copy music onto their personal networks and devices, the unrelenting shadow of consumer monitoring and surveillance ensures that recordkeeping quietly continues to protect against piracy.

One *Wired* blogger summarized the relationship between the recording industry and Apple perfectly when he opined, "They may have thought they couldn't live together, but they certainly couldn't thrive apart."[10] The same observation, ironically, is equally true of the relationship between copyright protection and civil liberties. The Apple decision, therefore, gives rise to a variety of opportunities for reflection by scholars and copyright enthusiasts. While the music industry has been known to offer the public a broad definition of illegal piracy, Apple's decision to offer DRM-free music suggests a sort of private decriminalization of unauthorized activity (albeit with recordkeeping methods in tow). Further, even as technology has developed more perfect means for filtering and surveillance over online piracy, a number of major players have opted in favor of "tolerated uses," a term coined by Professor Tim Wu to denote the allowance of uses that may be otherwise infringing, but that are allowed to exist for public use and enjoyment.[11] Thus, while the eventual specter of copyright enforcement and monitoring remains a pervasive digital reality, the market may fuel a broad degree of consumer freedom through the toleration or taxation of certain kinds of activities.

This Article is meant largely to address and to evaluate these shifts by drawing attention to the unique confluence of two important moments: the growth of tolerated uses, coupled with an increasing trend towards more passive forms of piracy surveillance in light of the balance between copyright enforcement and civil liberties. The content industries may draw upon a broad definition of disobedience in their campaigns to educate the public about copyright law, but the market's allowance of DRM-free content suggests an altogether different definition. The divide in turn between copyright enforcement and civil liberties results in a perfect storm of uncertainty, suggesting the development of an even further division between the role of the law and the role of the marketplace in copyright enforcement and innovation, respectively.

I. NETWORKS OF DETECTION

Intellectual property frameworks play two conflicting roles in digital space; at the same time that these frameworks govern the various content—music, pictures, film, software, web sites—that individuals utilize and access on the Web, these

9. *See* Fisher, *supra* note 6.

10. *See* Posting of Eliot Van Buskirk to Epicenter, http://blog.wired.com/business/ (Jan. 6, 2009, 15:41 EST).

11. Tim Wu, *Tolerated Use*, 31 COLUM J.L. & ARTS 617 (2008).

same frameworks also govern the creation, assembly and collection of consumer information through techniques of data mining and surveillance. For this reason, any specter of copyright enforcement always raises the risk of constant tradeoffs being made between intellectual property protection and consumer expectations in privacy and freedom of expression online. As the result of the DMCA, the conflict between intellectual property and civil liberties becomes focused almost entirely on the role of intermediaries, and the ideal role they should play in protecting the balance between the two interests. As Rebecca Tushnet has insightfully observed, the DMCA's regulation of intermediaries shows that it is possible to shape the contours of the marketplace of speech even without an intention to do so directly.[12]

Ten years ago, Congress unwittingly crafted the first real framework for piracy surveillance when it confronted the proliferation of online content and the need for the law to respond to the dangers of massive online infringement and unrestrained defamation. As many scholars have analyzed at great length, the perceived anonymity of cyberspace initially encouraged private citizens to adopt certain identities, engage in particular expressions and undertake certain activities they would probably never think to adopt in real space.[13] While the perceived anonymity of cyberspace seemed filled with endless possibilities of human expression, it also offered a tantalizing cloak for individuals who chose to engage in the online sharing and trading of content without authorization. One scholar deemed the internet a "Temporary Autonomous Zone," or TAZ, suggesting that online content was free for the taking, having been freed from the constraints of copyright regulation in the real world.[14]

These two developments—the increasing prominence of an electronic persona, coupled with an explosion of content—may seem distinguishable, but they are intimately related, and both developments increasingly focus on the role of the ISP in negotiating these trajectories. While the growth of the internet led to an immense explosion of content—music, computer software, and other media—it also spawned a number of difficult challenges regarding the protection of copyrighted works from unauthorized distribution. Put another way, the internet created a broadcast media that is permeated with potential for creativity and communication, but it also provided the mechanism for massive infringement.

The answer to these challenges, it seemed, was to focus primarily on reconfiguring the role of the intermediary in enforcing copyright protections. As Professor Edward Lee has eloquently explained, the Digital Millennium Copyright Act (DMCA) is composed of two principal, and potentially conflicting, elements: Title I, which expanded the scope of copyright protection by establishing protections against the circumvention of DRM restrictions; and Title II, which contracted the scope of copyright by establishing a set of safe harbors for Internet

12. *See* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1004 (2008).

13. *See* SHERRY TURKLE, LIFE ON THE SCREEN (1995).

14. *See* Hakim Bey, *The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*, at http://www.hermetic.com/bey/taz_cont.html (last visited June 25, 2009).

Service Providers (ISPs) to protect them from monetary liability.[15]

Title II represented an uncertain balance between preserving innovation and protecting against digital copyright infringement. To protect both dimensions, the DMCA distinguished between actions either directly (or indirectly) required of a copyright owner from those required of an Internet Service Provider. In choosing to implement Title II of the Digital Millennium Copyright Act, Congress rejected the option of imposing an absolute standard of liability for Internet Service Providers. Instead, Congress' answer to these tensions lay in a finely crafted compromise, known as a "notice and takedown" system, which required copyright holders to search the web to identify instances of infringement, and then, after undertaking an identification process, to request that the ISP "take down" the offending content. Under these provisions, an ISP is required either to identify the subscriber and/or to take down the posting as long as the copyright owner makes an assertion of a "good faith" belief that infringement has occurred.[16] In order for the Internet Service Provider to take advantage of the safe harbor provided in DMCA legislation, the ISP is required to act expeditiously in doing so.

It is important to note, however, that the DMCA did not place an obligation on the part of the ISP to actually *detect* instances of infringement on its own. Instead, under the DMCA, the responsibility for such a task fell largely to copyright owners, indirectly authorizing them to perform the arduous, though at times necessary, task of trolling and investigating web sites, peer-to-peer and other forms of plural networks to detect potential examples of infringement.[17] As a result, creators of intellectual property drew upon traditional methods of consumer surveillance—collecting information, surreptitious monitoring, recording one's online activities—to detect instances of piracy, employing the ISP as an intermediary in their efforts. In the past, I have defined "piracy surveillance" to encompass particular types of monitoring that: (1) are performed by private, non-government entities; (2) encompass extra-judicial determinations of copyright infringement and (3) are extra-legal in nature; that is, surveillance that takes place outside of ongoing litigation.[18]

Each of these activities has grown in the past few years, spawning a small cottage industry of anti-piracy enforcement technologies. For example, Audible Magic—the favored tool of MySpace.com and others, including over seventy-five universities—operates by scanning online for copyrighted material and then checking against a massive database of audio and video content that has been provided by the recording industry, and movie and television studios.[19] Other companies offering piracy surveillance services include Gracenote, advestigo,

15. *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233 (2009).

16. *See* Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 273 (2004-2005) (explaining provisions).

17. For more discussion of the techniques relied upon by intellectual property owners, see Part II; Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2003); Katyal, *supra* note16.

18. Katyal, *supra* note 16, at 292.

19. *See* Michael Liedtke, *Audible Magic Emerging as Top Copyright Cop in Digital Revolution*, USA TODAY, Mar. 23, 2007, http://www.usatoday.com/tech/news/techinnovations/2007-03-23-magic-police_N.htm.

