

## Rewinding *Sony*: The Evolving Product, Phoning Home and the Duty of Ongoing Design

Randal C. Picker\*

It has been clear for sometime that the Supreme Court would revisit its 1984 decision in *Sony* creating the famous (infamous?) “substantial noninfringing use” test for secondary liability for copyright infringement. The only question was how the challenge would emerge. Would it be a re-make of *Sony* with the digital video recorder playing the role of the VCR? Or would some other device force its way on the stage? Of course, we now know that peer-to-peer software has done just that and that the lower court decisions in *Napster*, *Aimster* and finally *Grokster* have put these key issues before the Court again.<sup>1</sup>

Much has changed during the intervening two decades. In 1984, the video content industry feared that the VCR would destroy the way in which broadcast television was financed by making it possible for home viewers to skip over commercials. The industry saw only dimly, if that, a possible future in which revenues for home viewing of movies through tape rentals and

---

\* Copyright © 2005, Randal C. Picker. All Rights Reserved. Paul and Theo Leffmann Professor of Commercial Law, The University of Chicago Law School and Senior Fellow, The Computation Institute of the University of Chicago and Argonne National Laboratory. Prior versions of this paper have been given at workshops at the law schools at Case Western Reserve University and the University of Toronto. I thank Tim Wu and the participants in the Bigelow Square Table Lunch for comments and also thank the Paul Leffmann Fund, The Russell J. Parsons Faculty Research Fund and the John M. Olin Program in Law and Economics at The University of Chicago Law School for their generous research support, and through the Olin Program, Microsoft Corporation and Verizon.

<sup>1</sup> *A&M Records, Inc v Napster, Inc*, 239 F3d 1004 (9<sup>th</sup> Cir 2001); *A&M Records, Inc v Napster, Inc*, 284 F3d 1091 (9<sup>th</sup> Cir 2002); *In re Aimster Copyright Litigation*, 334 F.3d 643 (7<sup>th</sup> Cir 2003); *Metro-Goldwyn-Mayer Studios, Inc v Grokster Ltd*, 380 F3d 1154 (9<sup>th</sup> Cir 2004), cert granted 125 S Ct 686 (2004).

---

purchases and now, of course, from DVD rentals and sales would far exceed ticket revenues from movie theaters.<sup>2</sup>

Now, in 2005, the video content industry fears that the DVR will destroy the way in which broadcast television is financed by ... well, perhaps things haven't changed so much after all. And of course the fact that the video content industry was wrong the first time doesn't mean that they are wrong this time.<sup>3</sup> But there is a more basic change that has taken place since Sony released the Betamax, and that change matters enormously for how we should think about the regulation of new products.

Product design was lumpy and episodic when Sony created the Betamax and the products were lumpy too. I mean by that that (i) a product would come with a well-defined set of features; (ii) once a particular VCR was sold, the features of that VCR would remain unchanged forever; and (iii) this created an installed base of products that had to be taken into account in considering changes to future versions of the VCR, which of course constrained how the product the VCR could evolve.

We are at a very different point now. Most interesting products that you don't eat come with software and indeed, the feature set of the product is defined in many ways by that software. The zero marginal cost feature of software means that there are no natural boundaries to define the features of the product.<sup>4</sup> But software alone isn't sufficient to break the lumpy

---

<sup>2</sup> For discussion, see Randal C. Picker, *From Edison to the Broadcast Flag: Mechanisms of Consent and Refusal and the Propertization of Copyright*, 70 U Chi L Rev 281, 288-91 (2003).

<sup>3</sup> For my views on the implications of the DVR, see Randal C. Picker, *The Digital Video Recorder: Unbundling Advertising and Content*, 71 U Chi L Rev 205 (2004).

<sup>4</sup> Elsewhere I have called these "scope-of-permission" goods and have considered how antitrust law should deal with the fundamental arbitrariness of product definition for this class of products. See Randal C. Picker, *Unbundling Scope-of-Permission*

---

design framework. We need to combine software with communication—networked products—and now we have products that can evolve in real-time (and do).<sup>5</sup> Design ceases to be a one-time event and instead becomes a continuous process. And that is true not only for the next product sold, but also for the entire installed base. The dead hand of the past and the constraints of backwards compatibility are lifted.

How does this matter as the Supreme Court reconsiders *Sony*? Those who fear any step back from the substantial non-infringing use test believe that it is essential for protecting innovation incentives.<sup>6</sup> The core fight over *Sony* turns on the uncertainty of what happens next: what is the next use of the product not seen today? But *Sony* is framed in the context of episodic design with an installed-base constraint and no real possibility of feedback between actual use of the product and design.

We are at a very different point now. Networked products evolve and we are now going to frame what ongoing design

---

*Goods: When Should We Invest in Reducing Entry Barriers?*, 72 U Chi L Rev 189 (2005).

<sup>5</sup> And, to continue the litany of self-cites, I have examined the consequences of networking for product design before in considering whether Microsoft should have been found to violate the Sherman Act for bundling Internet Explorer with Windows. See Randal C. Picker, *Pursuing a Remedy in Microsoft: The Declining Need for Centralized Coordination in a Networked World*, 158 J Inst & Theoretical Econ 113 (2002). I also consider the dark side of networked products—what the zombification of PCs means for cybersecurity—in Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky* (forthcoming, *The Law and Economics of Cybersecurity*, Mark Grady & Francesoco Parisi, eds, 2005). In that paper, I also address what the possibility of continuous design means for timing decisions about when to release software (earlier rather than later).

<sup>6</sup> See, for example, Brief Amici Curiae of Computer Science Professors Harold Abelson et al, *Metro-Goldwyn-Mayer Studios, Inc v Grokster Ltd*, No 04-480 (S Ct filed Feb 28, 2005) (available at [http://www.eff.org/IP/P2P/MGM v Grokster/20050301\\_cs\\_profs.pdf](http://www.eff.org/IP/P2P/MGM_v_Grokster/20050301_cs_profs.pdf)).

---

obligations should exist with regard to these networked products. Smart products “phone home” and update themselves. Phoning home—and the control that results from that—is a choice. Sony had no good way to control the Betamax after it was unleashed on the world. Sony couldn’t pull the plug on the Betamax, either physically or virtually. Sony couldn’t issue a 100%-effective electronic recall of the Betamax. But if the designers of Grokster lack ongoing control over their product, it is because they consciously chose to relinquish control. They could have evolved the product and done so not in thinking about potential uses of the product, but in light of actual use, in light of actual realization of the unanticipated next use. Sony couldn’t do that with the Betamax.

This means that it is a mistake to focus on all-or-nothing, thumbs up/thumbs down tests for evaluating networked products like the DVR or peer-to-peer networking. We need to focus on the process of product evolution, the choices that designers make regarding their ability to evolve the product in light of evolving use and who should have a stake in controlling that evolution.

