# THE IMPERFECT IS THE ENEMY OF THE GOOD: ANTICIRCUMVENTION VERSUS OPEN USER INNOVATION

*Wendy Seltzer*[†]

## TABLE OF CONTENTS



---



† Berkman Center for Internet & Society at Harvard University, and Silicon Flatirons Center at University of Colorado Law School, wendy@seltzer.org. The Author thanks many helpful discussants, including Yochai Benkler, Michael Carroll, Rashmi Dyal-Chand, Peter Jaszi, Fred von Lohmann, Benjamin Mako Hill, Paul Ohm, Betsy Rosenblatt, Seth David Schoen, Eric von Hippel, Jonathan Zittrain, and participants at the Telecommunications Policy Research Conference, Northeastern Law School's Colloquium, and Berkman Center for Internet & Society luncheon.

## I. INTRODUCTION

Imagine yourself a movie mogul wishing to use the latest and greatest in technology to protect your new release, "Pirates of the Caribbean, the Prequel."

You can, of course, limit the film to display in high-tech theaters, with bonded security guards scanning the audience for "cammers" and guarding the movie's physical path to the projection booth.[1] Before it gets there, you'll have to make sure everyone working on the film has the appropriate incentives to keep draft cuts from leaking pre-release.[2] Even then, the movie will likely leak to the streets through some chink in that armor (especially if it is as popular as you hope it will be). With luck, however, you have bought yourself some time and built enough buzz that people want to see the film in theaters even if they could get grainy copies to watch on small screens. You might even enhance the differential by showing in IMAX or 3D, creating an *experience* that is hard to replicate even as the bits are copied.[3]

Once its theatrical run winds down, though, you hope to exploit your investment further with a rental and sales run.[4] You could rent and sell unrestricted digital copies, relying on straight copyright law's prohibitions on commercial-scale reproduction, distribution, and public performance, but you want technological backup. So, to "keep honest people honest," you want to add "copy protection," wrapping the movie in either encryption or contract, or both.

---

1. *See, e.g.*, Dawn C. Chmielewski, *Secrecy cloaked 'Dark Knight,'* L.A. TIMES, July 28, 2008, at C1. Compare these protections with the more limited release-window protection Disney had for "Snow White." DAVID NIMMER, COPYRIGHT: SACRED TEXT, TECHNOLOGY, AND THE DMCA 17–18 (2003).

2. *See* Simon Byers et al., *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, *in* DIGITAL RIGHTS MANAGEMENT WORKSHOP (Moti Yung ed., 2003) (finding that "insider attacks" accounted for more than three-quarters of leaks, many of those prior to the DVD release).

3. *See* Mark Milian, *Which 'Avatar' to see? A look at IMAX, Dolby 3-D, RealD (and, yeah, boring old 2-D)*, L.A. TIMES BLOG, Dec. 29, 2009, http://latimesblogs.latimes.com/herocomplex/2009/12/which-avatar-to-see-a-look-at-imax-dolby-3d-reald-and-boring-old-2d.html.

4. *See* David Waterman et al., *Enforcement and Control of Piracy, Copying, and Sharing in the Movie Industry*, 30 REV. INDUS. ORG. 255, 258 tbl.1 (2007) (discussing release windows).

Encryption could prevent an unwanted user—one without the key—from being able to play the bits as a movie, no matter how many copies of them he makes.[5] An encrypted movie looks like a random string of ones and zeros when read off its disc—to the buyer, as well as to everyone else. But, unless you give the buyer the key, he's left with just a coaster (which he can buy more cheaply elsewhere). So you must also give the purchaser the means of decryption. If you hand him the key straight out, however, he once again possesses all the information necessary to make copies.

Instead of giving the secret key to the user directly, then, you entrust it to a "black-box" emissary,[6] a software program or hardware unit that you restrict to playing the movie in the form you have deemed permissible: play but do not copy, for example. Now that you have shared the secret with software or hardware, however, you have to guard that software or hardware as zealously as you did the original movie, preventing the key or the decrypted movie from leaking or being hacked out.[7] First, you've increased the number of assets to protect: neither the work *nor its decryption key* must be allowed to leak. Second, you've just shifted the locus of trust, not removed it. You still need to let the user see the movie, and you've determined you don't trust him (hence the need for DRM), but in order to trust the software or hardware manufacturer, you must make the manufacturers obey you rather than their products' user/owner. Simultaneously, you must take measures to prevent the user either from copying the physical object[8] or from obtaining any hardware or software that will play a copied object.[9]

---

5. If you use a known strong algorithm, properly, you can be assured that no one without the key will be able to decrypt it, at least not with computing power available today. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 152 (1996).

6. "Black-box" refers to the opacity of the processing between encrypted input and movie output. While the user can see the encrypted blob go in and get a movie in viewable format on the other end, he can't see what goes on in between/during the time the movie is decrypted.

7. *See, e.g.*, Ellen Messmer, *Black Hat: Researcher Claims Hack of Processor Used to Secure Xbox 360, Other Products*, NETWORK WORLD, Feb. 2, 2010, https://www.networkworld.com/news/2010/020210-black-hat-processor-security.html; Andy Patrizio, *Why the DVD Hack Was a Cinch*, WIRED, Nov. 2, 1999, *available at* http://www.wired.com/science/discoveries/news/1999/11/32263 (describing reverse engineering of the Xing software DVD decoder implicated in the first break of the DVD Content Scramble System).

8. The DVD format is controlled through a combination of patents on the format, copyright with anticircumvention, and even trademark. RealNetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913, 920 (N.D. Cal. 2009) (describing the DVD-CCA and its technology). *See generally* DEAN S. MARKS & BRUCE H. TURNBULL, TECHNICAL PROTECTION MEASURES: THE INTERSECTION OF TECHNOLOGY, LAW AND COMMERCIAL LICENSES (1999), http://www.wipo.int/edocs/mdocs/copyright/en/wct_wppt_imp/wct_ wppt_

You must, however, create this secure ecosystem with enough compatibility that users are attracted, *and* with enough control that content purveyors are assured their directives are being followed. After all, the users themselves are already in an environment before your movie comes along—they may have home computers, televisions, home theaters, home networks, video iPods, or iRivers. They are unlikely to want your single movie enough to retool all these systems around it or to buy a special-purpose viewing device just for it.[10] So your plan works best if you can take advantage of existing platforms. If those are insufficiently secure, you can try to engage a significant segment of the industry to work with you to move people simultaneously to a new standard (with the assistance of antitrust counsel to ensure that cross-industry collaboration is seen to expand the market, not control it).[11]

Thus you might, if you were a movie studio with enough market clout to be persuasive, propose to fellow studios, consumer electronics companies, and software developers that they jointly support a copy-protection scheme around a new digital format for video distribution, setting licensing terms for the use of and interoperability with that format.[12] Together, you could hope to achieve the market saturation that would make your format successful: only licensed "SuperDisc" players could show the latest and greatest Hollywood films in full digital glory. The virtual network thus created would make your usage rules seem to be natural complements to the new format rather than user-hostile restrictions of consumer rights. You would be able to hold companies to your licensing scheme with the threat of Digital Millennium Copyright Act (DMCA) liability if they defected; erstwhile

---

imp_3.pdf.

9. *See* Wendy Seltzer, *The Broadcast Flag: It's Not Just TV*, 57 FED. COMM. L.J. 209, 210 (2005) (describing the Broadcast Flag Rule's combined mandate of watermarking detection and obedience to flagged commands).

10. In special cases, that condition may be malleable. In 2005, the Motion Picture Academy sent 6,000 special-purpose limited-function DVD players to the Academy Awards screeners—a limited number of people designated to receive movies before their general DVD release. Even then, the limitations annoyed viewers and copies leaked. *See* Gary Gentile*, Studios eye new anti-piracy technology*, USA TODAY, July 2, 2004, http://www.usatoday.com/tech/news/2004-07-02-anti-piracy_x.htm; Britt Leach, Screeners for My Consideration, Veritas (Nov. 30, 2007), http://www.veritas-anydaynow.com/archives/reconsideringscr.html (detailing one Academy member's complaints and how precautions did not prevent copies from leaking).

11. *See, e.g.*, Letter from Joel I. Klein, Assistant Attorney Gen., Dep't of Justice, to Garrard R. Beeney, Sullivan & Cromwell (Dec. 16, 1998), *available at* http://www.justice.gov/atr/public/busreview/2121.htm.

12. *See id.*

competitors might even thank you (quietly) for helping to craft a set of legally sanctioned barriers to entry in the technology field.

While the copyright-backed licensing arrangement keeps the commercial players in check, you also want to limit upstart entrepreneurs and individual would-be copiers. It is not enough to demand that licensees limit the functionality of their devices if users can disable those limitations with a few keypresses of a remote control.[13] As your users get more sophisticated, you may also worry about their facility with screwdrivers, circuit boards, and software compilers. You therefore demand that your licensees impose their limitations in a manner "robust" against user modification.[14] The goal is that none but those who have bound themselves to your licensing terms must be able to access your movie.

Moreover, once you have succumbed to the technical-protection imperative, you are unlikely to stop at just one component. If you black-box the software or hardware decoder, but do not secure the digital outputs from that black-box, someone will be able to take the decrypted stream from there.[15] If you leave high-quality analog outputs, someone can re-digitize content obtained through the "analog hole."[16] If you shut down those outputs, however, you face the protests of early adopters and audiophiles who do not expect their functional, capable electronics to be selectively disabled.[17]

---

13. For example, many early region-locked DVD players could be made to play discs from any region with a few extra key-presses on the remote control. *See* Post-Hearing Comments of The Electronic Frontier Foundation, *In re Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Docket No. RM 2002-4 (June 5, 2003), at 6, *available at* http://www.copyright.gov/1201/2003/post-hearing/post10.pdf.

14. For a DRM implementation to make any sense in a scenario of limited trust, its barriers against user modification of the rights management must be at least as strong as those against user access to its protected content. *See* DVD-CCA CSS Procedural Specification § I.6.2.4–2.5, *available at* http://cyber.law.harvard.edu/seminar/internet-client/readings/week2/02-08CSS.pdf.

15. Hence High-Bandwidth Digital Content Protection (HDCP) for High-Definition Multimedia Interface (HDMI) and Digital Visual Interface (DVI) that provides for link-level encryption of digital video outputs, relying on digital handshakes to verify the trustworthiness of components on the other end of the video cable. *See* Digital Content Protection, HIGH-BANDWIDTH DIGITAL CONTENT PROTECTION SYSTEM 8, July 8, 2009, http://www.digital-cp.com/hdcp_technologies (click "HDCP Specification Rev. 1.4").