Auditude, Vobile, and Attributor, enabling copyright owners to "scan the entire Internet to uncover the unauthorized use of the material."[20] All of these strategies place the responsibility for infringement detection squarely upon the copyright owner. As an executive from the Internet Service Provider community explained:

> We believe that the task of ferreting out copyright infringement on the Internet should fall to the copyright owner. Today, copyright owners have access to a large array of Internet search engines and "spiders" to sniff out material they know belongs to them (unlike the ISPs, who cannot be certain who may have recently purchased which copyrighted material.) Once the copyright owners discover infringement, they can bring it to the attention of the ISPs. It is at this point that the ISPs can sensibly act.[21]

As a result of the DMCA, intellectual property owners have undertaken a program of monitoring for piracy, and ISPs have developed a response system that acts to "take down" allegedly infringing material in order to avoid allegations of contributory liability as a result.[22]

Although piracy surveillance was borne out of this compromise between copyright owners and ISPs, its function and operation in cyberspace masks several powerful unintended consequences. The most glaring of these ironies, for our purposes, lies in a key ambivalence regarding the proper role of ISPs. Intermediaries like ISPs play a key role in enforcing copyright law for two reasons. First, they serve as the conduit by which the intellectual property owner identifies the subscriber, and second, under the DMCA, they are forced either to take down the infringing material or to terminate internet access to the subscriber. Thus, they are often the only barriers between ordinary citizens and the surveillance measures used by content owners to identify them. As a result, ISPs are often caught between two conflicting motivations: the need to protect others' intellectual property to avoid liability and the need to protect their consumers' privacy and fair use in uncertain cases.[23]

These conflicting motivations often impose a much more malleable and ambiguous set of responsibilities on the part of the ISP. The DMCA expressly lacks an affirmative requirement for ISPs to monitor their systems or to seek facts that indicate infringing activity, ostensibly since copyright owners are expected to fulfill this responsibility.[24] In fact, as Professor Lee explains in his article, Congress "sought to avoid creating perverse incentives that would turn ISPs into effective censors of material, indiscriminately removing vast amounts of content to

---

20. Liedtke, *supra* note 19, at 1.

21. *See WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 105th Cong. 89 (1997) (statement of Roy Neel, President, United States Telephone Association).

22. *See* Katyal, *supra* note 16, at 278.

23. *See id.* at 276.

24. *See* Lee, *supra* note 15 at 254. Pursuant to § 512(m), the DMCA safe harbor protections are not conditional upon a service provider "monitoring its service or affirmatively seeking facts indicating infringing activity." 17 U.S.C. §512(m)(l), cited in Brian Yeh, *Safe Harbor for Service Providers Under the Digital Millennium Copyright Act*, available at: ipmall.info/hosted_resources/crs/ RL32037_030815. pdf at 8.

avoid liability . . . ."[25] Nor, it seems, did Congress want to require ISPs to make difficult decisions regarding whether an activity counts as infringement or not.[26] Instead, the wording of the DMCA requires that an ISP remove potentially infringing material if the ISP has "*actual* knowledge" of the infringing material, or if it is "aware of facts or circumstances from which infringing activity is apparent," and the knowledge standard tends to utilize a comparably much higher standard of proof to satisfy the "awareness" prong.[27] While the Senate Judiciary Committee suggests the need to judge "aware[ness]" from both a subjective and objective perspective, in which it explores both the actual state of mind of the ISP as well as "whether infringing activity would have been apparent to a reasonable person," this malleable standard often offers little concrete guidance for an ISP in evaluating its own policies and procedures.[28] The law suggests that the ISP is required to act expeditiously, but it does not provide any guidance for the ISP in addressing the merits of the accusation, suggesting, perhaps indirectly, that the ISP is required to simply defer to the copyright owner's overall determination instead.

The legislative history that Lee relies upon suggests that for infringing activity to be "apparent," it must be "obviously" or "clearly" infringing, such as a "pirate" site "where sound recordings, software, movies, or books were available for unauthorized downloading, public performance, or public display."[29] In such cases, the Senate reports direct that most sites actively rely upon words like "pirate" or "bootleg" in their titles, enabling an observer to note the illegal nature of their activities "from even a brief and casual viewing."[30] As Lee explains, Congress may have required such a high standard because it did not want to saddle ISPs with the difficult task of trying to make complex copyright determinations, given the myriad grey areas of legality in defining illegal activity. Cases such as *Perfect 10, Inc. v. CCBill, LLC* tend to bolster this view.[31] In *Perfect 10*, the Ninth Circuit held that the use of domain names like "illegal.net" and "stolencelebritypics.com" did not provide the requisite evidence of outright illegality, because the use of the terms might suggest "an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen."[32]

Yet while the law clearly weighs against requiring affirmative searches for infringement, and in favor of a high degree of awareness of illegality for liability to attach to an ISP, common law appears to be moving in a direction that suggests an increasing obligation on the part of ISPs to monitor the activities of their

25. *See* Lee, *supra* note 15, at 254.

26. *See id.* (citing both Senate and House reports).

27. *See id.* at 234 (quoting 17 U.S.C. § 512(d)(1) and 17 U.S.C. § 512(m) (2000)) (emphasis added).

28. *See id.* at 235 (quoting S. REP. 105-190, at 44).

29. *See id.* at 255-256 (quoting S. REP. 105-90, at 48-49).

30. *See id.* at 256 (quoting S. REP. 105-90, at 48-49).

31. 488 F.3d 1102 (9th Cir. 2007).

32. *Id* at 1114. In another case elaborating on this standard, the ISP had to be able to tell, just from looking at the user's activities, that the conduct constituted copyright infringement. *See* Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d. 1090, 1104-05 (W.D. Wash. 2004).

subscribers through the use of filters in order to avoid secondary liability. Here, the law's growing emphasis on filters contravenes, at least somewhat, the DMCA's language, which directly states that "websites have no affirmative duty to monitor their services or to "affirmatively seek[] facts indicating infringing activity."[33] As a result, the law sets forth a strained position for ISPs: even though ISPs are not required to "affirmatively" seek out information of infringement, the law has directed that an ISP who remains aware of infringement and fails to act risks liability.

The resulting inconsistency between the DMCA that expressly does not require affirmative monitoring of its users, and a common law trend that tends to indirectly expand the boundaries of secondary liability for ISPs often means that the law incentivizes risk averse content distributors to adopt preventative measures, i.e. filtering, in order to detect infringement before content is posted.[34] Filtering, like other *ex ante* methods of preventing copyright infringement, when coupled with the existing DMCA notice-and-takedown process, tend to redefine, and potentially expand, the responsibilities of Internet Service Providers, despite the DMCA's statutory assurances that presumably insulate ISPs from affirmatively searching for evidence of infringement.

Though Section 512 aims to split the burden of copyright enforcement between the copyright owner and the ISP, a chorus of case law has emerged that suggests that the boundaries of ISP responsibility are far broader than the DMCA standards suggest, requiring ISPs to undertake preventative precautions, like filtering, to deter infringement. Consider the Supreme Court's opinion in *Grokster*, for example, which tended to utilize a malleable standard of liability that leans towards increasing responsibility for the ISP.[35] The opinion set forth the requirement that a computer system operator possess "actual knowledge that specific infringing material" is on its system, and fail to undertake "simple measures" to remove the material.[36] At the same time, however, the Court found that the *absence* of filters was a significant part of its finding of contributory liability. The court found evidence of the defendants' unlawful intent because "neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software." Even though the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activity, as per the wording of the DMCA, the Supreme Court disagreed with the lower court, and stated instead that the evidence "underscores Grokster's and StreamCast's intentional facilitation of their users' infringement."[37] In other words, by finding the absence of filtering to be significant to the defendants' illegal inducement of infringement, the Court indirectly imposed an expectation that filtering would become part of the design of content distribution as

33. 17 U.S.C. § 512(m) (2000).

34. See James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882 (2007).

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

36. *See* Perfect 10, 508 F.3d at 1170-72 (citing *Grokster*, 545 U.S. at 929-32).

37. *Metro-Goldwyn-Mayer Studios Inc.*, 545 U.S. at 939 (2005).

a result.