This paper has four sections. Section I lays out some of the criticism of *Sony* and offers a quick overview of the recent case-law on peer-to-peer software. Section II offers examples of evolving networked products and the choices that are being made today about whether effective control is maintained over the product even after its initial distribution (phoning home). Some of our hottest products today—including TiVo and the Apple iPod—fall into this category. Section III considers how technology has altered the set of effective legal rights in sound recordings, the costs and benefits of that, and the innovation safe harbor created by *Sony’s* substantial noninfringing use test. Finally, Section IV sets forth an alternative test. The test is keyed to whether ongoing control is or is not retained over the

---

networked product. Relinquishing control should result in a test tougher than that set forth in *Sony*; retaining control should kick in the substantial noninfringing use test, but that would be coupled with a duty of ongoing design to reduce non-infringing use. I then consider three situations in which we have attempted to design systems to minimize copyright infringement (the Napster injunction process; the notice-and-takedown regime applicable to Internet service providers under Section 512 of the Copyright Act; and the FCC's broadcast flag process for digital television).

### I. The State of *Sony*

---

While technology has been racing forward for twenty years, the law remains mired in the goop. *Sony* was a tightly-contested 5-4 decision, where the internal workings of the Supreme Court were sufficiently fluid, as Paul Goldstein tells it,<sup>7</sup> that the Court held the case over to be re-argued and still flip-flopped between different majority opinions. The internal history of the *Sony* opinion makes concrete the fundamental ambivalence that the Court faced—and that we still face—about the right way to frame the test in this situation.

At the initial conference among the justices discussing the case, Justice Blackmun was assigned the task of writing a majority opinion in favor of the copyright holders. During the back-and-forth of opinion writing, Justice Brennan shifted his views. He had concluded that it was a mistake to consider the VCR under a “primary use” test and instead thought that the VCR should be evaluated on whether it had a “substantial non-

---

<sup>7</sup> Paul Goldstein, *Copyright's Highway: From Gutenberg to the Celestial Jukebox* 119-28 (rev ed Stanford U Press 2003).

---

infringing use.”<sup>8</sup> That was the language the Court used in framing what has become to be known as the *Sony* test:

The staple article of commerce doctrine must strike a balance between the copyright holder’s legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need nearly be capable of substantial noninfringing uses.<sup>9</sup>

Twenty years later, where do we stand? The defenders of *Sony* characterize its test as the Magna Carta of product innovation and hope that the test will survive the *Grokster* appeal intact. And what do the the motion picture studios and recording companies, petitioners in the Supreme Court, seek? In their merits brief in the Supreme Court, they argue that *Sony* should be read to say that the staple article of commerce doctrine doesn’t apply “when the primary or principal use of a product or service is infringing.”<sup>10</sup> Twenty years have passed, and we are exactly where the Supreme Court was in the beginning, choosing between “primary use” and the “substantial non-infringing use” safe harbor.

#### *A. The Chilly Sixth Floor*

The *Sony* test has been criticized on a number of grounds, and the test may have received its chilliest reception on the sixth floor of the University of Chicago Law School. So I argued in

---

<sup>8</sup> Id at 124.

<sup>9</sup> *Sony Corp v Universal City Studios, Inc*, 464 US 417, 442 (1984).

<sup>10</sup> Brief for Motion Picture Studio and Recording Company Petitioners, *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd*, No 04-480, 31 (S Ct filed Jan 24, 2005) (available at [http://www.eff.org/IP/P2P/MGM v Grokster/04-480 Petitioners brief.pdf](http://www.eff.org/IP/P2P/MGM_v_Grokster/04-480_Petitioners_brief.pdf)).

2002 that the substantial non-infringing use test did a poor job of aligning costs and benefits associated with a new product. The substantial noninfringing use test does create a safe harbor so that a product designer can be sure that she doesn't face liability, but it does so at the cost of allowing products that are, on net, wildly socially harmful to proliferate. Moreover, I emphasized that the *Sony* test failed to create *any* design incentives, even in circumstances where a redesign would be incredibly cost-efficient.<sup>11</sup> Two of my sixth-floor colleagues, Doug Lichtman and Bill Landes, jumped on *Sony* in 2003 and found "much to criticize in the Court's analysis." They emphasized how even small design changes in the VCR—the precision of the fast-forward button, for example—might have protected copyright holders without preventing legitimate uses.<sup>12</sup>

Finally, and most importantly, in June, 2003, my part-time sixth-floor colleague Judge Posner issued his opinion in *Aimster*. That opinion addressed both the net costs and benefits issue and the design-incentives issue. On the former, the Seventh Circuit tried to tease out of *Sony* the possibility that some sort of balancing of infringing and noninfringing uses was possible.<sup>13</sup> On the latter, the Seventh Circuit addressed directly

---

<sup>11</sup> See Randal C. Picker, *Copyright as entry policy: the case of digital distribution*, 47 Antitrust Bull 423, 444-45 (2002) ("The design issue makes the point even more powerful. You could spend \$5 to design the product to eliminate the social harm while still creating a \$100 in social benefits. Should you spend the money to redesign? Again, the answer should be straightforward and with a sensible liability rule, would be. In contrast, *Sony* removes any reason to redesign to minimize copyright infringement.")

<sup>12</sup> Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Analysis*, 16 Harv J Law & Tech 395, 400 (2002-03).

<sup>13</sup> *Aimster*, 334 F.3d at 649 ("What is true is that when a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respected magnitudes of these uses is necessary for a finding of contributory infringement.")

---

whether Aimster had an obligation to design its product to minimize infringing uses:

Even when there are noninfringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.<sup>14</sup>

This sensible design test has been criticized for being outside the scope of *Sony*,<sup>15</sup> but that isn't obviously right. While Justice Blackmun did consider the possibility of alternative designs for the VCR,<sup>16</sup> the majority opinion ignored the design issues. We shouldn't make too much of that silence.

*B. Meanwhile, in California ...*

The Seventh Circuit's decision in *Aimster* followed up on the Ninth Circuit's decision in *Napster*. Napster ran a "centralized" peer-to-peer service for distributing music. That meant that Napster provided a centralized index indicating what music was available for download, but Napster itself hosted no music and all downloading took place between peers. The *Napster* opinion addressed whether the downloading itself could be framed as legitimate fair use, a critical issue given that the recording industry was seeking to hold Napster liable as a secondary infringer, that is, an infringer who makes possible some other person's primary infringement. But the Ninth Circuit saw no

---

<sup>14</sup> Id at 653.

<sup>15</sup> See Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 Stan L Rev 1345, 1362 (2004).

<sup>16</sup> *Sony*, 464 US at 494 ("Sony may be able, for example, to build a VTR that enables broadcasters to scramble the signal of individual programs and 'jam' the unauthorized recording of them").

---



basis for overturning the lower court's opinion on fair use<sup>17</sup> and that allowed the Ninth Circuit to turn to the questions of secondary liability and *Sony*.

The Ninth Circuit found that Napster could be held liable, and that was interesting. The simple opinion would have held the other way and would have tracked *Sony* woodenly. Was Napster capable of substantial noninfringing uses? Sure. Napster could be used for peer-to-peer distribution of any content and there is lots of public domain content (U.S. governmental works being a key category). Even within the domain of music, some bands were happy to have their music distributed virally through peer-to-peer networks. This could be a great way for a band to capture an audience outside of the standard hierarchical system for distributing music that dominates the record industry.