16. *See* Copy Protection Technical Working Group, Charter of the Analog Reconversion Discussion Group, http://www.cptwg.org/Assets/TEXT%20FILES/ARDG/analogcharterfinal11403.doc (last visited Feb. 18, 2010) (addressing "[c]opyright owner concerns over the present and future security of commercial audiovisual content that has been converted from digital to analog format and reconverted to digital format").

17. *See* Mark Hachman, *TV Digital Rights Management Surfaces Again*, PCMAG.COM, Nov.

Before you know it, if you take technological copy-restriction seriously, you're requiring that your viewers upgrade every device in their home networks to satisfy the digital handshakes and cryptographic demands of secure communications, or you are downgrading that high-definition video to low enough resolution that users wonder what is worth the fuss.[18] You are demanding that every "digital media device" manufactured incorporate anti-copying technology.[19] Now if only we could use a neuralyzer to erase viewers' memories of the movie after it finished,[20] we could even prevent them from making around-the-water-cooler "derivative works" by sharing detailed synopses with friends.

We haven't gotten the neuralyzer into mass production yet, but attempts to implement or mandate the other technological measures are well beyond science fiction. A host of acronym-laden associations and lobbying groups have procured or attempted to legislate various parts of this scenario.[21] Those who count on technology to solve the problems they believe technology has exacerbated are drawn inexorably toward stricter and stricter regulations of technology. As those legal and architectural regulations widen, so too does a serious unintended consequence: the limitation of independent development and user innovation.

♦ ♦ ♦

So what if DRM freezes user innovation? Most people will never modify their own media players. In a world where VCRs (and their DVD successors) still flash "12:00," why should we care about facilitating the more difficult user innovation? User innovation indirectly benefits even the non-technical end-user. When tinkerers have access to modify and develop technology, they tend to share their improvements, making them easier for non-tinkerers

---

4, 2009, http://www.pcmag.com/article2/0,2817,2355382,00.asp (discussing MPAA petition to the FCC regarding Selectable Output Control, and Public Knowledge opposition).

18. *See* Eric A. Taub, *Encryption Schemes Aimed at Film Piracy*, N.Y. TIMES, Aug. 30, 2001, at G6.

19. *See* Consumer Broadband and Digital Television Promotion Act (CBDTPA), S. 2048, 107th Cong. (2d Sess. 2002). This bill was introduced by Sen. Fritz Hollings. *See id.* Princeton Computer Science Professor Ed Felten generated a "Fritz's Hit List" of technologies that would have been regulated had the bill passed—anything that digitized audio or video, including baby monitors and Big-Mouth Billy Bass, the talking fish. *See* Fritz's Hit List, Freedom to Tinker, http://www.freedom-to-tinker.com/tags/fritzs-hit-list (last visited Mar. 16, 2010).

20. In the movie *Men in Black,* agents equipped with neuralyzers selectively erase the memories of witnesses who have seen too much. MEN IN BLACK (Columbia Pictures, 1997).

21. The footnotes have pointed to the real-world scenarios on which this low-skimming flight of fancy is based.

to obtain. Thus even if you do not find yourself drawn into the do-it-yourself (DIY) culture of modifying your own gear, you might be able to buy an off-the-shelf product that suits your needs better because it has been developed by or with insights from other user-innovators with tastes like yours; or you might hire someone to add the features you would like to a purchased product, finding you have more, cheaper options because no manufacturer claims a monopoly on upgrades and improvements.

Contrast the ecosystems around pre-recorded music and movies. Since the early 1980s, recorded music has been available in unencrypted digital form, on compact discs, while movies basically jumped from analog (and Macrovision-protected) VHS to DRM-encumbered digital with the 1997 introduction of the DVD and 1998 DMCA.[22] This difference (which record labels endlessly bemoan) has meant that the pool of pre-recorded music may be lawfully manipulated much more readily than pre-recorded video. CDs provide music directly to end-users in high-quality, unencrypted, digital form. End-users could choose DRM-free digital music long before most publishers or music stores offered DRM-free tracks online. A complete environment of music is freely usable on open playback devices.

Innovators have taken that freedom and run. When the CD player was introduced in 1982 (at a retail cost of $900),[23] it could play a disk, skip to an identified track, seek, or repeat. In the years since, the digital music experience has been enhanced by participants of all shapes and sizes: large manufacturers, small startups, and end-users. Disc-based players have added shuffle modes, digital outputs, menu-driven controls, multi-disc changers, and portable versions. Perhaps more importantly, music has not been confined to discs. The Diamond Rio, introduced in 1998, brought digital music to pockets too small for the "Discman."[24] A decade later, though the Rio is no more, it ushered in hundreds of portable music players.[25] Some of these players are built open;[26] others have been opened.[27] Some features that

22. Laserdisc never reached significant market share. *See* Laura Landro, *Get Set for Laser Videodisks, Round Two*, WALL ST. J., Dec. 6, 1988, at B1.

23. John Marcom, Jr., *Sales of Consumer Electronics to Grow Modestly in 1985, Industry Group Says*, WALL ST. J., Jan. 7, 1985, at 7.

24. Ashley Dunn, *The Cutting Edge Gift Guide*, L.A. TIMES, Nov. 30, 1998, at C6 (noting that "the ultimate Christmas gift this year is Diamond Multimedia's $199 Rio PMP300 portable MP3 player—a cigarette-pack-size device"); *Sony Corp. Introduces New Compact-Disk Player*, WALL ST. J., Mar. 17, 1988, at 7 (describing a four-inch player in which five-inch disks "extend past the player's edges").

25. Mike Musgrove, *Everything Seems to Play MP3s Lately*, WASH. POST, Dec. 7, 2001, at E1.

26. *See, e.g.*, Teuthis Open Source Kits, Daisy MP3 Project Page, http://www.teuthis.com/daisy/index.html (last visited Mar. 20, 2010).

first appeared in user-written code, such as audio recording for the iPod, have since been commercialized, bringing user-designed features to the masses.

The Squeezebox, for example, started out as a little Ethernet-connected music gadget from a small start-up, Slim Devices. The early Slimp3 could take music from the computer to the stereo system, via a digital-to-analog converter, a bit of computing power, and a bright display. It has since spawned a full line of music devices, from wireless consumer-grade products to high-end audiophile ones.[28] Connected to a computer running Squeezebox Server software, the Squeezebox liberates music from the hard drive for listening anywhere in the home, adding a "now playing" display, a remote, web-based selection menus, and all the flexibility of a random-access computer-based music library—long, uninterrupted playlists, easy access to all your music in one place, and no disks to change or scratch. Because of music's open format and users' ability to move it around without copy-controls, the Squeezebox could be developed with no support or permission required from any in the established music industry. Its developers could take the user-availability of digital music as given, and build to interoperate at that interface.

Moreover, those who purchase the Squeezebox are not limited to what comes in the box; they can customize the open-source Squeezebox Server software. Many have, writing and sharing plugins to set musical alarms, program radio stations, show the weather, and integrate with other applications.[29] Even those who do not write code have access to the community's products, since many users share their additions.[30] Even the Chumby, an open-by-design hardware platform that looks like a beanbag

27. *See, e.g.*, Rockbox Software Project, http://www.rockbox.org/twiki/bin/view/Main/WhyRockbox (last visited Mar. 20, 2010).

28. *See* Logitech, Logitech Squeezebox, http://www.logitechsqueezebox.com/. Slim Devices is now a unit of Logitech.

29. *See* SqueezeCenter Plugins, http://wiki.slimdevices.com/index.php/SqueezeCenter_Plugins (last visited May 15, 2010). Users can create playlists with third-party recommendation engine MusicIP, organize the music's metadata against Gracenote or MusicBrainz indexes, or send listening habits as status listings to a blog.

30. The Squeezebox Server is released under the GNU General Public License, version 2. *See* Softpedia, Download SqueezeBox Server, http://mac.softpedia.com/get/Audio/SqueezeCenter.shtml (last visited May 15, 2010). The GNU GPL under which it was released does not *require* redistribution of the source, but says that one who distributes compiled binaries must also distribute their accompanying source. *See* Free Software Foundation, GNU General Public License, Version 2 § 3 (1991), *available at* http://www.gnu.org/licenses/gpl-2.0.html. Many user-developers find it attractive to share their work with the community, inviting others' improvements.

with a screen (and speaker), can be programmed to play music from a Squeezebox Server-managed library.[31]

The Squeezebox is but one example. Because of the open nature of digital music and broadcast television, users and independent developers can create and choose their preferred experience. We can fill portable devices with shuffled sets of music tracks; we can outfit our homes with networked audio–video systems that share content around the house or follow us as we move; we can time-shift television on our schedules; we can synchronize collections among devices and across formats. DJs—professional or home—can mesh beats seamlessly from track to track.[32]

Now contrast music's vibrant development environment and the range of music-capable devices to the limits around recorded movies. The DVD has been one of the most successful consumer electronics products of all-time, its numbers mounting rapidly after its 1997 launch,[33] but the movie-watching experience has barely changed since then. HD-DVD and Blu-Ray put more higher-resolution images on the disc, but still let consumers do little more than watch the movie and extras.[34] For the most part, new movie-watching technologies offer only the same basic features that DVD players have had since their introduction a decade ago. No DVD jukebox,[35] no easy direct navigation, no option to select scenes from a few movies to show in sequence or in comparison. Moreover, it is only in the last year that end-users have gotten a studio-authorized opportunity to copy a movie to a portable

31. *See* Chumby: Squeezebox Server, http://www.chumby.com/pages/cp_squeeze (last visited May 15, 2010).

32. True, copyright law constrains users when they make copies, but so long as they have purchased the music, they claim fair use rights to manipulate its listening experience even when that entails transitory "copies." *See* JESSICA LITMAN, DIGITAL COPYRIGHT 26–28 (2001) (describing the consequences of treating everything digital as copying). Copyright law should not constrain the mere act of listening; *cf.* The Cartoon Network, LP v. CSC Holdings, Inc., 536 F.3d 121, 139 (2d Cir. 2008) (finding that Cablevision's "remote storage" digital video recorder did not violate plaintiffs' copyrights).

33. *See* Ross Johnson, *Getting a Piece of a DVD Windfall; Sales Are Soaring And Hollywood Is Split Over Dividing Profits*, N.Y. TIMES, Dec. 13, 2004, at C1.

34. It is not even clear many consumers notice the difference. A number still have low-definition screens, and commercial counterfeiters have taken advantage of people's lack of visual acuity to sell fake Blu-Ray discs compressed to lower resolution. Geoffrey A. Fowler, *Pirates Prey on Blu-Ray DVD Format*, WALL ST. J., Nov. 17, 2008, at B1.