Grokster therefore places intermediaries on uncertain footing, perhaps in part due to the polarity between these statutory and common law positions. The DMCA expressly states that an affirmative search for infringement is not required, but the Supreme Court's analysis in *Grokster* suggests that the absence of filters is a relevant part of the contributory liability framework, leaving intermediaries lost in the middle. While ISPs, left to their own devices, would probably opt against affirmative searches of their clients' sites for evidence of infringement, *Grokster*'s inducement theory of liability, coupled with the Supreme Court's finding that the absence of filtering was statutorily significant, tips the scale further toward incentivizing ISPs to behave more like a copyright enforcer than the DMCA's original compromise might have envisioned.

For an example of how this uncertain status of affairs affects ISPs, consider the *Aimster* case, handed down a few years before *Grokster*.[38] Unlike Napster and Grokster, which enabled a relatively transparent exchange of copyrighted files, Aimster encrypted files before circulating them. Consequently, the court concluded that "a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used."[39] Following *Sony*, the court observed that, "[b]y eliminating the encryption feature and monitoring the use being made of its system, Aimster could have limited the amount of infringement."[40] Given Aimster's failure to do so, the court concluded that "its ostrich-like refusal to discover the extent to which its system was being used to infringe copyright is merely another piece of evidence that it was a contributory infringer."[41] Central to the court's determination was the need for a cost/benefit showing that demonstrated "that it would have been disproportionately costly for [the defendant] to eliminate or at least reduce substantially the infringing uses."[42] This finding has been interpreted by some to suggest that the defendant has to defend its design choices by showing that it would be prohibitively expensive to redesign its software—further suggesting that developers that opt against designs that inhibit infringement risk secondary liability.[43]

The consequence of this protracted trend towards filtering starts looking a great deal more like an affirmative obligation from the point of view of an ISP. If the "profit motivated failure to filter promotes an inference of intent to induce infringement" under *Grokster*, then it may also be true, as Tim Wu has suggested, that the presence of some filters establishes a kind of informal "safe harbor" from contributory liability.[44] This amounts to, of course, the suggestion that a

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

39. *Id.* at 650-51.

40. *Id.* at 654-55.

41. *Id.* at 655.

42. *Id.* at 653.

43. *See* Rebecca Giblin, *A Bit Liable? A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMPUTER & HIGH TECH L.J. 7, 36 (2008-2009).

44. 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, 587 (citing

technology developer that opts against installing a filter (or a similar mechanism) might risk facing secondary liability for infringement.[45]

Yet by suggesting that the failure to filter might support a claim of contributory liability, the Court left open the question of how much filtering is required, and how reliable the filtering must be. How much filtering is enough? And should the law require filtering, even at the expense of cabining valuable noninfringing uses? Even in the aftermath of the case, the district court in *Grokster* conceded, on remand, that perfect filtering was likely an impossible goal.[46] Nevertheless, the court concluded that the defendants must include a filter and encourage users to upgrade to filtered software.[47] However, it was careful to note that "[p]laintiffs' copyrights can be protected to the extent feasible, but Morpheus's noninfringing uses will not be completely enjoined," and decided to appoint a special master for the purpose of preserving the balance between utilizing a filtering regime to reduce the software's infringing capacity while preserving noninfringing functionality in light of potential cost concerns.[48]

As a result, the DMCA's assurances that initially insulated an ISP from the responsibility of "affirmative monitoring" appear to have receded into the background of common law findings that place a greater amount of responsibility on the ISP. In the famous suit filed against YouTube, for example, Viacom alleged that YouTube had "deliberately chosen not to take reasonable precautions to deter the rampant infringement on its site," arguing that it was not possible for "copyright owners to monitor YouTube on a daily or hourly basis to detect infringing videos and send notices to YouTube demanding that it 'take down' the infringing works."[49] The suggestion was that the responsibility to monitor should lie with YouTube, not Viacom.

Note the irony of what Viacom observes: that it is simply not possible for Viacom to monitor YouTube's content. But Viacom's observation suggests an important shift in the framework that the DMCA authorizes—Viacom no longer wants to carry the responsibility of determining infringement; instead it delegates this responsibility to YouTube to take up the reins. But if Viacom is not in a position to detect infringement, then who is? A copyright owner might opt for a system that is overinclusive of examples of actionable infringement, whereas an ISP might opt for a system that is underinclusive. The absence of a clear governing standard forces us to contemplate the tremendously powerful effect of this state of

---

Tim Wu, *The Copyright Paradox*, 2005 SUP. CT. REV. 229, 247).

45. *See* Pamela Samuelson, *Three Reactions to MGM v. Grokster*, 13 MICH. TELECOMM. TECH. L. REV. 177, 192 (2006).

46. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197, 1235 (C.D.Cal. 2007).

47. *See id.* at 1236.

48. *See id.* at 1236-37.

49. Complaint at 3, Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008) (No. 07 Civ. 2103). *See also* statement of Phillipe P. Dauman, President and CEO of Viacom, "[e]very day we have to scour the entirety of what is available on YouTube, so we have to look for our stuff . . . It is very difficult for us and places an enormous burden on us." Miguel Helft, *WhoseTube?: Viacom Sues Google over Video Clips on its Sharing Web Site*, N.Y. TIMES, Mar. 14, 2007, at C4.

affairs on content dissemination models and innovation. When YouTube adopted filters, for example, one commentator drily noted: "[Its] action today may have the practical effect of changing filtering from 'one' factor'[sic] to 'the' factor that a court considers in deciding whether an innovator should be liable for the copyright infringement of others."[50]

II. NETWORKS OF DISOBEDIENCE

The domains of piracy surveillance—filtering, monitoring, and the like—often mask a crucial, and foundational ambiguity: it is sometimes hard to tell at the outset whether user generated content is legal or not. At times, the decision to post copyrighted material crosses a perfectly clear line between legal and illegal conduct, making the "outlaw" moniker an appropriate one. In many cases, however, the boundaries of intellectual property rights are frequently unclear, leaving the legality of seemingly transgressive actions open to dispute. Consider the widely-watched mashup video entitled "Brokeback to the Future," which featured a variety of clips from the *Back to the Future* film series, set to the background score of *Brokeback Mountain*, the blockbuster from 2006. The clips were not actually digitally transformed, but they were remixed in a completely unique and creative manner to suggest the presence of a love relationship between Michael J. Fox and Christopher Lloyd's characters. Should the mashup count as fair use? Would YouTube's filters detect them? And if so, how would YouTube decide whether the content was legal or illegal? The answer might depend on how broadly (or narrowly) one interprets the definition of "transformative."

If law professors disagree on the meaning of such a contested term, it becomes even more likely that a copyright owner would generate a notice in even borderline cases, and even more likely that a risk-averse ISP would respond immediately by taking down the material in order to preserve its safe harbor status. Given the potential for divergent opinions over what constitutes fair use, it is often difficult to define what digital illegality comprises. Is it defiance of the law, or defiance of the wishes of a copyright owner, or both? If the conduct is not clearly illegal, how can it be considered copyright 'infringement' or 'piracy'?

Although copyright owners, particularly as they rely on the domain of piracy surveillance to detect infringers, may label all such detected behavior as "illegal," and refer to their adversaries as outlaws or pirates, the murkiness of intellectual property rights often makes it very difficult—in the absence of protracted litigation—to determine conclusively that the behavior in question is actually contrary to the law. Those who engage in intellectual property disobedience are therefore often in a position to counter that their actions are perfectly lawful under, for example, expansive conceptions of constitutional rights of free speech or of the fair use doctrine. Alternatively, they might argue that the law may not yet have developed a cohesive viewpoint on the activity. But at the outset, it is difficult to

50. Gigi Sohn, *Google Blinks, and Today the Internet is a Little Less Free*, PUB. KNOWLEDGE, Oct. 15, 2007, http://www.publicknowledge.org/node/1217.

say what a court will decide, and this suggests a greater degree of legal uncertainty than in a typical case of tangible property disobedience, civil or otherwise.