The Ninth Circuit's analysis saw Napster as having knowledge of infringement through the control that Napster could exert over its system:

The record supports the district court's finding that Napster has *actual* knowledge that *specific* infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material.<sup>18</sup>

The Ninth Circuit side-stepped *Sony* by ignoring the current design of Napster and instead focusing on what Napster could be, its could-have-been design. In the context of the case, we might think of that as the distinction between a product, such as the VCR, and a service, what Napster effectively was, though, as I have indicated already, I think the more important point conceptually is that Napster was a networked product.

---

<sup>17</sup> *Napster*, 239 F3d at 1019.

<sup>18</sup> *Id* at 1022.

---

The Ninth Circuit emphasized Napster's ongoing obligations to police its network in its consideration of whether Napster could be held liable under the secondary liability doctrine of vicarious liability:

Here, plaintiffs have demonstrated that Napster retains the right to control access to its system. Napster has an express reservation of rights policy ... . To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability. ... The district court correctly determined that Napster had the right and ability to police its system and failed to exercise that right to prevent the exchange of copyrighted material.<sup>19</sup>

In mid-2004, the Ninth Circuit revisited the status of peer-to-peer distribution networks in its decision in *Grokster*. The court recognized that “the software design [was] of great import,”<sup>20</sup> in particular, a key switch from Napster in the way that indexes were maintained and the corresponding control that resulted for the network creator. Napster was distinguished as a p2p network with central indexing, *Grokster* and its cousins as decentralized “supernode” networks.<sup>21</sup> *Grokster* was seen as lacking the direct involvement that an ISP might have or the ongoing role that Napster had:

“Failure” to alter software located on another’s computer is simply not akin to the failure to delete a filename from one’s own computer, to the failure to cancel the registration name and password of a particular user from one’s user list, or to the failure to make modifications to software on one’s own computer.<sup>22</sup>

---

<sup>19</sup> Id at 1023.

<sup>20</sup> *Grokster*, 380 F3d at 1163.

<sup>21</sup> Id at 1158-59.

<sup>22</sup> Id at 1163-64.

---

In similar fashion, the Ninth Circuit rejected the claim that Grokster should be found to be liable under the doctrine of vicarious liability: “We agree with the district court that possibilities for upgrading software located on another person’s computer are irrelevant to determining whether vicarious liability exists.”<sup>23</sup>

## II. The Evolving Product: Phoning Home and The Duty of Ongoing Design

---

I think that the Ninth Circuit’s core conception in *Grokster* is wrong. It depends on nonexistent vision of the difference between sins of omission and commission. It also ignores the new realities of networked products and what those should mean for ongoing design obligations.

Networked products can evolve. These are products with the possibility of communication and strong software components. Most importantly for the current discussion, this category includes the digital video recorder—TiVo being the most prominent brand—and peer-to-peer software resident on a personal computer. Consider three quick examples of evolving networked products:

- *Google Desktop Search*. The current fight for the computer desktop is over search capability. The problem is that it is easier to find a file on the Internet than it is on your own computer. The solution? A number of leading and not-so-leading companies have new programs; Google’s is Google Desktop Search (GDS) and you get it by downloading it from Google’s website. In December, 2004, computer science researchers at Rice Univer-

---

<sup>23</sup> Id at 1166.

---

sity discovered a security flaw in GDS that would have made it possible for third parties to invade the privacy of GDS users. Did GDS users need to go to Google's website to download a patch for their software? No. GDS automatically updates itself—it evolves on its own without any action by the consumer. The capabilities of the software sitting on your computer change without even having to click the mouse.<sup>24</sup>

- *Windows*. Microsoft Windows updates as well (visit [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com) for info). Windows is a complex product and is prominent target for hackers, so security updates are important. The visibility of the update process depends on your settings, but on my computer, the updates are quietly downloaded in the background, without any initiation by me. A window pops open to let me know that updates are ready for installation; I click and install.
- *TiVo*. The digital video recorder is a classic networked product. The DVR is just a souped up VCR, but the soup matters. The DVR uses a hard disk to store copied programs and so users need not put in a blank tape when they want to record a favored program. That would be a step forward over the VCR, but combine that with software to make recording easier, and now we have a worthy machine. The recording software simplifies programming and can even automate that process to record all of the episodes of your favorite show. To make that work, your TiVo phones home periodically to download the new TV schedule. To be mechanical, this means that the TiVo in your family

---

<sup>24</sup> See Scarlet Pruitt, *Security Hole Found in Google Desktop Search*, IDG News Service (Dec 20, 2004).

---

room is hooked up to the phone line and dials to a TiVo server somewhere for the new information. But, and now we head to controversy, TiVo also downloads the software that controls its operation. TiVo central has recently propagated a software change through the network of TiVos to embed in your TiVo a copy protection scheme from Macrovision.<sup>25</sup> From the consumer's standpoint, this means that the TiVo box in your living room is losing functionality, as you will lose the ability to record certain programs in your preferred way. You bought one box; it had certain capabilities but those features evolve as part of the TiVo service.

These are just three easy examples, but we could multiply this list many times over. So Apple controversially "updated" its iPod software so that iPod owners could not play songs from RealNetworks's online music store (Apple thinks that you are supposed to buy your songs at its iTunes website). That raises some delicious antitrust questions—should we think of this as a technological refusal to deal?—but more to the current point is just that Apple could do that if it wanted to do so.<sup>26</sup> To take another example, anti-virus software is more service than software: anti-virus software that didn't evolve would be worthless, so the software routinely updates to deal with new threats. But the software doesn't update forever: the software is an annual subscription and while you can keep the old software and its protection against old viruses without having to buy a new subscription, you instantly lose protection against new viruses.

---

<sup>25</sup> See Lucas Graves, *Has TiVo Forsaken Us?*, Wired Magazine (Nov 2004).

<sup>26</sup> See John Borland, *Apple fights RealNetworks' "backer tactics,"* Cnet News.com (Dec 14, 2004) (available at [http://news.com.com/2102-1027\\_3-5490604.html](http://news.com.com/2102-1027_3-5490604.html)); for lively commentary, see the byplay between James Boyle and Thomas Hazlett, *The Apple of forbidden knowledge*, FT.com (Aug 12, 2004); see also <http://www.musicfreedomofchoice.org/>.

---

In all of these cases, we have a product with a strong software component and ongoing communication with the mother-ship. This is a design choice and one made possible by the spread of cheap communications, machine intelligence and storage. Networked product evolution is going to put pressure on law. Do TiVo users have a disabled product cause of action against TiVo when the next software upgrade reduces the functionality of TiVo? That will obviously depend on the license agreements in place between TiVo and its customers and the nature of notice that is required to customers.<sup>27</sup>

Consider the phoning home capability. As this list should make clear, the producer of a networked product chooses whether or not to have ongoing contact with the product. Put differently, the producer chooses whether or not to create the possibility of future control of the product. For some products, this control is wholly natural. A disconnected TiVo or anti-virus software is worth very little. Both products have a natural obsolescence—new viruses and new programs arise and the products need to be updated to continue to be effective—that necessitates ongoing contact and that contact creates an easy opportunity for forcing other changes, such as TiVo's recent change regarding Macrovision's encryption technology.