35. Kaleidescape introduced a $8,000 system; although it won the first round of a contract fight with DVD-CCA, the appellate court reversed and remanded for consideration of the CSS General Specification that Kaleidescape contended was inapplicable, DVD Copy Control Ass'n v. Kaleidescape, Inc., 176 Cal. App. 4th 697 (Cal. App. 6th Dist. 2009). DVD-CCA successfully enjoined RealNetworks from building a cheaper competitor. *See* RealNetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913 (N.D. Cal. 2009).

player, send it to a mobile phone, or put it onto the home network so it moves from kitchen to living room to bedroom. Whereas both commercial and home-brew MP3 players, spurred by amateur development, have been able to do most of this for music for years, movies lag far behind. DVD's DMCA-backed encryption locks out independent developers and much experimentation. Users have had to wait years for the "business models" to catch up with features such as digital downloads or an authorized "digital copy."[36]

♦ ♦ ♦

An impressive body of scholarship has formed around digital rights management (DRM).[37] Most legal academics criticize DRM for its effects on fair use: in a DRM-encumbered world, a media educator cannot cue movie clips for classroom commentary without special exemption; a literary critic is blocked from extracting e-book pages (or has the e-book deleted out from under her)[38]; and a mashup artist is restricted in sampling scope. These restrictions are direct consequences of DRM, problematic for copyright and culture.[39] Most scholars have thus characterized the "DRM problem" as that of accommodating fair use. Some argue that the loss of some marginal fair uses is an appropriate tradeoff for greater security of copyright protection.[40] Others argue that fair use may be approximated by user permissions, overrides, or appeals to a third party.[41] Still others contend that fair use of the

36. *See, e.g.*, Disney File Digital Copy, http://disney.go.com/disneyvideos/disneyfile/ (last visited Mar. 25, 2010). Rentals are still limited in variety, and portability often restricted to a small and inconsistent set of compatible devices.

37. *See infra* Part III.

38. *See* Geoffrey A. Fowler, *An Orwellian Moment for Amazon's Kindle*, WALL ST. J. DIGITS BLOG, Jul. 17, 2009, http://blogs.wsj.com/digits/2009/07/17/an-orwellian-moment-for-amazons-kindle/ (describing Amazon's erasure of the e-book "Nineteen Eighty-Four" from users' Kindles because the supplier lacked the rights to sell it).

39. *See generally* LITMAN, *supra* note 32; Julie Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of 'Rights Management,'* 97 MICH. L. REV. 462 (1998); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

40. *E.g.*, Randal Picker, *Copyright and the DMCA: Market Locks and Technological Contracts*, *in* ANTITRUST, PATENTS AND COPYRIGHTS: EU AND US PERSPECTIVES 180 (Francois Leveque & Howard Shelanski eds., 2005); Jane Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC'Y U.S.A. 113 (2003).

41. *E.g.*, Barbara L. Fox & Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, 46 COMM. ASSOC. COMPUTING MACH. 61–63 (2003). *Contra* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001) (considering and ultimately rejecting this path); John S. Erickson & Deirdre K. Mulligan, *The Technical and Legal Dangers of Code-based Fair Use Enforcement*, 92 PROC. INST.

digital media is unnecessary, because fair use can be made from a work's other formats.[42] Yet others argue that because the heart of fair use is use without permission in unanticipated manner; technological controls and exceptions can never match the range of considerations a judge would be able to address if the matter came to litigation,[43] nor the spontaneity of "use first, ask permission later."

The fair use debate is important, but it is not the only problem with DRM. Equally important, but thus far largely overlooked, is the impact on user innovation and on the permitted development of media technology. Because DRM systems, by design and contract, must be hardened against user-modification, they foreclose a whole class of technology and an entire mode of development. Moreover, this problem is distinct from that of fair use. Even if we could wave a magic wand and fully accommodate fair use in DRM, the incompatibility with user innovation would persist, because it stems from a different and deeper aspect of the DRM system. Even the "fairest" DRM systems on the market today are unfair to the developers of new technology.

Anticircumvention law, backing technological protection measures (TPMs) and robustness rules, is fundamentally incompatible with deep-level user innovation. In a utilitarian copyright regime, where, as Thomas Macaulay put it, copyright is accepted as "a tax on readers for the purpose of giving a bounty to writers,"[44] the law must account for *all* the costs of foreclosing open modes of development. The "mode-of-development tax" is a significant unrecognized burden on the cultural, creative, and technology-based economy.[45]

---

ELECTRICAL & ELECTRONICS ENGINEERS 985, 995 (2004) ("In this sense the system would be broken from a copyright perspective: the system may protect the creator's copyright while upsetting the balance of copyright law by taking away users rights and the ability of new "rights" to emerge through the organic legal process.").

42. The court in *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), adopted the plaintiff's arguments to this effect.

> [T]he DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie.

*Id.* at 459.

43. *See* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 57–59, 85–87 (2006).

44. Thomas Macaulay, Speech Delivered in the House of Commons (Feb. 5, 1841), *in* PROSE AND POETRY 731, 734–35 (G.M. Young ed., 1952).

45. For an example of this technological tax, one need only look to the development of

Part II of this Article examines the law and technology of digital rights management, particularly the interaction of statutory law, technological measures, and the contractual "robustness" conditions generally attached to them. Part III briefly reviews the history and existing academic debates around DRM to consider why they have overlooked the user-innovation impacts. Part IV develops examples of the DRM conflict with open development, contrasting more flexible "advisory" anti-copying features. Part V then introduces the rich economics and business literature on disruptive technology and user innovation, to argue that DRM's copyright-driven constraints substantially harm cultural and technological development as well as user autonomy. Part VI concludes that the mode-of-development tax is too high a price to pay for imperfect copyright protection.

## II. THE MECHANICS OF CODE AND LAW

### A. BASIC TECHNOLOGY OF "DIGITAL RIGHTS MANAGEMENT"

The technology of digital rights management aims to "give" users digital works while managing their uses or copies: a DRM-protected track from the iTunes music store can be transferred to only five devices; a DVD can be played only on authorized players, coded to the region for which it was sold; a pay-per-view movie "expires" twenty-four hours after ordering. DRM's fundamental challenge is to provide the desired uses but not more: give users enough control to enjoy the work and not enough to allow them (or systems under their control) to copy the works.[46] At the extreme, of course, one could develop a completely secure system by denying access to everyone, but that would find few buyers in the marketplace.[47]

---

music players versus DVD players, described *supra*.

46. *See* Jason F. Reid & William J. Caelli, *DRM, Trusted Computing and Operating System Architecture*, CONFS. RES. & PRAC. INFO. TECH., Jan. 2005, at 127, *available at* http://crpit.com/confpapers/CRPITV44Reid.pdf.

> The essential premise of DRM is that a rights owner wishes to license digital content (which is represented as binary digits or bits) to a licensee or customer who agrees to be bound by the terms of the license. Note that the customer is not buying the bits themselves. Rather, they are buying the right to use the bits in a defined and restricted manner, as authorized in the terms of the license. Hence the license defines a type of usage policy.

*Id.*

47. Short of that extreme, media-producers dream of a price-segmented market, where each use can be priced according to its users' willingness to pay. *See* Michael J. Meurer, *Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works*, 45 BUFF. L. REV. 845, 877 (1997). *See generally* William W. Fisher III, *When Should We Permit Differential Pricing of Information?*, 55 UCLA L. REV. 1 (2007).

A digital media file is a series of bits—ones and zeros—written in a format that can be read by a hardware or software player and output as music, text, video, or a multi-media combination. Digital files are inherently copyable; there is usually no scarcity of bits or storage media to hold them. As cryptographer Bruce Schneier says, "trying to make digital files uncopyable is like trying to make water not wet."[48] To manage the bits, therefore, providers try to control access—restricting listening to authenticated, paying subscribers or hindering copying—by enclosing the bits in a container of sorts, either physical or digital, that resists access by a would-be copyist.[49]

Since bits are readily copied, copy controls depend on the cooperation of their access and playback devices to function. Publishers try to embed their works in an ecosystem where copies are unplayable. Videocassettes, an analog recording medium, use Macrovision's embedded noise as a containment strategy.[50] While this protection could be defeated if either the first VCR were told to suppress the Macrovision signal or the second to ignore it, it was effective when used with a pair of compliant devices.[51] Effective VHS copy-control, therefore, depended on both manipulating the format of the signal and constraining the design of playback and recording devices. Since what technology could set, technology could alter; technology is necessary but not sufficient to protect digital content. To control copying, anti-copying schemes control environments (and their inhabitants).

---

48. *See* Bruce Schneier, *Quickest Patch Ever*, WIRED NEWS, Sept. 7, 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/09/71738 (describing how quickly Microsoft patched its Media Player application to disable the newly-released FairUse4WM software, which stripped the copy protection from Windows Media DRM 10 and 11 files).

49. More precisely, we can distinguish *access controls*, *copy controls*, and *watermarks*: access controls aim to stop unauthorized users from accessing a resource; copy controls to prevent its reproduction; and watermarks to track the usage or copying of a resource, without necessarily preventing any action.

50. *See* How Stuff Works, How Does Copy Protection On a Video Tape Work?, http://electronics.howstuffworks.com/question313.htm (last visited Mar. 20, 2010) A signal embedded in the vertical blanking interval of the video data is not displayed on television playback, but instead interferes with the automatic gain control component of other videocassette recorders, hindering VCR-to-VCR recording. *Id.*

51. Macrovision initially took advantage of accidental properties of the VCR technology. Once they were aware of its use as copy-control, however, VCR makers could design their devices not to be fooled by Macrovision's spurious signals. Therefore, to make this copy-control more robust, Congress added a legal mandate in the DMCA. 17 U.S.C. § 1201(k)(1)(A)(i) (2006) ("[N]o person shall manufacture, import, offer to the public, provide or otherwise traffic in any . . . VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology. . . .").

Pure technology content control is a perpetual arms race. Protected environments persist for a time, then fall to stronger attacks through code analysis, hardware manipulation, or signal capture from the device.[52] Because there are many more people trying to break protection systems than to strengthen them, the attackers have the long-run advantage.[53] Thus,

52. If playback is in software, users might try to get the software to dump its unencrypted data, e.g., by copying it from memory, emulating a sound or video card, or emulating an entire environment. *See* SETH DAVID SCHOEN, TRUSTED COMPUTING, PROMISE AND RISK (2003), http://www.eff.org/files/20031001_tc.pdf; *see also* ANDREW HUANG, HACKING THE XBOX 119–37 (2003) (hacking hardware); Messmer, *supra* note 7 (same).