As Joseph Liu aptly pointed out in an earlier symposium piece in this Journal, the uncertainty that pervades copyright does not mean that there are not easy cases.[51] But the uncertainty over what constitutes fair use, particularly in cases of appropriation of content, often risks chilling the transformative work of artists who seek to incorporate the work of others.[52] Even though unauthorized activity takes place in both the physical property and intellectual property context, intellectual property law, particularly copyright, has tended to tolerate a greater degree of legal "grey" areas than have other types of property regulation. There are several reasons for this. One stems from the formal dynamism and complexity typical of intellectual property regulation. The type of property in question lacks the clear legal boundaries typical of land parcels and other tangible properties. Another is the murkiness of the extra-legal social and cultural norms that govern authorized uses, particularly in the areas of copyright and trademark. Consider, for example, the number of times individuals have copied, shared or distributed copyrighted music without acquiring permission beforehand. Were these acts of sharing always illegal? Many people never considered the possibility that these sorts of activities might be illegal until technological advances made it possible, particularly in the online context, for intellectual property owners to detect and punish them.

Throughout legal history, property principles historically developed through a series of chaotically eloquent metaphors—the "bundle of sticks," for example—that eventually came to be applied, through various parallels, to its milder cousin, intellectual property. Yet while these parallels between land and literature are useful in analyzing the limits and the possibilities behind the protection of intellectual property, they have given us little guidance in analyzing the diverse problems that are posed by the nature of cyberspace.[53] While property concepts tend to focus on the stability of commodities, intellectual property involves protecting an intangible, unstable and easily transferable good—a good that attaches itself to evanescent ideas, characters, identities and inventions. Moreover, unlike real property, intellectual property carries with it a host of inherent limitations on both access and use—durational limits, fair use exceptions, licensing restrictions—that often serve to complicate an intellectual property right by simultaneously limiting and strengthening it at different points, depending on the type of use, the type of intellectual property and the identity of the interested party.

If the boundaries of intellectual property are porous and often ill-defined, it makes the *defenses* to infringement even more so. Rather than establishing clear rules as to which uses of copyrighted material are permitted and which are not (rules that would provide unambiguous and accurate guidance to intellectual property users), the fair use test sets forth a series of factors that courts are to weigh

51. *See* Joseph P. Liu, *Constitutional Challenges to Copyright: Copyright and Breathing Space*, 30 COLUM. J.L. & ARTS 429, 435 (2007).

52. *Id.* at 434.

53. This section is drawn from EDUARDO MOISES PEÑALVER AND SONIA K. KATYAL , PROPERTY OUTLAWS (Yale Press, Forthcoming 2010).

in determining whether or not a particular use is lawful or infringing. As a consequence of its judicial malleability, the fair use test offers prospective fair users precious little guidance in determining how far they can go without crossing the boundary between lawful fair use and unlawful infringement. The consequence of this for copyright is that, unlike disobedience in real property which often involves the violation of clearly established legal norms, for an enormous number of uses of copyrighted material, it may be genuinely impossible to say *ex ante* whether the user is or is not an "outlaw."

Yet the delegation that piracy surveillance facilitates to the ISP through the DMCA's notice-and-takedown system enables no one but the copyright owner to make this determination. Given the risk of such pervasive inequality of both power and access to enforcement, the expansive legal claims of intellectual property owners have the tendency to take on the force of law, even in the absence of an objective legal basis for those claims. From the point of view of the intellectual property consumer or the small-scale creator, disobeying the commands of entrenched owners can feel just like (and have precisely the same consequences as) violating a clearly established legal norm.

Admittedly, there can be no question that piracy surveillance has grown much more sophisticated than in prior years, moving from a reliance on digital "hash" marks (which could be easily circumvented by changing a file) to more formidable (and reliable) acoustic or digital fingerprints. Sony and Universal rely heavily, for example, on the use of watermarks that can be traced on peer-to-peer networks.[54] Especially with respect to video content, however, most surveillance techniques cannot seem to discern whether the "match" is the result of verbatim infringement, or whether it is included as a clip in a longer piece. As a result, commentaries (like Michelle Malkin's piece on the rapper Akon) can be easily mistaken for infringing content without careful human supervision and attention for transformative uses.[55]

Consider the effect of piracy surveillance campaigns on the traditional "grey" areas of copyright legality—fan fiction, mashup creations and others.[56] Intellectual property owners regularly troll the internet looking for unauthorized uses of their content, and they often rely on automated strategies of detection that are overbroad, generating the risk of erroneous notification. Such monitoring, which often reflects similar strategies to those undertaken by classic consumer surveillance techniques, risks chilling either the creation or distribution of such content, even when individuals might have credible claims of fair use.[57] Although the DMCA does

54. David Kravets, *Analysis: FCC Comcast Order is Open Invitation to Internet Filtering*, WIRED, http://blog.wired.com/27bstroke6/2008/08/analysis-fcc-co.html.

55. Fred Von Lohmann, *YouTube's Copyright Filter: New Hurdle for Fair Use?*, ELECTRONIC FRONTIER FOUNDATION, Oct.15, 2007, http://www.eff.org/deeplinks/2007/10/youtubes-copyright-filter-new-hurdle-fair-use.

56. *See* Sonia K. Katyal, *Performance, Property, and the Slashing of Gender in Fan Fiction*, 14 J. OF GENDER, SOC. POL'Y, & L. 463 (2006).

57. The RIAA maintains a team of Internet specialists and an automated 24-hour web-crawler, a "bot" that continually crawls through the Internet to identify allegedly infringing activities. Once it locates the song, it notifies the ISP to terminate the person's online connection until she removes the offensive copy. The RIAA's software robot, dubbed Copyright Agent, has served millions of copyright

have a counter-notification process that allows a person to challenge the determination of infringement and restore access to the material, evidence suggests that most individuals fail to counter-notify even when they might have valid defenses.[58] As a result, significant fair use problems plague piracy surveillance techniques, because they can easily mistake legitimate files for copyrighted works.[59] Consider the following:

- In May 2003, the Recording Industry sent a notice to Penn State University after one of its "bots" detected an MP3 with the name "Usher" on the title.[60] The RIAA alleged that someone in the astronomy and astrophysics department had illegally uploaded songs by the artist for free distribution. However, they were sorely mistaken: it turns out that a member of the department's faculty, Professor Usher, had uploaded an a cappella mp3. Although the RIAA took responsibility for the mistake, it also admitted that it had sent out dozens of mistaken notices in the past, and at times, did not always fully confirm a suspected case of infringement.[61]

- In another widely reported case, the RIAA accused a sixty-six year old retired school teacher of downloading "I'm a Thug" by hip hop artist Trick Daddy, despite the fact that the woman's computer, a Mac, could not even host the alleged file-sharing program Kazaa.[62]

- A DMCA notice was generated after a "bot" detected a Prince song on YouTube, prompting a takedown. The video was a 29 second clip of a mother's infant son dancing to Prince's "Let's Go Crazy."[63]

---

violation notices to ISPs on behalf of hundreds of song writers and performers. *See* Katyal, at *supra* notes 16 and 17. Similar technologies are used by the Motion Picture Association of America, the Business Software Alliance, and the American Society of Composers, Authors and Publishers. Robert G. Gibbons & Lisa M. Ferri, *The Legal War Against Cyberspace Privacy*, N.Y. L.J., Aug. 5, 1999, at 1.

58. *See* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, *supra* note 12 at 1003. In the first empirical study of 512 notices, Jennifer Urban and Laura Quilter's findings suggest that 30% of 512 notices asserted copyright infringement where the notice raised "significant questions related to the underlying copyright claim, including fair use defenses, other substantive defenses, very thin copyright, or non-copyrightable subject matter." Jennifer M. Urban & Laura Quilter, *Efficient Process of "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 667 (2006).