In other cases, the electronic tether is critical to the business model. Napster has gone legit with its Napster To Go service. Its ads poke fun at the iPod and iTunes's 99 cents a song pricing noting that you could spend \$10,000 to fill up your iPod. Napster just wants \$15 and will hand over a million songs. The catch? Napster is a music rental service; it's \$15 a

---

<sup>27</sup> And we are already starting to see consumer litigation when product features are disabled. See Christopher Rhoads, *Cellphone Users Sue, Saying Carrier Cut Phone's Features*, Wall Street J B1 (Jan 13, 2005) (alleging that Verizon disabled phone's native Bluetooth wireless technology to direct more traffic to its wireless network).

---

month forever, and if you don't pay the \$15 some month, your MP3 player can no longer play any of the songs stored on it. Napster To Go requires monthly renewal and your downloaded songs will die without it.<sup>28</sup>

In other products, the control is more obviously a choice. Google Desktop Search automatically updates—it just does it—no questions asked.<sup>29</sup> And, similar to Napster To Go, software can easily build-in obsolescence, by giving the software an expiration date and thereby a limited life.<sup>30</sup> Once the software has stopped working, the end-user is forced to download new software if she wants to continue to use it, and that software can upgrade or downgrade the user's experience.<sup>31</sup>

---

<sup>28</sup> See Wilson Rothman, *Music Buffet: Loading Up for Takeout*, NY Times E1 (Mar 17, 2005); Walter S. Mossberg, *'Napster To Go' Offers Alternative to iTunes—If You Keep On Paying*, Wall Street J B1 (Mar 17, 2005).

<sup>29</sup> See the Terms and Conditions of Use for Google Desktop Search (“Automatic Updates. Google Desktop Search may communicate with Google’s servers to check for available updates to the software, such as bug fixes, patches, enhanced functions, missing plug-ins and new versions (collectively, ‘Updates’). During this process, Google Desktop Search sends Google a request for the latest version information. By installing the Google Desktop Search, you hereby agree to automatically request and receive Updates from Google’s servers.”) (available at <http://desktop.google.com/eula.html>).

<sup>30</sup> See, for example, RealNetworks’s discussions of this for its beta software (available at <http://service.real.com/help/faq/betaexp.html>).

<sup>31</sup> Both of these possibilities—automatic updates of the sort seen with Google Desktop Search or built-in software expiration with required renewal for continuing functioning—suggest that software designers can force updates. That makes it hard to understand some claims to the contrary. See, for example, Brief of Computer Science Professors Harold Abelson et al, *Metro-Goldwyn-Mayer Studios, Inc v Grokster Ltd* at 14 (cited in note 6) (“Even assuming that Respondents have the right and ability to deliver such software to end users, there can be no way to ensure that software updates are installed, and stay installed. End users ultimately have control over which software is on their computers. If an end user does not want a software update, there is no way to make her take it.”) Of course, a consumer could remove her computer from the network completely and avoid updates, but you can’t search the Internet off the network and you can’t download the next great song offline either.

There is little reason to believe that the private incentive for ongoing control will match with the possible social costs and benefits. Grokster is a good example of this. The *Napster* decision offered a roadmap for software designers seeking to limit their potential liability as secondary infringers. Don't be at the center of the p2p network and be sure not to have any ability to police the network. Intentionally relinquish control over the software.

The actual facts of *Grokster* are fuzzy on the extent of control retained by the software producer. Grokster and StreamCast were both defendants in the *Grokster* litigation. Both based their p2p software on the FastTrack software developed by KaZaa BV, a Dutch company. (KaZaa subsequently transferred control over FastTrack to Sharman Networks.) A dispute arose between StreamCast and KaZaa, and StreamCast switched from FastTrack to software that StreamCast created from the open-source p2p software Gnutella. In the course of that dispute, a FastTrack software upgrade was propagated throughout the Grokster and KaZaa user bases, and the consequence of that was to cut off StreamCast users from access to the Grokster and KaZaa networks.<sup>32</sup>

It is precisely this ability to propagate changes to products that is at stake in *Grokster*. The defendants wanted to disclaim control when in fact a modicum of control was retained. More importantly, how much control was retained was just a design choice, and one that might be made to limit potential legal liability. And we should note how different this is from *Sony*. As the Seventh Circuit made clear in *Aimster*, in *Sony*, the Supreme Court was unwilling to attempt to "demix" infringing

---

And going offline would not prevent expiration of time-limited software.

<sup>32</sup> *Grokster*, 380 F3d at 1159 n.5.

---



and noninfringing uses “because once Sony sold the recorder it lost all control over its use.”<sup>33</sup>

We should be nervous about this. We need to regard the choice about how and whether a product evolves as being one of the central decisions that arises in product design. This is much like viruses and antidotes: You shouldn’t build a virus if you can’t build and distribute the antidote. We could regard a product that doesn’t phone home as having been recklessly isolated. We should think of this as an intentional relinquishment of control. The manufacturer has set a process into motion and has willfully chosen to tie its hands so as to avoid any subsequent control over events.

We recall physical products with some frequency. So go to the web site of the U.S. Consumer Product Safety Commission—[www.cpsc.gov](http://www.cpsc.gov)—and see whether your car has been recalled. You know how this works: you get a letter in the mail from your car manufacturer asking you to bring your car so that something can be fixed, which they assure you, really wouldn’t be a problem at all were it not for the government’s finickiness with regard to safety. We have the ability to recall electronically networked products and the only question is whether we are going to create the right incentives for producers to design mechanisms to recall these products automatically.

---

### III. What is at Stake?

---

We should step back and figure out what we are trying to accomplish. The p2p technology that has given us *Napster*, *Aimster* and *Grokster* has put enormous pressure first on the music business, and soon—probably—on video as new approaches to

---

<sup>33</sup> *Aimster*, 334 F.3d at 648.

---

file sharing, such as BitTorrent, speed up downloading.<sup>34</sup> But we shouldn't fret about major changes in how an industry is organized. That inevitably is wrenching for the people most directly involved, but we accept this as the natural process of destruction and creation in a capitalist economy. If online distribution of music is really vastly cheaper than physical distribution of CDs—and it could easily be<sup>35</sup>—we should want the old means of distribution to die, just as the car replaced the horse and buggy.

Instead, we should focus on three issues: (1) the determinants of the effective scope of rights in sound recordings; (2) whether focusing on the balance of infringing and noninfringing uses captures the issues that we should care about in defining those rights; and (3) the benefits of creating an innovation safe harbor.

#### *A. The Scope of Effective Rights in Sound Recordings*

Before Napster, technology ensured the core one-to-one match between the physical CD and the use of the music. Sure, you could share a CD with your friends or make a copy using a tape recorder of some sort, but the transaction costs and imperfections of all of this limited sharing of CDs, either through physical transfer or through copying. Obviously, Napster changed all of that and destroyed the assumption that the sale of a CD put one copy of the music into one person's hands.