53. Readers may ask how DRM differs from strong encryption, which can be implemented in open code and yet withstand breaks against the significant state and non-state actors who would like to break it. Encryption to protect content against eavesdropping by a third-party adversary is a hard but well-understood problem. We now have algorithms implementable (and implemented) on personal desktop computers that are believed to be impervious to attack by all the computing power in the world. Only a brute force attack, trying every possible key, could decrypt, and even with a mere 64 bit key, that leaves $1.8 \times 10^{19}$ possibilities.

DRM's problem is different, though. As Cory Doctorow puts it, "In DRM, the attacker is *also the recipient*." Cory Doctorow, Address to the Microsoft Research Group, June 17, 2004, *available at* http://craphound.com/msftdrm.txt. The viewer of DRM-protected media is also the one against whose eavesdropping the system is trying to protect. The speedbump must block the user from doing unwanted things with the file, while permitting him or her to do the things for which he or she paid. While modern cryptography has solved many hard problems, it is helpless against the challenge of showing you something and simultaneously preventing you from seeing it.

Open source works beautifully for encryption because modern cryptosystems are built, following Kerkhoffs' Principle, on the maxim of least secrecy: disclose your algorithms, and secure your keys. Anyone can implement encryption compatible with Pretty Good Privacy (PGP), and decrypt a PGP-signed message in the open-source GNU Privacy Guard (GPG) so long as he has the private key to which it was encrypted. Users can independently verify (or have third parties verify for them) the security of their applications—and yet keep particular communications secured by the algorithms secret from anyone who does not know the private keys to that particular exchange. The threat model, as security researchers describe it, is the third party eavesdropper. Alice and Bob may communicate securely without Eve listening in. Even if Eve captures the communications stream, without the key, she sees only a stream of gibberish.

Asymmetric, or public key, encryption lets senders and recipients exchange encrypted messages without ever exchanging prior secrets. The recipient publishes a public key, half of a public-private key-pair, and guards the private key. The sender encrypts to the public key using public algorithms, and only the recipient in possession of the private key can decrypt the message. Even the eavesdropper, with all the other information about the message (algorithm and public key), can do nothing but try brute force attacks, which will fail if the parties have used a sufficiently long key-length.

This method works fine as an initial *access* control: only those who have the private key can read the messages sent to it, but it fails to assert any *use* controls after decryption, as DRM attempts. Yet when DRM systems use encryption for *use*-control, they are trying to secure communications against the same users to whom they're trying to sell media, all the

anticircumvention law tries to prevent this inevitability by bringing the heavy artillery of civil sanctions and criminal punishment to the battle between DRM-makers and DRM-breakers. It supports the DRM manipulation of the environment in which digital media can be played, constraining devices so that they can "contain" protected media. Copy protection can never regulate just the object itself—it must regulate the entire ecosystem to protect a work effectively. Thus, DRM technology entails a whole collection of subsidiary regulations to enforce it.[54]

### B. THE MECHANICS OF ANTICIRCUMVENTION LAW.

Anticircumvention law extends the control of copyright, providing a legal hook from which to hang additional *contractual* restrictions. U.S. entertainment industries pushed the World Intellectual Property Organization (WIPO) to mandate legal protection for technical protection measures in the WIPO Copyright Treaties, Article 11 Obligations Concerning Technological Measures.[55] To comply, Congress added Chapter 12 to the Copyright Act through the DMCA.[56]

Section 1201, the core anticircumvention provision, provides that copyright holders who put technological locks on their works can use the law's civil and criminal penalties[57] to block others from "circumventing"

---

while needing to give the user the use for which she has paid. It is as though the same person is both Bob, the intended recipient, and Eve the eavesdropper. DRM's solution is to hand the keys to Bob for viewing without giving them to Eve, his alter ego. We could forbid Bob from doing bad things with the keys, but that is what copyright law already does in forbidding infringement. So now there are two things the system must hide while making them usable: its key and the plaintext.

54. *See* Susan Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM. & ENT. L.J. 603, 629 (2003) (providing an extreme example of the environmental impact: once bitten by the DRM vampire, every other device connected to a broadcast-flagged DTV system would have been subject to regulatory control).

55. World Intellectual Property Organization Copyright Treaty, art. 11, Dec. 20, 1996, 112 Stat. 2860, 2186 U.N.T.S. 152.

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

*Id.*; *see also* LITMAN, *supra* note 32, at 134–45.

56. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, 2863 (1998). For more discussion of the DMCA's genesis, see *infra* Section III.A.

57. 17 U.S.C. §§ 1203–1204 (2006) set out the civil and criminal enforcement provisions.

those protections.[58] The law protects DRM technology with three prohibitions, forbidding anyone to "circumvent a technological measure that effectively controls access" to a copyright-protected work,[59] or to

> manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[60]

A parallel anti-trafficking provision prohibits tools for circumvention of *copy* controls, while the act of circumventing those controls—copying—is left to the prohibitions on ordinary infringement.[61]

The technological prerequisites for legal protection are minimal. "[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[62]

Critical to the functioning of the anticircumvention hook, "authority of the copyright holder" can be granted conditionally.[63] While early critics argued that access control should be binary—that once "access" had been authorized, further uses were no longer within the realm of the DMCA but subject only to ordinary tests of infringement[64]—the courts have not agreed. Rather than determining that authority to access was granted

---

58. 17 U.S.C. § 1201(a)(3)(A) ("[T]o 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner . . . .").

59. 17 U.S.C. § 1201(a)(1)(A).

60. 17 U.S.C. § 1201(a)(2).

61. 17 U.S.C. §§ 501, 1201(b)(1) (2006).

62. 17 U.S.C. § 1201(a)(3)(B).

63. *See* MARKS & TURNBULL, *supra* note 8, at 10.

64. *See, e.g.*, Letter from Copyright's Commons to David O. Carson, Esq., General Counsel (Mar. 31, 2000), *available at* http://www.copyright.gov/1201/comments/reply/109selzer_bcis.pdf (giving reply comments in anticircumvention rulemaking).

straightforwardly through purchase of a DVD, the Second Circuit found it instead to be acquired only with a licensed DVD player, and only for licensor-approved uses.[65] With such an option, the copyright holder can then condition access on adherence to terms that are well beyond copyright, such as the region coding requirements in the DVD-CCA license, limitations on features or interconnections, and robustness rules.[66] Anticircumvention transforms weak technical measures into strong use controls, limiting technological possibility.

A copyright holder's adoption of a technological measure fortifies these works against access without the "authority" of the copyright holder; it also protects officially sanctioned playback devices against unauthorized competition or tinkering.[67] Even a weak scrambling scheme imports the full panoply of anticircumvention rights. Interoperation with a scrambled work against the "authority" of the copyright holder becomes a violation of the law, even if none of the aims of interoperation or intended uses of the product is an infringement of traditional copyright.

In short, before § 1201, someone who wanted to build a multimedia player for a newly acquired work would be legally free to do so,[68] perhaps improving the player options along the way. Under an anticircumvention regime, however, if any "technological measure" has been applied to the works, developers must seek permission to lawfully build a player or modify an existing one.[69] Section 1201(f), which permits some acts of circumvention for "reverse engineering,"[70] has not been useful as a shield for independent development of media technology.[71]

As described above, the DMCA protection on DVDs helps explain the lag in video playback options compared to their music-player counterparts. Other legal cases illustrate the comparative leeway pre-DMCA copyright gave

---

65. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317 n.137 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 73 F.3d 429, 443 n.13 (2d Cir. 2001).

66. *See* Prepared Testimony of Gwen Hinze, Staff Attorney, Elec. Frontier Found., May 15, 2003, http://w2.eff.org/IP/DMCA/copyrightoffice/20030515_region_dvd.php.

67. *See* 17 U.S.C. §§ 1201(a)(1), 1201(b).

68. This assumes the only IP rights available are copyright restrictions. Patents, such as those claimed on MP3 encoding, may serve as a separate impediment.

69. *See* 17 U.S.C. § 1201.

70. *See* § 1201(f).

71. *See* Universal v. Reimerdes, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000) ("[T]he legislative history makes it abundantly clear that Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works, such as movies."); *see also* Davidson & Assocs. v. Jung, 422 F.3d 630, 642 (8th Cir. 2005).

to reverse engineering and investigation. For example, when Sony tried to use copyright to monopolize its PlayStation platform, for which it manufactured the game consoles and licensed games, the Ninth Circuit rejected Sony's claims against the interoperable "Virtual Game Station."[72]

> The district court found that "[t]o the extent that such a substitution [of Connectix's Virtual Game Station for Sony PlayStation console] occurs, Sony will lose console sales and profits." We recognize that this may be so. But because the Virtual Game Station is transformative, and does not merely supplant the PlayStation console, the Virtual Game Station is a legitimate competitor in the market for platforms on which Sony and Sony-licensed games can be played. For this reason, some economic loss by Sony as a result of this competition does not compel a finding of no fair use. Sony understandably seeks control over the market for devices that play games Sony produces or licenses. The copyright law, however, does not confer such a monopoly.[73]

The Ninth Circuit similarly rejected Sega's copyright attempt to lock the converse market, for games to run on its proprietary consoles: "[A]n attempt to monopolize the market by making it impossible for others to compete runs counter to the statutory purpose of promoting creative expression and cannot constitute a strong equitable basis for resisting the invocation of the fair use doctrine."[74]

Anticircumvention gives Sony and Sega a power copyright alone did not. As Dean Marks and Bruce Turnbull describe, anticircumvention laws supporting technical protection measures serve as the binding agent between technological controls and multi-party licensing agreements governing the

---

72. Sony Computer Entm't v. Connectrix Corp., 203 F.3d 596, 606–07 (9th Cir. 2000).

> We find that Connectix's Virtual Game Station is modestly transformative. The product creates a new platform, the personal computer, on which consumers can play games designed for the Sony PlayStation. This innovation affords opportunities for game play in new environments, specifically anywhere a Sony PlayStation console and television are not available, but a computer with a CD-ROM drive is. More important, the Virtual Game Station itself is a wholly new product, notwithstanding the similarity of uses and functions between the Sony PlayStation and the Virtual Game Station. . . . Connectix reverse-engineered the Sony BIOS to produce a product that would be compatible with games designed for the Sony PlayStation. We have recognized this purpose as a legitimate one.

*Id.*

73. *Id.*

74. Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1523–24 (9th Cir. 1992).

use and limitations of media subject to those controls.[75] Only those who promise to obey various non-copyright conditions may be granted authority.[76]

Though nothing in the text of the law speaks specifically to modes of development, that does not mean that the law has no hand in it. Under majority interpretation, anticircumvention prohibits user modification of players (hardware or software) used to play copyrighted works that have had any technical protection.[77] Tinkering with a device would seemingly void the "authorization" conveyed by the player license. The prohibition on open development more generally comes from a common feature of the license agreements through which DRM platforms are created: "robustness rules" and their implementation.