59. *See Piracy of Intellectual Property on Peer-to-Peer Networks: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property*, 107th Cong. 23 (2002) (statement of Gigi B. Sohn, President, Public Knowledge).

60. *See* Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH J.L. & TECH. 13, 34 (2008), http://law.richmond.edu/jolt/v14i4/article13.pdf; Urban & Quilter, *supra* note 58.

61. Mulligan, *supra* note 60, at 34.

62. *Id.* at 35.

63. *See* EFF.org, Lenz v. Universal, http://www.eff.org/cases/lenz-v-universal (last visited Apr. 3, 2009).

- In an even more dramatic case, media giant Viacom threatened a satirical parody of comedian Stephen Colbert that was created by Moveon.org. Entitled "Stop the Falsiness," it included clips from the show, as well as interviews about Colbert.[64] Although Viacom at first denied sending the notice, it eventually admitted its error and took a number of positive steps towards safeguarding fair use. These steps included setting up a hotline and web site to review complaints from its notices.[65]

- In another case, an eight-second clip used in a thirteen minute video was taken down by YouTube.[66]

- Warner Brothers, owner of the copyright to "Harry Potter and the Sorcerer's Stone," sent a notice to ISP UUNet asking it to disable a user's internet access because of a single (allegedly infringing file) titled "harry potter book report.rtf."[67]

- The Business Software Alliance targeted a company who used a software named "Open Office," sending it a false form notice that it was making copies of Microsoft Office available simply because its "bot" detected the use of the word "office" in the program.[68]

It is true that some major content providers are careful to use a variety of means to protect fair use, including: (1) manual review of potential takedown targets; (2) training of reviewers to understand what may constitute fair use; and (3) claiming to avoid takedown notices for works that are "creative, newsworthy or transformative" or limited excerpts.[69] But as the examples above establish, no system of filters is ever foolproof, and the risk of chilling legitimate expression is highly pronounced in such a system of piracy detection that relies so heavily on automation.

Given the reach of piracy surveillance strategies, there is also a significant risk that internet intermediaries, particularly service providers, will increasingly be asked to play visible and powerful roles as "proxy censors," as Seth Kreimer has termed their new role.[70] However, enabling a copyright owner to determine what

64. *See* EFF.org, *MoveOn,* Brave New Films v. Viacom, http://www.eff.org/cases/moveon-brave-new-films-v-viacom (last visited Apr. 3, 2009).

65. *Id.*

66. *See* EFF.org, Sapient v. Geller, http://www.eff.org/cases/sapient-v-geller (last visited Apr. 3, 2009).

67. *See Piracy of Intellectual Property on Peer-to-Peer Networks: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property*, 107th Cong. 29 (2002) (statement of Gigi B. Sohn, President, Public Knowledge).

68. *See* Posting of Declan McCullagh, declan@well.com, to politech@politechbot.com (Feb. 28, 2003) (available at http://www.politechbot.com/p-04511.html).

69. *See* EFF.org, MoveOn, Brave New Films v. Viacom, *supra* note 64 (describing Viacom's practices).

70. *See* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11 (2006).

counts as fair use raises the important question of whether the DMCA should be delegating such a delicate responsibility to the party who may have a powerful motivation to censor the material. After all, copyright owners have the strongest incentives to claim copyright infringement, particularly in cases where they might prefer to censor or silence threatening or critical speech. For example, when Savitri Durkee, a city activist, created a web site parody of New York City's Union Square Partnership (a private group that supports redevelopment of the neighborhood), the Partnership sent a DMCA notice alleging that her parody infringed its copyright.[71] (The case eventually settled, but not before Durkee was forced to contact the Electronic Frontier Foundation for a defense). In another case, an organization posted videos exposing nearly two dozen incidents of animal cruelty at rodeos; YouTube promptly took down the videos and even cancelled the animal advocates' registration, even though the alleged copyright owner (the Professional Rodeo Cowboys Association) did not own a copyright in the taping of the live rodeo events.[72] Other DMCA notices have been generated for blocking trademark uses instead of copyright uses.[73] And, in many of those cases, claims of copyright infringement might never have made it to court because of their weak merits. However, the DMCA notice and takedown system creates a world that incentivizes ISPs to respond by taking down material almost immediately, even in hard cases, and largely without any substantive judicial oversight or intervention.

Given the array of issues that arise with a DMCA notice-and-takedown regime that delegates responsibility to copyright owners, it is also important to note that ISPs are also saddled with their own host of concerns regarding their roles in safeguarding against piracy. Some ISPs, for example, have opted for even more restrictive controls over their networks by prohibiting certain types of peer-to-peer software, and are substantially aided in this effort by piracy surveillance techniques. To the extent that doctrines like network neutrality operate as safeguards for the freedom of expression, the chilling effect that is raised by these may raise deeper structural concerns about the open nature of the internet. Consider Audible Magic's position, favoring a high degree of delegation to the network owner to determine the boundaries of allowable uses:

> We feel strongly that network owners have the right to dictate how their networks are used. If a network owner chooses to create a policy that no copyright [sic] works may be transferred over their networks, then they should be free to use technology to enforce those policies. That is where Audible Magic fits in.[74]

This reasoning has been increasingly challenged recently, culminating in a powerfully worded FCC decision which ordered Comcast to stop throttling traffic

---

71. *See* EFF.org, USP v. Durkee. http://www.eff.org/cases/usp-v-durkee (last visited Apr. 3, 2009).

72. *See* EFF.org, SHARK v. PRCA, http://www.eff.org/cases/shark-v-prca (last visited Apr. 3, 2009).

73. *See* EFF.org, Jones Day v. Blockshopper, http://www.eff.org/cases/jones-day-v-blockshopper (last visited Apr. 3, 2009).

74. Letter from Audible Magic to a subscriber (July 15, 2004) (available at http://w2.eff.org/share/audible_magic.php?f=audible_magic_letter.html).

via BitTorrent, a popular peer to peer service. The decision found that Comcast violated rules against net neutrality when it blocked file transfers from BitTorrent:

> We also note that because "consumers are entitled to access the *lawful* Internet content of their choice," providers, consistent with federal policy, may block transmissions of illegal content (*e.g.* child pornography) or transmissions that violate copyright law. To the extent, however, that providers choose to utilize practices that are not application or content neutral, the risk to the open nature of the Internet is particularly acute and the danger of network management practices being used to further anticompetitive ends is strong.[75]

Further explanation was provided by Chairman Kevin Martin, who explained that in determining whether a carrier violated principles of net neutrality,

> [The FCC considers] whether the network management practice is intended to distinguish between legal and illegal activity. The Commission's network principles only recognize and protect user's access to legal content. The sharing of illegal content, such as child pornography or content that does not have the appropriate copyright, is not protected by our principles.[76]

While the FCC's intent to preserve the openness of the Internet is admirable, the presumption that a carrier can easily distinguish between legal and illegal uses of copyrighted content is largely overstated. This distinction is fraught with difficulty, particularly in an age that relies so heavily on appropriating and remixing works.

Finally, an overinclusive approach to piracy surveillance risks not only chilling some forms of valuable speech, but it also risks having a deleterious effect on the technologies that distribute content as well, making it even more costly for new technologies to develop unless they devote substantial resources to the perfection of such strategies. One is reminded by Professor Lawrence Lessig's observations regarding the "zero tolerance" of infringement standard, set forth by the district court in the *Napster* case so long ago:

> If 99.4 percent [compliance with copyright protection] is not good enough, then this is a war on file-sharing technologies, not a war on copyright infringement. There is no way to assure that a p2p system is used 100 percent of the time in compliance with the law, any more than there is a way to assure that 100 percent of the VCRs or 100 percent of Xerox machines . . . are used in compliance with the law. . . . The court's ruling means that we as a society must lose the benefits of p2p, even for the totally legal and beneficial uses they serve, simply to assure that there are zero copyright infringements caused by p2p.[77]

Perfect enforcement of copyright, as Lessig suggests, will hamper the development of distributive technologies by setting forth a standard that may be

---

75. *See* Posting of David Kravets to Threat Level, http://blog.wired.com/27bstroke6/2008/08/analysis-fcc-co.html (Aug. 20, 2008) (quoting Free Press and Public Knowledge, 23 F.C.C. Rec. 13028, 13058 (2008)).