---

<sup>34</sup> See Clive Thompson, *The BitTorrent Effect*, *Wired Magazine* 151 (Jan 2005); Sarah McBride, *Threatening Lawsuits, Hollywood Launches War on Online Piracy*, *Wall Street J B1* (Nov 5, 2004). See also Kevin Werbach, *The Implications of Video P2P on Network Usage* (forthcoming in *Video Peer to Peer*, Columbia Institute for Tele-Information, 2005).

<sup>35</sup> For discussion, see generally William W. Fisher III, *Promises to Keep* (Stanford Law & Politics, 2004).

---

The business model of the industry was based on this one-to-one match. But that match also tracked the rights model of the law: copyright rightfully distinguishes ownership of the physical CD from ownership of the copyright, and ownership of the CD doesn't give the possessor any right to make or distribute copies of the music.<sup>36</sup> Prior to Napster, copyrights in the sound recordings were meaningfully enforceable, because the technology didn't make large-scale violations possible. With Napster and its successors, a single act of public access—sale of a CD or even playing a song on the radio—makes possible widespread distribution without regarding to the rights of the copyright holder.

The question is what to do in response to this technological shift, which, without a further response, has greatly shrunk the effective rights of the copyright holder. We could simply acquiesce in this change in effective rights and hope that copyright creators can make enough money elsewhere through touring and T-shirt sales or have sufficiently other strong reasons to want to create.<sup>37</sup> But a market for live music has always existed and the real question is the size of the net shift in revenues that will result if sound recordings can no longer be sold and whether such a shift is a good thing or a bad thing.

---

<sup>36</sup> See 17 USC §§ 106(1) (right to reproduce the work in copies or phonorecords), 106(3) (right to distribute same), 202 (“Ownership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied. Transfer of ownership of any material object, including the copy or phonorecord in which the work is first fixed, does not of itself convey any rights in the copyrighted work embodied in the object; nor, in the absence of an agreement, does transfer of ownership of a copyright or of any exclusive rights under a copyright convey property rights in any material object.”)

<sup>37</sup> See Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U Chi L Rev 263, 269-70 (2002).

---

Or we can look for approaches to putting the fear of God into end-user downloaders.<sup>38</sup> The standard deterrence story calculates expected punishments based on the probability of getting caught and prosecuted times the resulting punishment. Depending on our tastes, we can play with both sides of that, putting additional resources into pursuing end-users—both the RIAA and the MPAA have done that—and thereby increasing the probability of detection. We can boost penalties too, though much of the current discussion of the statutory penalties for copyright violation argues that those penalties are already too high.

And copyright holders will take steps to protect themselves too, to take a variety of measures of self-help.<sup>39</sup> The movement towards digital rights management (DRM) is one of, at a minimum, restoring the core one-to-one relationship we saw with physical CDs: one CD, one copy and one end-user. DRM seeks to restore the control over copies that naturally came with the limited opportunities defined by the offline environment of the world of physical CDs. To be sure, it may do more than that as well, as DRM makes possible more finely-grained control and a possible broad shift from a model of ownership and zero marginal cost per use to rental and per-use charges.

### *B. Assessing Infringing and Noninfringing Uses*

While we might choose to calibrate our copyright tests in terms of the extent of infringing and noninfringing uses—as *Sony* does and as the record companies and movie studios would have us do in *Grokster*—those metrics don't immediately match to social benefits and harms. The focus on infringing and non-

---

<sup>38</sup> Lemley & Teece, 56 *Stan L Rev* at 1351 (cited in note 15).

<sup>39</sup> As discussed in greater detail in Douglas Lichtman, *How the Law Responds to Self-Help*, 1 *J Law Econ & Public Policy* (forthcoming 2005).

---

infringing uses is just how copyright keeps score, but there is a big gap between this scorekeeping and the issues that we actually care about.

The copying of copyrighted works usefully forces us to consider the virtues and vices of ordinary theft of physical goods and then to work our way back to unauthorized copying of intangible works. So consider the theft of a bushel of apples from my back yard. Stealing the apples just transfers the apples from me to the thief, but the apples themselves remain as before and so social wealth appears unchanged.

But there are two key problems with this theft. First, we have no assurance that the apples are moving to someone who values the apples more than those apples were valued by me. The thief may value the apples at \$1 while I value the apples at \$10, and, if so, the transfer reduces wealth by \$9. Of course, you might say, it is just as likely that the thief values the apples at \$10, while I value them at \$1, so we can't say anything sharp about the involuntary transfer.

But we can say something more precise if we compare involuntary transfer to voluntary transfer. So suppose that I consider swapping the apples for a bunch of bananas. If I value the apples more than the bananas, the voluntary transfer doesn't take place. If my potential trading party values the bananas more than the apples, the transfer doesn't take place. The deal only happens if we both prefer the trade over the status quo, and in that case, we know society is better off from the trade. Voluntary transactions should be wealth enhancing—relative to the status quo—while involuntary transfers of physical goods lack any such presumption.

Now for the second point. When property can be stolen, we will see investments relating to the possibility of theft by both the owner and the thief. The owner will invest to protect the property, and the thief will invest to overcome the owner's

---

protective steps. Both sides can spend substantial resources and yet the risk of theft may be completely unaltered. In the absence of easily enforced state-defined property rights, parties will invest resources to create their own property rights.

Contrast physical property with intangible property. The first point changes while the second continues to bite. As to the latter, absent meaningful legal protections for intangible property, we will see measures and countermeasures relating to the protection of that property, just as we saw with physical property.

But the transfer analysis is quite different. If I copy a song from your CD, you continue to have the song as well. Holding everything else constant, my copy of the song creates more use of the song and that raises social welfare. The record companies will talk about lost profits and lost sales and the academics can see if they can quantify that claim, but whatever the empirical results actually are on that, nonconsensual use is an increase in use and that is a social good.<sup>40</sup> Put this way, this is an exercise in price discrimination similar to selling hard-bound and paperback books. Some customers buy the song on a CD or through an online music service such as iTunes. Others users download the song for nothing through a P2P network.

---

<sup>40</sup> Recent empirical work includes Stan J. Liebowitz, *File Sharing: Creative Destruction or Just Plain Destruction?* (Working Paper Dec 2004) (available at <http://som.utdallas.edu/capri/destruction.pdf>) Felix Oberholzer & Koleman Strumpf, *The Effect of File Sharing on Record Sales: An Empirical Analysis* (Working Paper Mar 2004) (available at [http://www.unc.edu/~cigar/papers/FileSharing\\_March2004.pdf](http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf)); Rafael Rob & Joel Waldfogel, *Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students* (Working Paper Sept 30, 2004) (available at <http://www.law.upenn.edu/polk/dropbox/waldfogel.pdf>); and Alejandro Zentner, *Measuring the Effect of Music Downloads on Music Sales* (Working Paper) (available at <http://www.law.upenn.edu/polk/dropbox/zentner.pdf>).

---

We can identify two natural sources of harm here. One is the reduced number of creations that artists will make if artists cannot hold a property right in their work. A second source of harm is the resources that, say, record companies and artists will invest to create their own property rights in the absence of meaningfully enforceable legal property rights. This is the war of attrition idea: I spend resources to protect my rights and you spend resources to invade them, and so it goes. But the non-consensual use of the music itself is not a harm, and indeed, it may be a benefit of p2p technology.