### C. LICENSING FOR ROBUSTNESS: HOW CONTENT PRODUCERS EXERT INFLUENCE IN THE HARDWARE MARKET

If one can access DRM-encumbered works only with the "authority of the copyright owner,"[78] then the licenses on which that authority is conditioned become the public law for those works. Those licenses enforce terms on the playback-device maker, and through them, upon the end-user for the copyrighted works.

While their particular usage terms may vary, DRM system licenses follow a common structural pattern. They require protection of the content with "usage rules" to be passed through to the end-user, and protection of the DRM system itself, with internal "compliance" and "robustness" rules.[79] If you are going to impose technical protection measures, it is because you distrust your users and want to stop them, through technology, from doing things that would otherwise be possible. As your understanding of users' abilities and interests improves, you try to fill the cracks in your technical protections. In the logic of DRM designers, this condition makes sense: if

---

75. MARKS & TURNBULL, *supra* note 8, at 10–15.

76. *Id.*

77. *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); RealNetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913 (N.D. Cal. 2009); 321 Studios v MGM Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004).

78. 17 U.S.C. § 1201(a)(3)(A) (2006).

79. "Compliance" rules regulate the licensee devices' adherence to the usage rules, while "robustness" requires efforts to withstand modifications. *See, e.g.*, Advanced Access Content System Adopter Agreement F-1 (June 9, 2009), http://www.aacsla.com/license/AACS_Adopter_Agrmt_090619.pdf; DVD-CCA CSS Procedural Specification ¶ 6.2.6, http://cyber.law.harvard.edu/seminar/internet-client/readings/week2/02-08CSS.pdf; Microsoft Corp., Compliance and Robustness Rules for Windows DRM, http://wmlicense.smdisp.net/wmdrmcompliance/ (last visited Mar. 25, 2010).

anticircumvention is to stop copying, the anti-copying system must be as resistant to hacking as the encryption itself. After all, a chain is only as strong as its weakest link, and a speedbump will not slow traffic if it is easy to avoid at full speed. And so § 1201 entails hardening of playback technology even if the law itself does not directly require it.

A review of license agreements for various content protection systems finds nearly identical robustness rules across the board.[80] The hardware or software implementations of media playback or transport must be designed to "effectively frustrate"[81] or "resist attempts to modify such products so as to defeat"[82] the content-protections: they must not include in the protected path any user-modifiable components such as switches, buttons, jumpers, or traces that may be cut; they must not be accessible to a debugger; and they must "keep secrets." In short, to be authorized to access a work, an implementation must be hardened against tinkering and user exploration.[83]

The robustness rules are design rules.[84] They shape the architecture of the systems licensees are permitted to make available to end users. As Tarleton Gillespie describes it, these rules restructure the relationship of the user not only with the media, but also with the technology itself. They set the user up as a passive consumer, rather than an active participant in creating both

80. *See* sources cited *supra* note 79; *see also* Tarleton L. Gillespie, *Designed to 'Effectively Frustrate': Copyright, Technology, and the Agency of User*s, 8 NEW MEDIA & SOC'Y 651, 651–69 (2006).

81. Advanced Access Content System Interim Content Participant Agreement, Exhibit C, Part 2, § 3.2, *available at* http://www.aacsla.com/license/AACS_Interim_Content_Participant_Agrmt_090605.pdf ("Licensed Products shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Licensed Products or the performance of such Licensed Products to defeat the Content Protection Requirements."). Even Sun's DrEAM, the purportedly open DRM specification, mandates robustness on its clients: "Client security: the implementation of a robust client that will be required for a viable solution. The implementation of the robust client will depend on the hardware and software support available." DReaM-CAS Client Specification Version 1.0 Rev A, Technical Specification, § 1.1 (2007) (on file with author).

82. Microsoft, Microsoft Windows Media 10 SDK Robustness Rules, http://wmlicense.smdisp.net/wmdrmcompliance/ (click on "Robustness Rules for WMDRM10 Devices") (last visited Mar. 20, 2010) ("Licensed Products as shipped . . . must be designed and manufactured so as to resist attempts to modify such products so as to defeat the functions of the Microsoft Implementation.").

83. *See* TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 225–29 (2007).

84. *See* CARLISS Y. BALDWIN & KIM B. CLARK, DESIGN RULES, VOL. 1: THE POWER OF MODULARITY 80 (2000) (describing design rules as a set of constraints on manufacture).

culture and technology.[85] As Lawrence Lessig puts it, the rules move us from a "Read/Write" to a "Read/Only" culture.[86]

Section 1201's authority requirement imports the terms imposed by contractual licenses. When all the licenses for major DRM systems require robustness as a condition, robustness becomes the equivalent to a direct legal requirement. Private law is transmuted into public. As scholars such as Lessig have pointed out, however, this private law can be both equally constraining and more opaque for its indirection.[87]

Indeed, the robustness mechanism could have been written into public law. In the Broadcast Flag Rules, regulations adopted by the FCC for the protection of digital television transmissions, robustness was mandated in the Rule.[88] So written, it could be challenged in court. The American Library Association and other public interest groups did just that, and successfully argued that the Broadcast Flag Rule exceeded the FCC's authority.[89] Challenges to DMCA-backed DRM should get the same hearing.

---

85. GILLESPIE, *supra* note 83, at 226–27.

86. LAWRENCE LESSIG, REMIX 28 (2008).

87. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 95–98, 223–25 (2000); *see also* GILLESPIE, *supra* note 83, at 219 (describing "technically imposed copyright protections that depend on encrypted content, technologies that abide by a set of rules applied to that content, and laws making it illegal to tamper with or produce alternatives to those technologies").

88. *See* Robustness Requirements for Covered Demodulator Products, 47 C.F.R. § 73.9007 (2005) ("The content protection requirements set forth in the demodulator compliance requirements shall be implemented in a reasonable method so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment.") Even "generally available" is defined in the regulation:

> Generally-available tools or equipment means tools or equipment that are widely available at a reasonable price, including but not limited to, screwdrivers, jumpers, clips and soldering irons. Generally-available tools or equipment also means specialized electronic tools or software tools that are widely available at a reasonable price, other than devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this subpart. Such specialized electronic tools or software tools includes, but is not limited to, EEPROM readers and writers, debuggers or decompilers.

*Id.* at note.

89. *See* Am. Library Ass'n v. Fed. Commc'n Comm'n, 401 F.3d 489 (D.C. Cir. 2005).

### D. OPEN SOURCE SOFTWARE IS INCOMPATIBLE WITH ROBUSTNESS REQUIREMENTS

In sharp contrast to the constrained environment of the DMCA, free and open source software invites end-user modification.[90] By disclosing its details and granting users permission to modify (in copyright terms, to create derivative works), free and open source software both opens the car's hood and provides a schematic diagram (more or less well labeled) of the mechanical components. Even relative novices can learn their way around by tweaking a few lines and recompiling to see the effect—much as one learning web design can "view source" on a webpage and learn by imitation and adaptation. Experts can refine the software to their needs, both fixing bugs and adding features. User communities formed around free and open source software have developed complex applications, operating systems, and environments.[91] Free and open source software powers much of the Internet's infrastructure. More than half of Internet webservers run the open -source Apache web server,[92] often on the free GNU/Linux operating system, and many of their visitors now use open-source browsers such as Mozilla Firefox or Google Chrome. Even someone who never reads a line of source code benefits from openness: from the competition of independent programmers available to service the software, from the pressure it puts on proprietary vendors, and from the ease of developing complementary applications.

Free and open source software development depends critically on openness. While the terms "free software" and "open source" reflect different emphases and motivations of their participants,[93] at heart, both refer to software whose source code (the human-readable version of the computer

90. "Free software" tends to be the label of choice for those who, following the Free Software Foundation, give an explicitly political dimension to the sharing of source code and the freedom to modify software; "open source" is often used pragmatically to emphasize the economic and efficiency benefits of disclosed source. Whether by philosophic or economic temperament, their mode of development has the effect of making software features much more accessible to user innovation.

91. Karim R. Lakhani & Eric von Hippel, *How Open Source Software Works: "Free" User-to-user Assistance*, 32 RES. POL'Y 923, 924 (2003).

92. *See* Netcraft, Web Server Survey Archives, http://news.netcraft.com/archives/web_server_survey.html (last visited Mar. 20, 2010).

93. *See* Wendy Seltzer, *Why Open Source Needs Copyright Politics*, *in* OPEN SOURCES 2.0: THE CONTINUING EVOLUTION 149, 149 (DiBona et al. eds. 2005); Yochai Benkler, *The Battle over the Institutional Ecosystem in the Digital Environment*, 44 COMM. ASS'N COMPUTING MACHINERY 84, 84 (2001).

instructions) is made available to the programs' users for use and modification.[94]

The Free Software Foundation expresses the core principles of Free Software as "four essential freedoms":

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this.[95]

All four of these components are necessary to give users full autonomy in their software environment; to use and learn from the program and to modify it to suit their needs. They guard against lock-in to an uncooperative vendor or defunct system, and assure that users will be able to reuse their individual investments in the program. Moreover, the Free Software Foundation asserts, "Freedom 1 [the freedom to modify] must be practical, not just theoretical; i.e., no tivoization."[96] Version 3 of the GPL, issued in 2007,[97] requires licensees to provide with a program "installation information" sufficient to allow the use of modified code in the same manner as the originally installed program.[98] "Look but don't touch" is not freedom.

---

94. *See* Free Software Foundation, The Free Software Definition, http://www.gnu.org/philosophy/free-sw.html (last visited Mar. 5, 2010); Open Source Initiative, The Open Source Definition (Annotated) http://www.opensource.org/docs/definition.php (last visited Mar. 5, 2010).

95. Free Software Foundation, *supra* note 94.

96. *Id.* (referring to the TiVo digital video recorder, which runs a GNU/Linux operating system and makes source available, but does not permit the user to install modifications on the TiVo box).

97. Developers of code can choose which license to apply, subject to any requirements they inherit from upstream code they wish to use under license. The Linux kernel remains under GPLv2, while new versions of the FSF's GNU utilities are released under GPLv3. Those who wish to distribute the newest GNU utilities, therefore, are required to make both source and installation information available.