76. *See id.* at 13073.

77. Hannibal Travis, *Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law*, 84 NOTRE DAME L. REV. 331, 357 (2008) (quoting LAWRENCE LESSIG, CODE 177 (2006)).

difficult to comply with over time.

III. RETHINKING THE COPYRIGHT OUTLAW

Piracy surveillance techniques thus suggest an increasing tendency towards the "perfection" of copyright enforcement strategies.[78] However, outside of the copyright realm, it is important to note that the law has never really developed with the goal of perfect and total deterrence in mind.[79] Instead, most types of enforcement involve a mode that allows for some discretion, either on the part of the law enforcer (prosecution or police) or the putative plaintiff.[80] In the context of copyright, however, we see a disparate set of strategies. One set, seemingly favored by the recording and movie industry seems to favor strategies of copyright enforcement that aim towards perfection, and thus risk being overbroad, like filtering and digital rights management. At the same time, another set of strategies involves the tendency of copyright owners to tolerate certain uses that might otherwise constitute infringement, as described eloquently by Tim Wu.[81] Yet the confluence of these trends—overbroad piracy surveillance, coupled with tolerated uses—suggests a continuing degree of uncertainty. The result is a pervasive divide between what the law requires, and what the market tolerates, leaving consumers open to an unpredictable interpretation of their activities, and an even deeper vulnerability than the DMCA intended.

In the past two years, however, despite the outcome of cases like *Grokster*, which have expanded the legal boundaries of secondary liability, the role of private industry has attempted to answer questions left unanswered by the DMCA by favoring an emerging trend towards industry self-regulation. As a result, just as the law has expanded the general boundaries of secondary liability, more and more copyright owners are also pulling back on aggressive strategies of copyright enforcement, and instead are refining partnerships with ISPs instead.

Consider the RIAA's strategy as one example of this trend. For the last several years, the music industry has crafted a response that offered a unique coupling of direct enforcement through litigation against end users with public education. The industry filed suits against peer-to-peer operators (along with tens of thousands of their subscribers), and undertook a massive educational campaign to largely convince the public that a significant number of the activities they previously enjoyed were actually illegal. This campaign prompted a number of trade and public interest groups to criticize their efforts as overly simplistic given copyright's substantial complexity.[82]

Consider, for example, the recording industry's "back to school" anti-piracy

78. *See* Mulligan, *supra* note 60, at 7.

79. *See id.*

80. *See id.*

81. There is some evidence that content providers choose to avoid blocking uploads of "tiny amounts" of content or "mashups." *See, Media Companies Can Make Content Free—With Respectful Talks*, WASH. INTERNET DAILY, Oct. 9, 2008 (*available at* 2008 WLNR 19571201).

82. *See* Greg Sandoval, *RIAA Copyright Education Contradictory, Critics Say*, CNET NEWS, Aug. 30, 2006, http://news.cnet.com/2100-1027_3-6111118.html (last visited Mar. 28, 2009).

educational campaign in 2006, which was sent free of charge to hundreds of schools. The seven-minute video offered an incredibly simplistic rendition of copyright's complexities—the video narrator made observations such as "Making copies for your friends, or giving it to them to copy, or e-mailing it to anyone is just as illegal as free downloading." [83] The campaign was resoundingly criticized by a number of trade and public interest associations as "inaccurate, self-contradictory, and a disservice and embarrassment to the respectable institutions that RIAA has enlisted."[84] Consider one advocate from the Electronic Frontier Foundation's response:

> They claim that making any copies of any music for friends is "just as illegal as downloading." Presumably, this includes making a mixed CD for a girlfriend or buddy — something most people consider to be fair use. It's exactly these kinds of extreme positions that make the RIAA look ridiculous and out of touch with today's music fans.[85]

While the campaign did note an allowance for scholarly uses, it makes almost no mention of the law's allowance for home recordings, something that *Sony* plainly permits.[86]

Eventually, the RIAA's aggressive position against end users—lawsuits, monitoring, threats, and expensive settlements—prompted a variety of educational institutions to double back on their attempts to cooperate with the RIAA, arguing that valuable staff time had become overloaded with "copyright takedown notices, 'pre-litigation settlement letters,' RIAA-issued subpoenas, lobbying efforts, and panicked students accused of piracy."[87] After a variety of schools noticed a serious rise in the number of DMCA notices in 2007, they became even more concerned with overloading precious staff hours to address the industry's concerns. And then, finally, a few schools began to explore the option of resisting the RIAA altogether—either by erasing network logs, challenging subpoenas or by plainly refusing to forward settlement letters.[88] Even more significant was a growing concern among academic institutions that the recording industry was attempting to pressure Congress to obtain legislative rules that compromised the values of academic openness and privacy that the institutions had attempted to protect.[89]

In the last few months of 2008, facing these challenges, the RIAA ultimately took the unusual step of ending its relentless campaign of lawsuits against infringers (35,000 in all) and announcing a decision to emphasize working with

---

83. Christopher Dawson, *RIAA Video for Students if Full of Lies*, ZDNet.com, http://education.zdnet.com/?p=458.

84. Mark Hefflinger, *CEA, Public Knowledge Deride RIAA Copyright Education Campaign*, DIGITAL MEDIA WIRE, Aug. 31, 2006, http://www.dmwmedia.com/news/2006/09/01/cea-public-knowledge-deride-riaa-copyright-education-campaign.

85. Dawson, *supra* note 83.

86. *See id.*

87. Catherine Rampell, *Antipiracy Campaign Exasperates Colleges*, THE CHRON. OF HIGHER EDUCATION, Aug. 15, 2008, http://chronicle.com/free/v54/i49/49a00104.htm.

88. *See id.*

89. *See id.*

ISPs directly to identify and contact infringers instead.[90] Executives from the industry explained that the decision was precipitated by a recognition that the amount of piracy had not decreased enough to justify the costs of the suits, and (in the words of one executive): "[e]verybody realized this was making us the most hated industry since the tobacco industry."[91] Consequently, the industry opted to end its lawsuit campaign and instead simply notify the ISP directly if the RIAA detects infringement. The ISP, in turn, has the responsibility to notify the user, and if the infringement continues, terminate the user's access.[92]

The key difference between the previous strategy and the new one involves a simple, but important difference: protection of the user's identity. Previously, the RIAA's strategy was to file lawsuits in order to compel the ISP to reveal the identity of the alleged infringer. Under the new regime, however, the identity of the actual infringer is held by the ISP alone, and not disclosed to the RIAA. While the RIAA reserves the right to sue in a few egregious cases, the responsibility for managing and terminating the user's access rests solely with the ISP instead.[93]

This shift marks an important step in the protection of user privacy, but it also signals a dramatic delegation to the ISP to enforce the boundaries of copyright protection. In the past, piracy surveillance techniques included a variety of mechanisms including monitoring, management and direct interference with copyright infringement online.[94] All of these strategies relied on the copyright owner, rather than the ISP, to detect infringement. And, as many examples above have suggested, these modes of detection have often been fraught with mistakes.[95] In one case, the industry attempted to file suit against a deceased woman who allegedly "hated computers" until she passed away at age 83.[96]

Yet the RIAA's decision to partner with ISPs tracks a growing trend towards industry self-regulation, also favored by the video content industry, which had recently announced its own partnerships with ISPs. In October of 2007, after much discussion, a variety of prominent media companies and service providers—CBS, DailyMotion, Fox Entertainment Group, Microsoft, MySpace, NBC, Veoh and Viacom announced a series of "Principles for User Generated Content Services."[97] The principles aim to both foster creativity and respect copyright law, and made a number of powerful observations, among them that "[d]istributors of copyright-infringing content stifle both technological innovation and artistic creation in ways

90. *See* Steve Knopper, *RIAA's Gaze Turns from Users to ISPs in Piracy Fight*, ROLLING STONE, Dec 19, 2008, http://www.rollingstone.com/rockdaily/index.php/2008/12/19/riaas-gaze-turns-from-users-to-isps-in-piracy-fight/.