### *C. The Sony Test as Innovation Safe Harbor*

The great virtue of *Sony's* substantial noninfringing use test is that it creates an innovation safe harbor. And it does so in a context where we could reasonably fear that we will find it difficult to coordinate innovation over time. Consider a two-stage innovation. The first-stage creator can't participate in second stage benefits—assume difficulties of coordination and negotiations—but assume that the first stage is essential to have the second stage development. Frame this innovation as having first-stage social benefits of  $B_1$  and social harms of  $H_1$  and second-stage social benefits of  $B_2$  and social harms of  $H_2$ . If the applicable legal rule forces the first-stage innovator to internalize all the harm, she will move forward if  $B_1 > H_1$  and not otherwise. But socially we want her to move forward if  $B_1 + B_2 > H_1 + H_2$ . We will want to move forward as a society but won't do so given the private incentives if a disproportionate amount of the net social benefit appears at the second stage and can't be captured by the first-stage mover.

The *Sony* test avoids this problem for the innovator, as the test effectively just looks to the size of  $B_1$ . At the same time, the *Sony* test never confronts the question of whether the sum of the benefits of the two stages of innovation exceeds the sum

---

of the costs. That is its central problem, and the question is whether we can do better than *Sony*. I think we can.

#### IV. A New Test for Networked Products

---

We should modify the *Sony* test of substantial noninfringing use and replace it with a more textured test that reflects the control and evolution opportunities available with networked products.

In some sense, the design point and the current mix of uses are orthogonal issues. Here is what I mean by that. My prior criticism of the *Sony* test emphasized that the test created no incentives to design a product to eliminate infringing uses.<sup>41</sup> So long as the product is cable of substantial noninfringing uses, the producer of the product avoids third-party liability. The extent of infringing uses is irrelevant as is the question of whether the product could have been designed to minimize infringing uses.

But suppose that we replaced the *Sony* test with a primary use test, stating that a producer avoided third-party liability if the primary use of the product was noninfringing. What are the design incentives then? The producer has the incentive to eliminate additional infringing uses only at the tipping point between liability and non-liability. If the product has a sufficiently large set of noninfringing uses, then again the producer has no reason to reduce infringing uses, even if it would be cost-effective to do so.

The real question is just that: is it cost-effective to reduce infringing uses? That question exists independent of whatever mix of infringing and noninfringing uses will result from the

---

<sup>41</sup> See Picker, 47 Antitrust Bull at 444-45 (cited in note 11).

---



currently-designed product. To be extreme, imagine a product that will create \$10 million worth of beneficial noninfringing uses and only \$100 in harmful infringing uses. This is a wonderful product. But if we could spend \$5 for a modified design that would keep the same benefits while eliminating the harmful infringing uses, we should do so.

So *Sony* does a poor job with design incentives. Under its test, altering the extent of infringing uses has *nothing* to do with whether the producer will face liability for the product. A primary use test would do somewhat better but only in the zone of altering liability. The test would create no design incentives for a product outside of that zone, such as my \$10 million product in the last paragraph. Given all of that, what role should a use test place if it bears little relationship to the design inquiry?

The use test matters for the question of whether to release a product in the first place. As discussed in Section III.C. above, *Sony* creates a safe harbor for product release and there could be circumstances where we think that having such a safe harbor is sensible. That really depends on how frequently you think the particular conditions described above occur. The mistake is to treat the existence of that question as dispositive of the question of whether the producer should have an original design obligation to minimize infringing uses or, now with networked products, an ongoing design obligation to do so.

#### *A. The New Test*

The new test should be a conditional test:

- If the producer chooses to let go of the product so that the producer cannot exercise control going forward and therefore cannot evolve the product in response to actual use, the producer should face a hard use test. I haven't spent much time thinking about whether that

should be framed as “primary use,” “dominant use,” “predominant use” or something else. There are obviously differences there—certainly between the first formulation and the second and third—but those differences aren’t my focus here. Given the \$10 million example set forth above, we should probably couple that with an independent obligation to take sensible design steps to eliminate infringing uses.

- If instead the producer ensures that the product can phone home so that updates can be promulgated throughout the system for the networked product, the producer should face a substantial noninfringing use test, coupled with the duty to evolve the product to eliminate infringing uses. “Eliminate” is quite strong, of course, so this could be framed instead in a number of ways, say, “eliminate infringing uses when it is cost-effective to do so” or “eliminate [the majority/the predominant number] of infringing uses.” As to the evolution duty, more on the in a minute, but do note that Section 512 of the Copyright Act creates a version of this for Internet service providers and that framework provides a natural starting point. And the litigation in *Napster* itself offers another look at product evolution. Both of these turn on a notice-and-takedown mechanism.

We should start by getting rid of one bogey, namely shouldn’t we reject any test that the VCR itself would have failed? We need to be careful about retrospective curve-fitting. As I have emphasized, for the products of interest, the core control and evolution properties have changed. Sony couldn’t evolve the installed base of VCRs and would always be constrained by the installed base for any possible changes in the product going forward. Cheap communications, storage and

---

machine intelligence have made the world in which the VCR was launched the world of yesterday. We shouldn't build a test that doesn't match the opportunities of the times.

As to the suggested test itself, a couple of points are important. As to the first part of the test, I continue to think that the Court was wrong to embrace the substantial noninfringing use test in *Sony*,<sup>42</sup> taking as a given copyright's scorekeeping system of infringing and noninfringing uses. As Section III.B. above suggests, we should be skeptical about that scheme, and perhaps we should understand *Sony* itself as embracing that skepticism in adopting the substantial noninfringing use test. But we should address the problems with the use tests directly, and hence I continue to believe that if a product has to be evaluated as is, on a one-time basis—as we will do if the potentially networked product has been disconnected and won't phone home for updates—we should apply a more stringent test, such as one that finds contributory infringement if the primary use of the product is infringing.

But we need not live with a single point-in-time evaluation of the product, and should not if the producer can exercise control over the product at a distance. The two-part test suggested above creates an incentive for the producer to maintain control and continues to allow an innovation safe-harbor while avoiding the draconian irrelevance of costs and missing design incentives associated with the current *Sony* rule.

### *B. Implementing the Ongoing Design Obligation*

How should we implement this ongoing design obligation? Do note one of the key virtues of this structure: this is an exercise in ex post design, not ex ante design by committee. We should be concerned about creating mechanisms which give a substan-

---

<sup>42</sup> Id.

tive or procedural veto over new designs. Match this with the First Amendment's strong presumption against prior restraint: the core instinct there is that we will too often make mistakes that block valuable speech, and that we are better served by trying to correct matters after the fact. The test suggested above does exactly that, as the networked product creator will be able to exercise control over the product at a distance, but can also release a new product immediately so long as it has substantial noninfringing uses.