98. Free Software Foundation, GNU General Public License, Version 3 § 6 (2007),

The GNU General Public License (GPL) maintains these freedoms by a "copyleft" provision: anyone is free to reuse GPL-licensed code, so long as those who do release their derivative works on the same terms, under the GPL.[99]

The Open Source Initiative (OSI) is more explicitly oriented toward the "economic and strategic advantage" to be gained from openness.[100] It takes openness as a foundation for diversity and productive innovation. "We require access to un-obfuscated source code because you can't evolve programs without modifying them. Since our purpose is to make evolution easy, we require that modification be made easy."[101] The OSI aims to leverage the community of open source developers: "In order to get the maximum benefit from the process, the maximum diversity of persons and groups should be equally eligible to contribute to open sources. Therefore we

---

*available at* http://www.gnu.org/licenses/gpl.txt. The GPL states:

> If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information.
>
> "Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

*Id.*

99.

> [5] You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code . . . provided that you also meet all of these conditions:
>
> a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
>
> b) The work must carry prominent notices stating that it is released under this License . . . .
>
> c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy.
>
> [6] You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License. . . .

*Id.* §§ 5, 6.

100. Open Source Initiative, About the Open Source Initiative, http://www.opensource.org/about (last visited Mar. 5, 2010).

101. Open Source Initiative, *supra* note 94.

forbid any open-source license from locking anybody out of the process."[102] OSI identifies a number of licenses as "Open Source" compliant.[103] Like the GPL, which is among them, all Open Source-licensed distributions include the source code and ability to modify the software.[104]

It would be impossible to build a player for DRM-encumbered media that complied with either the Free Software or the Open Source definition. DRM is incompatible with both the letter and the spirit of open source and free software licenses.[105] Anticircumvention forbids users from exploring the possibilities of their media, and it forecloses developers from offering media players that can be user-modified.

The Internet multiplies the opportunities for open development, connecting the forces of plentiful open source software, a critical mass of networked potential contributors, and cheaper communications among them on a neutral platform. As Federal Communication Commission Chairman Julius Genachowski asked in the September 2009 speech launching the Commission's "open Internet" discussion: "Why has the Internet proved to be such a powerful engine for creativity, innovation, and economic growth? A big part of the answer traces back to one key decision by the Internet's original architects: to make the Internet an open system."[106]

---

102. *Id.*

103. *See* Open Source Initiative, Open Source Licenses by Category, http://www.opensource.org/licenses/category (last visited Mar. 5 2010).

104. The Open Source Definition does not require a copyleft-style provision mandating openness on downstream redistributors, although it is compatible with the GPL's copyleft requirement. *See* sources cited, *supra* note 94.

105. *See infra* Section V. In the 2007 revision of the GPL, the Free Software Foundation added a clause explicitly forbidding the use of GPL in technological protection measures. *See* GNU General Public License, *supra* note 98, § 3 ("No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 [*sic*] of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures."). This specific prohibition is distinct from the general incompatibility of DRM with the free and open source mode of development.

106. Julius Genachowski, Chairman, FCC, Remarks at The Brookings Institution: Preserving a Free and Open Internet: A Platform for Innovation, Opportunity, and Prosperity (Sept. 21, 2009), *available at* http://openinternet.gov/read-speech.html. Genachowski stated:

> The Internet's creators didn't want the network architecture—or any single entity—to pick winners and losers. Because it might pick the wrong ones. Instead, the Internet's open architecture pushes decision-making and intelligence to the edge of the network—to end users, to the cloud, to businesses of every size and in every sector of the economy, to creators and speakers across the country and around the globe. In the words of

## III. THE ACADEMIC DEBATE

### A. ANTICIRCUMVENTION'S ADVOCATES

Attempts to "copy protect" media have been around for a long time, but the rise of digital storage accelerated their move from technology to law. Digital media, copyright holders argued, allowed users to make perfect copies, while high-speed communications networks would allow them to share those copies easily.[107] Intellectual property industries proclaimed a "digital dilemma": there would be no cars to transit the digital information superhighway unless copyright law guaranteed protection for their copyrighted contents.[108] They sought this protection in both technology and law.

Publishing industries laid out a syllogism: "content" was key to the growth of the nascent Internet—then known as the National Information Infrastructure (NII); content production would halt if its protection could not be assured; therefore, content protection must be made a core part of the Internet.[109] The NII taskforce did not overestimate technology: "it is clear

---

> Tim Berners-Lee, the Internet is a "blank canvas"—allowing anyone to contribute and to innovate without permission.

*Id.*

107. *See, e.g.*, *NII Copyright Protection Act of 1995: Hearing on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 104th Cong. (1996) (statement of Barbara A. Munder, Information Industry Association); *see also NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the House Judiciary Comm. and the Senate Judiciary Comm.*, 104th Cong. (1995).

108. INFORMATION INFRASTRUCTURE TASKFORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 10–17 (1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.txt [hereinafter NII REPORT].

109. *Id.* at 10–11.

> [T]he full potential of the NII will not be realized if the education, information and entertainment products protected by intellectual property laws are not protected effectively when disseminated via the NII. Creators and other owners of intellectual property rights will not be willing to put their interests at risk if appropriate systems—both in the U.S. and internationally—are not in place to permit them to set and enforce the terms and conditions under which their works are made available in the NII environment. Likewise, the public will not use the services available on the NII and generate the market necessary for its success unless a wide variety of works are available under equitable and reasonable terms and conditions, and the integrity of those works is assured. All the computers, telephones, fax machines, scanners, cameras, keyboards, televisions, monitors, printers, switches, routers, wires, cables, networks and satellites in the world will not create a successful NII, if there is no content. What will drive the NII is the content moving through it.

that technology can be used to defeat any protection that technology may provide,"[110] but it drew from that the conclusion that law must be added to the mix, in support of technology-based restriction. The NII White Paper proposed the hybrid: legal prohibition on circumvention of technical measures.

> The Working Group finds that legal protection alone will not be adequate to provide incentive to authors to create and to disseminate works to the public. Similarly, technological protection likely will not be effective unless the law also provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works.
>
> The Working Group finds that prohibition of devices, products, components and services that defeat technological methods of preventing unauthorized use is in the public interest and furthers the Constitutional purpose of copyright laws. Consumers of copyrighted works pay for the acts of infringers; copyright owners have suggested that the price of legitimate copies of copyrighted works may be higher due to infringement losses suffered by copyright owners. The public will also have access to more copyrighted works via the NII if they are not vulnerable to the defeat of protection systems.
>
> Therefore, the Working Group recommends that the Copyright Act be amended to include a new Chapter 12, which would include a provision to prohibit the importation, manufacture or distribution of any device, product or component incorporated into a device or product, or the provision of any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights under Section 106. The provision will not eliminate the risk that protection systems will be defeated, but it will reduce it.[111]

From the White Paper, through the "policy laundering"[112] of treaty-making at WIPO, Chapter 12 was added to the Copyright Act in 1998.[113]

---

*Id.* That the NII taskforce could not have envisioned or explained Wikipedia, whose authors and editors contribute knowing that their works are shared freely—even so that others may profit—or the Creative Commons licenses many use to share their works is perhaps the first hint that theirs is not the only path to the Progress of Science.

110. *Id.* at 136.

111. *Id.* at 139–40.

112. Policy laundering takes an unpalatable policy argument from the domestic realm and "launders" it through an international treaty organization, WIPO, before bringing it back to the national legislature as "treaty obligation." *See* Ian Hosein, Paper Presented at the

Section 1201 of the DMCA prohibits "circumvention" of technological access-control measures, and prohibits trafficking in circumvention tools for access or copy controls.[114] It gives legal force to technological barriers, however weak or strong they may be, and forbids distribution of the tools of circumvention even when their intended aim is not copyright infringement.[115]

The anticircumvention provision has been controversial from its inception. Early critics questioned its constitutionality[116] and blamed it for expanding the rights of copyright holders at the expense of the public[117]; while proponents argued that it was necessary to keep the traditional rights of copyright holders viable in new markets.[118] By and large, these arguments have taken place *within copyright*, sharing copyright's focus on the production, use, and (perhaps) marketing of creative expression, which explains why they tend to miss anticircumvention's *outside-copyright* effects on technology development.

Technologists and academics supporting anticircumvention law said it would sustain copyright and an ecology of new business models around copyrighted works.[119] Mark Stefik first described a "trusted system" to envelop copyrighted works and control their transfer:

> The term *trusted system* refers to computers that can be relied on to do certain things. For example, suppose that a creator or publisher forbids all copying of a particular digital work. A trusted system in this context would reliably and infallibly carry out that stipulation; no amount of shouting or coaxing would coerce it to copy the work.[120]

Similarly, Jane Ginsburg acknowledges that anticircumvention provides new rights, but argues that the technological shift from possession of hard copies to "experiencing works" required more extensive grants.[121] To

---

International Studies Assocation, Montreal, Quebec, Canada: International Relations Theories and the Regulation of International Dataflows: Policy Laundering and other International Policy Dynamics 136 (Mar. 17, 2004).

113. WIPO Copyright to Performances and Phonograms Treaties Implementation Act of 1998, 17 Pub. L. No. 105-304, 112 Stat. 2860, 2863.

114. Digital Millennium Copyright Act, 17 U.S.C. § 1201 (2006).

115. *Id.*; *see also supra* Section II.B.

116. *See, e.g.*, Neil W. Netanel, *Locating Copyright Within the Fair Use in the First Amendment Skein*, 54 STAN. L. REV. 1, 78–80 (2001); *see also infra* Section III.B.

117. *See infra* Section III.B.

118. *Id.*

119. *See* Mark Stefik, *Trusted Systems*, SCI. AM., Mar. 1997, at 78–81.

120. Mark Stefik, *Letting Loose the Light: Igniting Commerce in Electronic Publication*, *in* INTERNET DREAMS: MYTHS, AND METAPHORS 249, 257 (Mark Stefik ed., 1996).

121. Jane Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access*

Ginsburg, anticircumvention law flows from the spirit of the Copyright Clause of the Constitution[122] as a natural response to changes in technology and the markets it supports, suggesting that "in the digital environment, the 'exclusive Right' that the Constitution authorizes Congress to secure to authors is not only a 'copy'-right, but an access right."[123] As copyright holders lost control in dissemination, they should get back a different lever of control.

## B. ANTICIRCUMVENTION'S CRITICS

### *1. Anticircumvention Stops End-User Fair Use*

Much of the previous anticircumvention scholarship has focused on the direct constraints DRM places on media usage and the constrictions that places on fair use.[124] When media is available only through DRM-respecting applications, users are forced to accept the usage limitations even if those limitations are more restrictive than those of copyright. A user buying a song tethered to the computer on which she downloaded it can never resell that purchase.[125] A film critic seeking to display a clip from DVD cannot easily take an excerpt for this purpose.[126]

For some, this tradeoff is the cost of access to digital copies. With finer-grained permissions comes a more tailored set of costs—price discrimination that gives users access to lower cost and more abundant copies.[127] For others, the tradeoff is too great, damaging the important public benefits of fair use: privacy in reading,[128] freedom from asking permission in advance, and freedom to criticize.[129] The positive externalities of fairly-used media, for

---

*Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC. 113, 115 (2003).