91. *Id.*

92. Sarah McBride and Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1.

93. *Id.*

94. *See* Katyal, *supra* note, 16 at 229.

95. JR Raphael, *RIAA's New Piracy Plan Poses a New Set of Problems*, PCWORLD, Dec. 19, 2008, http://www.pcworld.com/article/155820/riaas_new_piracy_plan_poses_a_new_set_of_problems.html.

96. *Id.*

97. Principles for User Generated Content Services, www.ugcprinciples.com/press_ releases.html (*hereinafter* "UGC Principles").

that ultimately will hurt the consumer and hinder the digital economy."[98] Consequently, the Principles were developed with a variety of objectives in mind: (1) to eliminate infringing content; (2) to encourage uploads of "wholly original and authorized user-generated audio and video content;" (3) to accommodate fair use; and (4) to protect user privacy.[99] The stated ultimate goal is to utilize filtering regimes and identification technologies that eventually block infringing uploads "*before* they are made available to the public."[100]

At first glance, the partnership's ability to reconcile these divergent interests is certainly impressive. The partnership works as follows: the copyright owner provides information (reference data on the content it wants protected—video, music, etc.—and instructions on how matches should be treated) to the ISP. If a user uploads content that matches the protected content, then the ISP is authorized to use the identification technology to block the upload entirely. Or, alternatively, the copyright owner can also specify that it does not want its content to be blocked, perhaps due to a preference for licensing or for allowing the content to be uploaded.[101] If the ISP adheres to the Principles in good faith, the copyright owners agree that it will not mount a copyright claim against the provider alleging contributory liability.

For the most part, industry self-regulation appears to be significantly more dynamic than either the common law or the DMCA, both of which have developed governing principles on a much slower basis. There are a variety of benefits to industry self-regulation, in the form of lower transaction costs, a greater knowledge of technological limitations in the implementation of filters and in the ability to develop "best practices" that take into account a variety of divergent perspectives between the two sides through compromise.[102] At the same time, however, industry self-regulation, like much of the notice and takedown system itself, relies on a copyright owner's determination of what infringement comprises, and thus tends to overlook the very uncertainties that the law's flexible fair use standard attempts to protect. As Pamela Samuelson and Jason Schultz have observed, the content industry has long argued against a formation of consumers "rights" to fair use or personal copying for noncommercial purposes, tending instead to relegate these as "expectations" that can be managed by a reliance on digital rights management in any event.[103]

---

98. *See id.*

99. *See id.*; *see also*, Brette G. Meyers, Filtering *Systems or Fair Use? A Comparative Analysis of Proposed Regulations for User-Generated Content*, 26 CARDOZO ARTS & ENT. L.J. 935, 944 (2008); Note, *The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance*, 121 HARV. L. REV. 1387 (2008).

100. *See* UGC Principles, *supra* note 97 (emphasis added).

101. *See* Meyers, *supra* note 99, at 944-45.

102. *See* Pamela Samuelson and Jason Schultz, *Should Copyright Owners Have to Give Notice of Their Use of Technical Protection Measures?*, 6 J. TELECOMM & HIGH TECH L. 41, 68 (2007-2008). *See also* Jennifer E. Rothman, *Why Custom Cannot Save Copyright's Fair Use Defense*, 93 VA. L. REV. IN BRIEF 243 (Feb. 2007) (*available at* http://www.virginialawreview.org/inbrief/2008/02/ 18/rothman.pdf).

103. *Id.* at 69.

Moreover, despite the Principles' stated commitment to user privacy and fair use, the parties' agreement failed to really secure its preservation. For example, the Principles called for a manual review of content that suggested fair use implications, but only at the "option" or "in addition" to the use of identification technology:

> UGC Services may, at their option, utilize manual (human) review of all user-uploaded audio and video content in lieu of, or in addition to, use of Identification Technology, if feasible and if such review is as effective as Identification Technology in achieving the goal of eliminating infringing content. If a UGC Service utilizes such manual review, it should do so without regard to whether it has any licensing or other business relationship with the Copyright Owners. Copyright Owners and UGC Services should cooperate to ensure that such manual review is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use.[104]

In response, EFF issued its own series of principles, largely focused on the preservation of fair use, noting that "a commitment to accommodating 'fair use' alone is not enough."[105] It argued, instead, for a more general standard that set forth clearer guidelines, explaining that both creators and copyright owners would benefit from a clearer and objectively ascertainable standard.[106] As a result, the EFF standard calls for filtering technologies that incorporate fair use protections within them. It called for a "three strikes before blocking" rule that required a match between (1) audio, and (2) video and also required (3) that nearly 90% of the challenged content was composed of a single copyrighted work. The EFF standards also called for the creator to be able to challenge an automated match, enabling the "user" to dispute the findings of the filtering process.[107] It also asked for ISPs to provide more information to the user, including the entire takedown notice and the rights of the user under the DMCA. Finally, it asked for the creation of a hotline to request reconsideration of a takedown.

Importantly, both Google and YouTube were absent from the UGC principle discussions, and YouTube announced its own VideoID technology just a few days before the UGC principles went public.[108] This effort was probably an indirect response to the lawsuit it faced from Viacom, where the court must determine whether YouTube had the right and ability to control infringement, or whether it derived a financial benefit from the infringing activity.[109] In another lawsuit

104. *See* UGC Principles, *supra* note 97, at para. 3(f).

105. *See* EFF.org, Fair Use Principles for User Generated Video Content, http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen.

106. *Id.*

107. Most notably, the EFF called for a precise, granular interpretation of the DMCA putback procedures—(1) the right to sue if the removal is the result of a knowing material misrepresentation, and (2) the counter-notice and putback provision that overrides a takedown unless the copyright owner files an action in court. *See* Fair Use Principles for User Generated Video Content, *supra* note 105.

108. *See* Meyers, *supra* note 99, at 946.

109. For more information, including the filings in the case, see http://news.justia.com/cases/featured/new-york/nysdce/1:2007cv02103/302164/ (last visited June 25, 2009).

involving user generated video sharing, however, the *Veoh* case, a court found that a service provider's inability to control posted content, along with other facts suggesting a lack of control, served to qualify Veoh for safe harbor protection under the DMCA, absolving the potential for contributory liability.[110] The outcome of such a case plainly suggests that YouTube's scope of liability may very well rest on whether or not a court reaches similar factual determinations. After the *Veoh* decision was announced, for example, YouTube counsel Zahavah Levine stated, "It is great to see the Court confirm that the DMCA protects services like YouTube that follow the law and respect copyrights . . . YouTube has gone above and beyond the law to protect content owners while empowering people to communicate and share their experiences online."[111] In response, Viacom retorted, in its own statement:

> Even if the *Veoh* decision were to be considered by other courts, that case does nothing to change the fact that YouTube is a business built on infringement that has failed to take reasonable measures to respect the rights of creators and content owners. Google and YouTube have engaged in massive copyright infringement—conduct that is not protected by any law, including the DMCA.[112]

Nevertheless, YouTube's approach, while buoyed perhaps by the outcome of cases like *Veoh*, appears to be ready and willing to take a greater role in policing posted content. In response to its own lawsuit, YouTube assured the public that it "hopes to be able to block pirated uploads before they post at all."[113] Towards that end, it utilizes a system called VideoID, which enables a copyright owner to either block the clip, leave it up or enable YouTube to "monetize" the clip by selling ad revenue, which it then splits with the copyright owner.[114] When VideoID locates a match, it draws upon one of three usage policies: Block, Track or Monetize. If a rights owner specifies a Block policy, the video will not be viewable on YouTube. If the rights owner specifies a Track policy, the video will continue to be made available on YouTube and the rights owner will receive information about the video, such as how many views it receives. For a Monetize policy, the video will continue to be available on YouTube and ads will appear in conjunction with the video. The policies can be region-specific, so a content owner can allow a particular piece of material in one country and block the material in another.[115]

---

110. For more information on the Veoh case and its filings, *see* Rafat Ali, *Veoh Wins Copyright Infringement Lawsuit; Viacom-YouTube Next?*, at http://www.washingtonpost.com/wp-dyn/content/article/2008/08/28/AR2008082800217.html (last visited June 25, 2009).