We have a few data points on, as it were, contested, managed design. So consider three situations: the injunction process that followed the Ninth Circuit's first *Napster* decision; the approach taken towards Internet service providers (ISPs) in Section 512 of the Copyright Act; and the content-control certification process occurring as the FCC implements its broadcast-flag regime.

#### 1. NAPSTER II

After the original decision in *Napster* in the Ninth Circuit, on remand, the district court implemented an injunction that required Napster to take steps to block the sharing of copyrighted works. This meant ensuring that the work didn't show up in the centralized index that Napster presented to its users. The plaintiffs in the suit were required to give Napster notice of songs that were available in the index, and Napster was to take steps to delete those songs from the index. The subsequent appeal to the Ninth Circuit addressed exactly how that was to be done.<sup>43</sup> The district court had ordered Napster to shut down until it was able to block the distribution of the copyrighted works as to which it had already received notice: "It's not good enough until every effort has been made to, in

---

<sup>43</sup> *A&M Records, Inc v Napster, Inc*, 284 F3d 1091 (9<sup>th</sup> Cir 2002).

fact, get zero tolerance. ... [T]he standard is, to get it down to zero.”<sup>44</sup>

Napster is precisely the sort of networked product that I have in mind: it was capable of substantial noninfringing uses and, as a centralized file-indexing network, Napster could continue to exercise substantial control over its system. And indeed, the injunction process is the type of product evolution that I have in mind. So how did we do? Focus on the evolution of the filters and the interim shutdown. The iterative process on the filters is precisely what we should anticipate. The district court wanted to make sure that the full capabilities of the Napster system were used to block transfers of noticed copyrighted works. I confess to a certain agnosticism, so far, at least, as to who should bear the cost of creating these filters. We could easily imagine that the copyright holders would need to program the filters and bring those to Napster and that Napster would have had a duty to implement those filters. Think of this as a carriage obligation, perhaps a duty to deliver plug-ins created by the content creators. I don't know that I know enough to say who is better situated to produced these filters, hence the agnosticism.

It is easy to criticize the “zero tolerance” policy as articulated, though at some level, it does nothing more than insist that the full capabilities of the system be implemented. But zero tolerance is insensitive to the cost of achieving it. The standard lore of fixes is that you spend 10% of your effort to achieve 90% success, and 90% to get the last 10%, be in copyright infringement on Napster or pollution air particulates. That is why a sensible evolution duty might shift the burden of producing filters or other changes after a few iterations.

---

<sup>44</sup> Id at 1097.

---

The interim shutdown is another version of zero tolerance. Were I a district court judge, I could imagine implementing a shutdown in response to the perceived bad faith of Napster in implementing changes. You can imagine foot-dragging in this process, and the judge might have to resort to something tougher—daily fines or a shutdown—to command full attention to the necessary changes. But to move too quickly to shutdown will be to lose the incentive effects of my two-part test. If a product creator retains control, they shouldn't face an immediate shutdown merely because they can evolve the product to minimize infringing uses.

## 2. ISPs AND SECTION 512 OF THE COPYRIGHT ACT

Section 512 of the Copyright Act was added in 1998 as part of the Digital Millennium Copyright Act. Section 512 addresses the potential liability for copyright infringement of Internet service providers (ISPs) and establishes an administrative regime to control that liability. We can easily think of Section 512 as a jointly designed process to control potential copyright infringement that might arise from the services that ISPs provide to their customers.

ISPs provide a number of services. ISPs serve as the communications conduits through which customers upload and download content. ISPs also provide megabytes of storage space for customers and often provide hosting services for websites maintained by customers. All of this could put ISPs squarely in the middle of potential copyright infringement and could expose the ISPs to direct and indirect copyright liability.

Like most of us, ISPs would prefer not to face liability for their activities and Section 512 creates a safe-harbor for ISPs.<sup>45</sup>

---

<sup>45</sup> As to the broad question of ISP liability, see Douglas Lichtman & Eric Posner, Holding Internet Service Providers Accountable (forthcoming, *The Law and Economics of Cybersecurity*, Mark Grady & Francesoco Parisi, eds, 2005).

If ISPs dot their I's and cross their T's, they do not face liability for potential copyright infringement for online materials that are transmitted, routed, cached or stored on their systems.<sup>46</sup> To get the safe harbor, the ISP needs to do a number of things. First, the ISP needs to have in place a revocation policy, so that the ISP has a mechanism to kick off customers who are, as the statute puts it, "repeat infringers."<sup>47</sup> Second, the service provider must operate a service that accommodates standard technical measures designed to identify or protect copyrighted works.<sup>48</sup> Third, for material stored by ISP customers on the ISP's computers, the statute implements what is known as the notice-and-takedown procedure. The ISP must be set up to remove material from its system in response to complying notices regarding alleged infringement.<sup>49</sup> The statute addresses possible ISP liability for taking down material and creates a counter notification mechanism for customers to who believe in good faith that their content was mistakenly removed.<sup>50</sup>

This is a mechanism for evolving the service to minimize copyright infringement. As with any safe harbor, there will be issues about how it works. Both Napster and Aimster sought refuge in the safe harbor, but the 7<sup>th</sup> Circuit quickly dismissed the idea that Aimster could qualify and the 9<sup>th</sup> Circuit intimated that Napster wouldn't qualify either.<sup>51</sup>

---

<sup>46</sup> 17 USC §§ 512(a) (transitory digital network communications), 512(b) (system caching), 512(c) (information stored by customers) and 512(d) (use of search tools).

<sup>47</sup> 17 USC § 512(i)(1)(A).

<sup>48</sup> 17 USC §§ 512(i)(1)(B), 512(i)(2).

<sup>49</sup> 17 USC § 512(c).

<sup>50</sup> 17 USC 512(g).

<sup>51</sup> Respectively, *Aimster*, 334 F3d at 655 and *Napster*, 239 F3d at 1025.

---

### 3. TIVOGUARD AND THE BROADCAST FLAG

As part of the design of the new digital television system, the Federal Communications Commission has created a “broadcast flag” architecture. The flag captures Justice Blackmun’s notion in his dissent in *Sony* that it might be possible for the broadcast TV signal to contain a separate signal indicating whether or not the copyright holder authorized taping of the program.<sup>52</sup> As implemented by the FCC, the broadcast flag doesn’t control *copying* of content but instead creates a consent regime regarding the *redistribution* of content.<sup>53</sup> Toggling the flag will make it possible for the broadcaster to indicate whether it will allow its content to be redistributed. The Broadcast Flag Order is controversial<sup>54</sup> and has been appealed to the D.C. Circuit, where the court may get to the merits regarding the scope of the FCC’s authority, but only after the D.C. Circuit sorts through standing.<sup>55</sup>

---

<sup>52</sup> *Sony*, 464 US at 494.