111. *See id.*, quoting Levine.

112. *See id.*

113. Rob Hof, *YouTube Intros VideoID System; Will Studios Go Along?*, BUS. WK. ONLINE, Oct. 15, 2007 (*available at* http://www.businessweek.com/the_thread/techbeat/archives/2007/10/youtube_intros.html).

114. *See* Greg Sandoval, *YouTube's Filters Help Copyright Owners Profit From Pirated Videos*, CNET.com, http://news.cnet.com/8301-1023_3-10027509-93.html.

115. *See YouTube Copyright Policy: Video Identification Tool*, http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=83766. For commentary on this policy, *see* Tony Bates, *The Perils of YouTube Filtering: Parts I and II*, The MTTLR Blog, http://blog.mttlr.org/2007/12/perils-of-youtube-filtering.html.

Google has stated that most copyright owners choose to leave the clips up 90 percent of the time.[116] Some predict that technology will develop that will search for unauthorized videos and automatically insert advertisements into the clips.[117] In a study completed for ZDNet of Google's filters for YouTube, the authors concluded that filters catch illegally uploaded content (using a "Saturday Night Live" clip from NBC), roughly 75 to 80 percent of the time.[118]

These strategies have been heralded as win-win outcomes for both the consumer and the copyright owner. As one advocate observes, "[p]irates look less like scoundrels and more like ambassadors as they share their favorite content and evangelize on behalf of the owner."[119] Yet no guideline principles regarding transparency—how the content is selected, for example—are established so that users can modify their activities; "We don't want people to steer around (the technology)," Zahavah Levine, YouTube's chief counsel, explained.[120] In fact, one recent study suggested that YouTube's audio fingerprinting process, while seeming incredibly broad and comprehensive, was also prone to some mistakes.[121] Moreover, although the monetization process theoretically sounds very strong in terms of offering a clear compromise between copyright owner and consumer, the statistics on whether this outcome is more preferable than the others have yet to be empirically verified.[122] And Viacom, while reluctantly congratulating YouTube on "stepping up its responsibility and ending the practice of profiting from copyright infringement," has not yet altered its lawsuit to addressing acts of past infringement.[123]

The confluence of piracy surveillance strategies, with the increased prominence of industry self-regulation brings us to a curious moment in copyright history. We are still unsure of where the responsibility should lie for detecting infringement online—should it lie with the copyright owner, an Internet Service Provider, or some other administrative outlet instead? And how does one ensure due process and transparency in efforts to self-regulate? In the end, the presence of a filtering option, coupled with the increasingly laudatory responses that surround monetization, suggests that market resolution of these principles may overshadow any claims to copyright law's granular ability to govern what is legal and what is not. Further, even aside from the risk of chilling both expression and innovation,

116. *See* Sandoval, *supra* note 114; *see also Making Money on YouTube with Content ID*, OFFICIAL GOOGLE BLOG http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html.

117. *See* Sandoval, *supra* note 114.

118. *See* Tom Steinert-Threlkeld, *YouTube's Video System: Is 75 Percent Accuracy Good Enough?*, ZDNET UNDERCOVER, at 3 (Nov. 2008).

119. David Sarno, *Waltzing Around the Piracy Issue*, L.A. TIMES, Aug. 20, 2008, at E1.

120. Scott Kirsner, *YouTube's New Tools Axe Illicit Video*, VARIETY, Oct. 15, 2007, *available at* http://www.variety.com/article/VR1117974071.html?categoryid=1009&cs=1.

121. *See* Electronic Frontier Foundation, Testing YouTube's Audio Content ID System, at http://www.eff.org/deeplinks/2009/04/testing-youtubes-aud.

122. *See* Sarno, *supra* note 119. Yet Time Warner and the News Corporation, NBC Universal and Walt Disney have not yet signed on to the cause. *See also* Brian Selter, *Now Playing on YouTube: Clips with Ads on the Side*, N.Y. TIMES, Aug. 16, 2008, at C1.

123. *See* Selter, *supra* note 122.

the more unsettled issue continues to be the degree of delegation that the DMCA should extend to a copyright holder in determining the boundaries of legality. Consider Google's own observation:

> Now, when it comes to spotting pornography and graphic violence, and other content prohibited by our terms of use, nothing beats our community flagging. Once a user flags a video, we immediately review it and remove it if we find a violation. But our community can't identify infringing content. We all know pornography and violence when we see them. But copyright status can only be determined by the copyright holder. That is because almost anyone who creates an original video has the copyright for that work, and such a wide range of copyright holders' preferences vary widely.[124]

Google's observation suggests the need for an almost wholesale delegation to the copyright holder in determining the boundaries of legality. Given the strong incentives that operate in favor of using ISPs as proxy censors, the law should be careful about encouraging further delegation as it takes up these issues in the future.

CONCLUSION

We are at a moment of important ambiguity in the balance between copyright enforcement and civil liberties. For the past several years, we have seen a barrage of headlines predicting regarding the fall of the music industry due to digital piracy. Today, as we watch the industry shift to accommodate new models for content distribution, we also see the growth of less prominent and invasive forms of surveillance, filtering and monitoring to guard against potential piracy.

While other scholars in this Symposium have performed masterful analyses of the various statutory tensions that arise from these regulations in terms of the question of vicarious and contributory liability, I have suggested, more broadly, that the DMCA's provisions, in light of common law developments, have affected the granularity and significance of classic civil liberties—privacy, freedom of speech and fair use—in relation to the protection of digital intellectual property. In the past, the preexisting balance between intellectual property and civil liberties co-existed, mostly due to the panoply of different laws and principles—constitutional,

---

124. *See* Steve Chen, Youtube Co-Founder, *The State of Our Video ID Tools*, OFFICIAL GOOGLE BLOG http://googleblog.blogspot.com/2007/06/state-of-our-video-id-tools.html. The blog continues:

> Some copyright holders want control over every use of their creation. Many professional artists and media companies post their latest videos without telling us, while some home video-makers don't want their stuff online. Some legal departments take down a video one day and the marketing department puts it up the next. Which is their right, but our community can't predict those things, and neither can we. The same is true for technology. No matter how good our video identification technology gets, it will never be able to read copyright-holders' minds.
>
> If a content owner identifies material that she doesn't want on YouTube, she can request its removal with the click of a mouse. If particular users repeatedly infringe copyrights, we terminate their accounts. We have long made a practice of creating a unique "hash" of every video removed for alleged copyright infringement and blocking re-uploads of the hash. We educate users on what is and isn't permissible under the law. Our upcoming video identification system will be our latest way of empowering copyright holders, going above and beyond legal requirements.

statutory, common law—governing each interest. Yet an emerging conflict in these areas regarding the role of intermediaries poses a number of interesting philosophical and practical problems, particularly where the role of intellectual property is concerned. Consequently, shifts in the market, as well as shifts in technology, suggest the need for a more precise balance maintained by constant supervision.