<sup>53</sup> See *In the Matter of Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rulemaking*, 18 FCCR 23,550, 23,555 (2003) (“In light of our decision to adopt a redistribution control scheme and to avoid any confusion, we wish to reemphasize that our action herein in no way limits or prevents consumers from making copies of digital broadcast television content.”). On mechanisms of consent generally, see Picker, 70 U Chi L Rev (cited in note 2). Do note also that although the broadcast flag doesn’t implement a copy control for broadcast TV, copy controls are implemented for basic cable and premium cable services in the FCC’s so called Plug-and-Play Order. See *Compatibility between Cable Systems and Consumer Electronics Equipment: Second Report and Order and Second Further Notice of Proposed Rulemaking*, FCC 03-225 (Oct 9, 2003). HBO immediately implemented this system, limiting home users to one copy of its “linear” broadcasts—ordinary, scheduled broadcasts—and barring all copying of its nonlinear, on demand programs. See HBO FAQ page for Copyright Protection (available at <http://www.hbo.com/corpinfo/cgmsafaq.shtml>).

<sup>54</sup> See, for example, Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 Hastings Comm & Ent LJ 603 (2003).

<sup>55</sup> As to authority, see Robert T. Numbers II, *Note: To Promote Profit in Science and the Useful Arts: The Broadcast Flag, FCC Jurisdiction, and Copyright Implications*, 80



But my concerns here aren't FCC authority or standing. The Broadcast Flag Order contemplated further rulemaking about particular technologies and how those technologies would satisfy the redistribution control requirement. In the subsequent proceeding, thirteen technologies were considered, including a Windows DRM technology from Microsoft and a competing DRM approach by RealNetworks. Most of the technologies implemented measures tied to proximity to control redistribution. While the Internet is famous for collapsing distance, that doesn't mean that there still aren't metrics for capturing "distance" over the Internet. The proximity controls in the proceeding focused on the number of routers that a packet could cross before it would be discarded—Time to Live or TTL—or on establishing a cut-off time for a packet to travel between devices—Round Trip Time or RTT (measured in milliseconds).<sup>56</sup> This would make it possible for me to share content between my upstairs and downstairs TVs, but not between my downstairs TV and a TV in Siberia.

But TiVo—makers of the digital video recorder of the same name—instead looked to an authority-based model of control. In that framework, TiVoGuard, as the technology is known, would define a secure viewing group of ten devices that could share content, independent of the distance between those devices. So I could put my home TV in the same group as my TV in my summer home in Siberia, but the limit on the number of devices is intended to control mass redistribution.<sup>57</sup>

---

Notre Dame L Rev 439 (2004) (arguing FCC's adoption of broadcast flag exceeds its jurisdictional grant; on standing, see *American Library Ass'n v Federal Communications Commission*, No. 04-1037 (Mar 15, 2005) (ordering further briefing on standing issues).

<sup>56</sup> See *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, FCC 04-193, ¶ 8 (Aug 12, 2004) ¶ 8.

<sup>57</sup> Id at ¶¶19-23.

---

The MPAA objected to TiVoGuard, both in its then-current form, but also as to how TiVoGuard might evolve. This is the process of “change management,” a critical question of how dynamic technology can evolve given the FCC’s duties as to technology certification.<sup>58</sup> The MPAA sought to have the FCC approve all changes prior to implementation, which would give the FCC a powerful ex ante role in design choices.<sup>59</sup> Understanding that this would slow the pace of innovation, the FCC instead stepped back from ex ante evaluation of non-material changes to technology instead deferring to privately-agreed to procedures for change management.<sup>60</sup> But the FCC retained direct control over technical changes that were “material and substantial in nature,” even in circumstances where private parties had agreed to change management procedures.<sup>61</sup>

This is an interesting mix of private and public ex ante review of design choices. And matters got even more interesting in considering the MPAA’s motion for reconsideration. MPAA switched from advocating universal FCC ex ante review and instead favored having the FCC cede ex ante review authority to the private change management process.<sup>62</sup> In contrast, TiVo feared that private and public ex ante review might move on different time tracks. The MPAA could gain a modicum of control over technological change by favoring one technology over another, and that might be especially powerful if

---

<sup>58</sup> Id at ¶¶ 94-99.

<sup>59</sup> Id at ¶ 94.

<sup>60</sup> Id at ¶ 98.

<sup>61</sup> Id at ¶ 99.

<sup>62</sup> See Petition for Partial Reconsideration and Clarification by the Motion Picture Association of America et al, *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, MB Docket Nos. 04-55 to 04-68, 13 (Sep 13, 2004); Omnibus Reply Brief 9-10 (Oct 5, 2004).

---

private review move forward faster than the FCC's public review.<sup>63</sup> TiVo therefore favored all-or-nothing public review, meaning that either all of the technologies needed to go through the same public process or none of them did.

\*\*\*

These three examples—the subsequent litigation about Napster after the 9<sup>th</sup> Circuit's initial decision; the notice-and-takedown structure of Section 512 of the Copyright Act creating a safe harbor for ISPs; and the content-protection certification process for the broadcast flag—give a real sense of the complexities of designing rules and administrative processes for controlling copyright infringement. This is obviously ongoing and we are likely to see more of these in the future, but nothing here suggests to me yet that we can't move forward on managing design obligations related to copyright infringement.

---

## Conclusion

The emergence of distributed storage, machine intelligence and cheap communications has give rise to the networked product. These are products that can evolve even after versions of the product have been put into the hands of consumers. The most interesting consumer products of the day are networked products. This includes the natural successor to the VCR—whether the plain digital video recorder or the TiVo favored by the digerati—and the ubiquitous iPod and its less chic cousin MP3 players. This category also includes peer-to-peer software in its various forms, whether as Napster, Aimster or Grokster.

---

<sup>63</sup> Opposition of TiVo, Inc to the Petition for Partial Reconsideration and Clarification, , *In the Matter of Digital Output Protection Technology and Recording Method Certifications*, MB Docket Nos. 04-55 to 04-68, 21 (Sep 27, 2004).

---

More than twenty years have passed since the Supreme Court confronted the VCR in the *Sony* case. The substantial noninfringing use test has both virtues and vices. It has provided a safe harbor for product innovation. It makes it possible for a creator to toss a product onto the waters to see what happens, having only a vague sense of what will happen next. But *Sony* also provides no reason for a creator to design products to eliminate infringing uses.

The core fight over *Sony* turns precisely on the uncertainty of what happens next: what is the next use of the product not seen today? But *Sony* is framed in the context of episodic design with an installed-base constraint and no real possibility of feedback between actual use of the product and design. We are at a very different point now. Networked products evolve and we are now going to frame what ongoing design obligations should exist with regard to these networked products.

Once we combine software with communication to create networked products we then have products that can evolve in real-time (and do). Smart products “phone home” and update themselves. Phoning home—and the control that results from that—is a choice and one that designers of networked products make every day. Design ceases to be a one-time event and instead becomes a continuous process. And that is true not only for the next product sold, but also for the entire installed base. The dead hand of the past and the constraints of backwards compatibility are lifted.

We need to update the *Sony* test to reflect these possibilities. If the producer chooses to let go of a networked product so that the producer cannot exercise control going forward and therefore cannot evolve the product in response to actual use, the producer should face a hard use test, perhaps one tied to whether the primary use of the product is noninfringing. If instead the producer ensures that the product can phone home so

---

---

that updates can be promulgated throughout the system for the networked product, the producer should face a substantial non-infringing use test, coupled with the duty to evolve the product to eliminate infringing uses.

---