122. U.S. CONST. art. 1, § 8, cl. 8.

123. Ginsburg, *supra* note 121, at 115.

124. *See, e.g.*, sources cited *supra* note 39.

125. *See* LITMAN, *supra* note 32, at 83 ("Augmenting copyright law with legally enforceable access control could completely annul the first sale doctrine."); *see also* 17 U.S.C. § 109 (2006) (first sale doctrine).

126. See the petitions for exemptions in the Copyright Office's triennial rulemaking under 17 U.S.C. § 1201(a)(1)(C), U.S. Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, *available at* http://www.copyright.gov/1201/.

127. *See* Tom Bell, *Fair Use Vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 588(1998); 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, 296 (2003).

128. Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1007–10 (1995).

129. *See* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 410 (1999); Netanel, *supra* note 116, at

example, mean the law should be willing to subsidize it rather than restrict it. Cutting off fair use diminishes the commons on which future creativity depends.[130]

Academic critics attacked anticircumvention first from within copyright: technological protections interfere with the fair use limitations built into copyright law.[131] While some unauthorized use of copyrighted works is legally non-infringing, DRM has no way to recognize the difference between a fair reproduction for classroom use, commentary, or parody, and an infringing reproduction. The statute prohibits DRM's circumvention even when the protection blocks access for non-infringing uses.[132]

Pamela Samuelson, Jessica Litman, Julie Cohen, and Yochai Benkler have all highlighted the inconsistency between technological enforcement of absolutes and the nuanced case-by-case and use-by-use exceptions fair use grants to copyright's "exclusive" rights.[133] Some, including the author of this Article, have argued that this incompatibility renders the DMCA unconstitutional, because its making absolute of copyright-style rights, "paracopyright," in David Nimmer's terms, violates the First Amendment.[134]

A number of these arguments have been raised in constitutional challenges to the DMCA,[135] but as these challenges appeared to defend conduct that could also enable mass reproduction, assertions of fair use harms fell on deaf ears. For example, the Second Circuit told the *Universal v.*

---

26.

130. LAWRENCE LESSIG, FREE CULTURE: THE NATURE AND FEATURE OF CREATIVITY 97–99 (2005); PATRICIA AUFTERHEIDE & PETER JASZI, UNTOLD STORIES: CREATIVE CONSEQUENCES OF THE RIGHTS CLEARANCE CULTURE FOR DOCUMENTARY FILMMAKERS (2004), *available at* http://www.centerforsocialmedia.org/files/pdf/UNTOLDSTORIES_Report.pdf.

131. Copyright does not prohibit *all* reproductions, only those that interfere with the copyright holder's rights. Reproductions "for purposes such as criticism, comment, news reporting, [and] teaching" are permitted as fair use. 17 U.S.C. § 107 (2006).

132. *See* Samuelson, *supra* note 39, at 524 ("[T]here are far more legitimate reasons to circumvent a technical protection system than the DMCA's act-of-circumvention provision expressly recognizes.").

133. *See generally* Benkler, *supra* note 129; Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998); Cohen, *supra* note 128; LITMAN, *supra* note 32; Samuelson, *supra* note 39.

134. Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Plaintiff's Opposition to Defendant's Motion for Partial Summary Judgment at 321 Studios v. Metro Goldwyn Mayer Studios Inc., 307 F.Supp.2d 1085 (N.D. Cal. 2004) (No. C 02-1955 SI); DAVID NIMMER, 3 NIMMER ON COPYRIGHT § 12A.15[C] (1999 supp.); Netanel, *supra* note 116, at 78.

135. *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); *321 Studios*, 307 F. Supp. 2d 1085.

*Corley* defendants that would-be fair users of DVD video could point camcorders at their television screens.[136]

A second round of fair use-inspired critics has asked whether technology can help solve the problems technology has created: can fair use be accommodated within "hybrid" DRM systems? While we cannot put a judge on a chip, some have proposed that we can approach the pre-DMCA regime (and public good) more effectively by pairing more generous defaults with systems built to accommodate a call-out to an external authority or trusted third party. Julie Cohen and Dan Burk note the law's shortcomings in the cultural realm, but wonder whether that is a mere function of implementation.[137] Could a "fair use infrastructure" for rights management systems, a trusted third party who could adjudicate requests for access to make fair use, capture the nuance and spontaneity of fair use abilities? Burk and Cohen endeavor to design a "second-best solution designed to make the best of a bad situation," but ultimately reject even their modified DRM.[138] Tim Armstrong proposes a system that sets the defaults toward use, while keeping an audit trail of asserted fair uses.[139] Deirdre Mulligan and John Erickson describe the possible use of rights expression languages, rather than automated restrictions.[140]

The fair use strain of scholarship often comes down to a cost–benefit analysis within copyright: does DRM increase expression and artistic creation, by providing greater security in the chance to profit from that work, and does that benefit outweigh the cost in the expressive opportunities of audiences and follow-on creators? In the decade since the DMCA's enactment, evidence on the harm side of the balance sheet has mounted.[141] Moreover, while proposals for technical recognition of fair use go some distance toward mitigating one of the problems with DRM and anticircumvention, they create a new set of problems. By mandating that developers of technology harden their devices or software, they force the deployment of user-resistant technology and methods capable of being hardened before distribution to end-users.

---

136. *Corley*, 273 F.3d at 459.

137. Burk & Cohen, *supra* note 41, at 50–51.

138. *Id.* at 80.

139. Armstrong, *supra* note 43, at 99–108.

140. Erickson & Mulligan, *supra* note 41, at 994.

141. *See generally* Deirdre K. Mulligan, John Han & Aaron J. Burstein, *How DRM-based Content Delivery Systems Disrupt Expectations of "Personal Use," in* DIGITAL RIGHTS MANAGEMENT WORKSHOP 77 (Moti Yung ed., 2003); FRED VON LOHMANN, UNINTENDED CONSEQUENCES: TEN YEARS UNDER THE DMCA (2010), http://www.eff.org/wp/unintended-consequences-ten-years-under-dmca/.

*2. DRM Does Not Stop Copying*

Along with the fair use criticisms,[142] analysts have added another concern in the copyright sphere: DRM does not in fact stop copying. Even if the technical restrictions are defended as "speedbumps," to "keep honest people honest,"[143] even honest drivers can take simple detours to avoid the bump. As Peter Biddle and colleagues explained in the "Darknet" hypothesis, it takes only one user to break copy protection and make content available on peer-to-peer networks; all subsequent users need merely to find that copy.[144] Ironically, finding illegal copies on the internet remains simpler than programming a VCR, despite entertainment industry attempts to crack down on the practice. DMCA notwithstanding, popular new movies and music tracks are available DRM-free from file sharing networks or download sites almost as soon as they are released in DRM-encumbered form.[145] Reviewing this evidence of *increased* copying, Fred von Lohmann concludes that "the DMCA has thus far failed to deliver under its policy rationale."[146] Von Lohmann suggests that on its own terms, as a measure to stop mass digital distribution of copyrighted works, anticircumvention-backed DRM has failed, instead causing end-users to seek out the unauthorized copies that are more functional than the DRM-saddled licensed versions.[147]

The upshot is that copyright holders are getting little of the copyright benefit they claimed—DRM is not reducing infringing reproduction—while adding hurdles to lawful but perhaps unwanted or unanticipated uses of their works.[148] A few industry players have managed to turn the momentum toward more open offerings, but most continue to use the weaknesses of

142. *See supra* Section III.B.1.

143. *See Piracy Prevention and the Broadcast Flag: Hearing Before the Subcommittee on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 108th Cong. 45–49(2003) (statement of Fritz Attaway, Exec. Vice President, Gov't Relations & Wash. Gen. Counsel, Motion Picture Ass'n Am.); BBC News, Digital Film: Industry answers, http://news.bbc.co.uk/2/hi/entertainment/4691232.stm#7/ (last visited Mar. 20, 2010).

144. Peter Biddle et al., *The Darknet and the Future of Content Distribution*, *in* DIGITAL RIGHTS MANAGEMENT WORKSHOP 155, 156 (Joan Feigenbaum ed., 2002).

145. *See* Douglas Wolk, *Days of the Leak*, SPIN MAGAZINE, Aug. 2007, at 86–88. (describing how albums are often leaked to the public on file sharing services before official release).

146. Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 640 (2004).

147. *Id.* at 642–43.

148. This Article does not defend copyright infringement. Rather, it concludes that the cost of technological measures against infringement is too high, and that there is no way of drawing a less costly technical barrier.

existing DRM systems as an excuse to ramp up the "protections" even further.[149]

*3. Anticircumvention Hinders Technology Innovation*

If DRM does not stop copying, then, what does it do? Both critics and proponents have recognized it as a method of technological control that continues to function, through the mechanism of anticircumvention, despite its weakness against piracy.

Fair use and use without permission are not the only casualties of DRM. A second branch of scholarship has focused on anticircumvention's impact on scientific inquiry and innovation in product design. Pamela Samuelson decried the impact on science, since the opacity of the DMCA's research exemptions, the difficulty of obtaining permission to research, and the need for clarification of the right to do so without permission chill investigation into computer security.[150] Ed Felten became an active critic of anticircumvention after a computer science research paper garnered DMCA threats.[151] Fred von Lohmann chronicled the "unintended consequences" of anticircumvention law, particularly in dampening the opportunities to innovate in the complementary markets *around* copyrighted works.[152]

These criticisms broaden the inquiry beyond fair use. Even if DRM furthered copyright's purpose, promoting creative authorship, extra-copyright effects add to the cost side of the equation. These cross-domain comparisons add the challenge of even greater incommensurability, forcing policymakers (if they want to make a fully informed decision) to compare the value of a new playback technology to that of a new creative work.

Anticircumvention changes the market structure around copyrightable expression, giving the creator of a *work of authorship*—or, more often, a group of copyright holders—the right and ability to control the market for *playback technologies*. It lets copyright holders leverage their statutory monopoly on

149. In some realms, DRM use is now diminishing, most notably through Apple's recent change of track to offer DRM-free sales from the iTunes Music Store. This shift came from Apple, not the music labels, once Apple had achieved sufficient dominance in the music market to maintain its technological hold without the DRM lock. *See* Steve Jobs, Thoughts on Music, http://www.apple.com/hotnews/thoughtsonmusic/ (last visited Feb. 22, 2010).

150. Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 SCIENCE 2028, 2028–29 (2001).

151. *See* Edward W. Felten, *DRM and Public Policy*, 48 COMM. ASS'N COMPUTER MACHINERY 112 (2005); *see infra* Section IV.B.

152. *See* VON LOHMANN, *supra* note 141, at 1; Fred von Lohmann, *Fair Use as Innovation Policy*, 23 BERKLEY TECH. L.J. 829, 851–53 (2008).

expression into technology.[153] Tim Wu finds that DRM's market structure holds back innovation. Giving copyright holders too much control over dissemination of their works and communications denies opportunities to a more widely distributed pool of potential innovators.[154] On a probabilistic analysis, having fewer potential innovation opportunities lowers the chances of successful innovation.[155]

Not all those who look at copyright and innovation oppose this extension of control. Randall Picker argues that technological tying can add market opportunities. By giving creators a broader scope in which to exploit their monopolies, he suggests tying can facilitate price and product differentiation.[156] Picker argues that between the increased incentives for the creators of copyrighted works and the decreased opportunities for "distributional" entry, on balance, DRM does more good than harm.[157]

More scholars, however, question the DMCA's impact on market structures. Anticircumvention's control presumes either that the successful creator is in the best position to design or recognize playback technologies or that these technology markets matter less than the creator's incentive.[158] This technological copyright control exacts a high price, however, given the multi-purpose nature of many playback technologies, and the "long tail" and communicative aspects of media,[159] many of whose most important applications relate to personal uses and freedoms, not mass market content.

153. *See* WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS 165 (2009) ("One of the new rights in the DMCA granted the motion picture studios the power to dictate the functional design of consumer electronic devices.").

154. *See* Timothy Wu, *Copyright's Communications Policy*, 103 MICH. L. REV. 278, 331–32 (2004); Tim Wu, *Intellectual Property, Innovation, and Decentralized Decisions*, 92 VA. L. REV. 123, 141–46 (2006).

155. *See* ARNOLD KLING & NICK SCHULZ, FROM POVERTY TO PROSPERITY 8 (2009) ("Often, innovation is the result of the unplanned trial-and-error learning that takes place among new enterprises, rather than the organized research and development efforts of large organizations.").

156. Picker, *supra* note 40, at 181.

157. *Id.*

158. *Cf.* DAN L. BURK & MARK A. LEMLEY, THE PATENT CRISIS AND HOW THE COURTS CAN SOLVE IT 73–74 (2009) (discussing cumulative innovation in patent improvements).

159. *See generally* CHRIS ANDERSON, THE LONG TAIL (2006); Andrew M. Odlyzko, *Content Is Not King*, FIRST MONDAY (Feb. 5, 2001), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/833/742/.

## IV. ANTICIRCUMVENTION'S APPLICATION

Law-backed technical protection measures throw a wrench into the mix of ever more user-accessible technologies and greater "generative" power in the hands of individuals and small-scale entrepreneurs.[160] By confining tinkering, experimentation, and exploration to those authorized by copyright holders, the law chokes off much of the potential of user-created technological improvements.[161] The examples of music and movie copy controls demonstrate the impact of anticircumvention on innovation and research, while that of Adobe PDF suggests that similar anti-infringement goals could be served less intrusively with advisory rather than mandatory features.

### A. CD VERSUS DVD: THE EFFECT OF A LOCKED-DOWN MEDIA FORMAT

This Article contrasted music's vibrant development environment and the range of music-capable devices against the limits around recorded movies, *supra* Part I. The DMCA explains this comparative poverty: in contrast to the CD, which, to preserve compatibility with legacy equipment has remained a vector for unencrypted, unprotected content,[162] the DVD was born encrypted. Since that encryption triggers the anticircumvention protections of the DMCA, no one may decrypt "without authorization" or build players to do so.[163] In order to play back a commercially recorded DVD movie, the player requires multiple keys: player, disc, and title.[164] Player keys

160. *See supra* Section II.D.

161. *See infra* Part V (discussing the benefits of user-created technological improvements).

162. Vendors have tried to deploy "copy-protected" CDs, by pushing the CD format's specification in attempts to foil copying but not playback as Macrovision did for VHS, e.g. by introducing bogus tracks that a player will pass over but a copier will hang trying to correct. *See Low-Tech Pen Foils CD Copy-Protection Device*, L.A. TIMES, May 21, 2002, at C1. The multitude of unprotected CDs keeps player manufacturers on the right side of the anti-trafficking provisions of 17 U.S.C. § 1201(a)(2)(B) (2006), however, if they develop better anti-skip mechanisms for copying.

163. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001); *see also infra* Section IV.A.

164. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2001).

> One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license.

(which give access to the other keys on the disc) are distributed only in players licensed by the DVD consortium (DVD CCA). Thus, the terms on which the consortium is willing to license players—including required limitations on outputs, restrictions on copying, and geographically-limited playback enforced by region coding—set a ceiling on *all* players' capabilities, while the requirement of authorization prevents independent development without permission.[165] Hence the public's options for movie playback and manipulation are significantly poorer than those for music.[166]

Under the threat that movie studios would withhold their content from insufficiently secure devices, consumer electronics companies and software makers negotiated protections through a cross-industry consortium with movie studios. They had competing interests in places: the studios wanting strong protection for their movies, the consumer electronics and software wanting something achievable in hardware and software, respectively, at commercially feasible cost under the manufacturing constraints of the early '90s. Their discussions produced the Content Scramble System (CSS)—a combination of disc and player keys and a scrambling system that relied upon both to decrypt the contents of the movie on disc. "What CSS does," explains Tarleton Gillespie, "is prevent consumers from watching the DVD using the wrong device—that is, one that hasn't been certified by the movie studios."[167]

As important as the technological scrambling were the conditions of authorization in the licenses required to de-scramble. The scrambling, no matter how weak, serves as the hook for a collection of usage rules and limitations: stay within the bounds of the license agreement and you could be authorized to descramble; or proceed without a license or exceed its authorization and it will be deemed a circumvention.[168] Only those licensed

---

*Id.*

165. *See infra* Part V.

166. The difference between options available for pre-recorded music and movies is not merely one of consumer preference. While we may enjoy video differently from music, the market reflects significant innovation around modes of video delivery other than pre-recorded movies, both the creation and hosting of short video, and the manipulation and time- and space-shifting of television broadcasts, which are sent unencrypted—from the early disrupter Betamax, through TiVo and Slingbox. Ultimately, non-movie video may grow large enough to fuel its own ecosystem, putting pressure on that of pre-recorded movies, but not yet.

167. *See* GILLESPIE, *supra* note 83, at 171 (2007) ("Control of copying and redistribution is imposed by ensuring that authorized DVD players themselves do not allow copying; CSS ensures that consumers will only use these authorized machines.").

168. MARKS & TURNBULL, *supra* note 8. One might ask whether patent already does this work, making anticircumvention superfluous. Namely, DVD playback also implicates

by the consortium can decrypt; and once hooked, only to do a limited set of activities: playback, on a region-matched playback device, without permitting copying or the skipping of promotional content. And do so "robustly," with prohibitions on end-user reverse engineering.[169]

These conditions were ineffective to prevent CSS from being broken. In late 1999, programmers analyzed the CSS scheme and produced DeCSS, a computer program capable of decrypting the scrambled contents of a DVD.[170] Jon Johansen, a fifteen-year-old Norwegian on the team who posted the code to his website, stated that he did so to enable people to play DVDs on Linux, as no available player at the time ran on that platform.[171] *2600 Magazine* took the DeCSS code and posted it to their website.[172] They were forced to remove and then link to the code after receiving a takedown notice. Despite arguments about the communicative power of code, the courts found this posting to be a provision of circumvention tools, in violation of §§ 1201(a)(2) and (b)(1).[173]

The court never distinguished carefully between access and copying, finding that DeCSS circumvented both types of controls. Moreover the court only cursorily analyzed the question of authorization. Since descrambling or decrypting amounts to circumvention only when conducted "without the authority of the copyright owner,"[174] we need an account of "authority" to distinguish between the legitimacy of the DVD player that decrypts CSS and the circumvention of DeCSS through substantially the same mathematical

---

numerous patents, licensed by the DVD-CCA pool. *See* Letter, *supra* note 11. Patent seems to exert less of a chill on independent research and innovation. *See* Mark A. Lemley, *Ignoring Patents*, 2008 MICH. ST. L. REV. 19 (2008). MP3 is claimed by Fraunhoffer yet widely implemented without license. Because it is not legally bound to the usage rules, the patent hook sinks less deep.

169. *See Reimerdes*, 111 F. Supp. 2d at 310.

170. *Id.* at 311.

171. While the *Reimerdes* court finds that "[a]t the time of trial [early 2000], licenses had been issued to numerous hardware and software manufacturers, including two companies that plan to release DVD players for computers running the Linux operating system," *id.* at 310, no commercially available DVD player was available for Linux at that time. *See id.* at 337 n.243. As late as 2004, companies were still heralding the "First Linux DVD Player," years after DVD playback was possible in Windows or Mac (the Xing player implicated in the CSS break was released in 1998). *Xing's Premier Software-Only DVD Player Provides Most Complete, Highest-Quality Solution for Multimedia PCs*, BUS. WIRE, Sep. 8, 1998, *available at* http://findarticles.com/p/articles/mi_m0EIN/is_1998_Sept_8/ai_50290471/. Of course the offering of any Linux player already depends on a different threat model, since in an open source environment, the player can even less effectively secure against capture of the decrypted data between the player and the content's human viewer.

172. *Reimerdes*, 111 F. Supp. 2d at 309.

173. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 455 (2d Cir. 2001).

174. 17 U.S.C. §§ 1201(a)(3)(A), (b)(2)(A) (2006).

operations. The customer, after all, is not party to license agreements among the consortium, nor asked to sign a license on purchase of a DVD. It is unclear therefore how the DVD or its player conveys to the viewer her authorization to watch the DVD.

The CD/DVD fork in media paths stems from the interaction of law and technology, in which law supports privately created systems of copyright protection through technological restriction. With access to open music formats, developers can invent first, negotiate market position later (if at all), and users can become developers. By contrast, faced with encrypted movies, only those developers who can pre-negotiate access can offer improvements, and only in locked-down ways approved and licensed by the movie producers. Thus the law-backed encryption on DVDs (and their high-definition successors) locks out interoperation and modification from those who hope to be public about their work. While those who care little about the legal consequences have already broken the encryption and built work-arounds, anticircumvention law largely deters mainstream developers from building without permission—and thereby from building much of the innovative use that video might support. The markets for both copyrighted works and their complementary tools and players are stunted by these conditions.

### B. SDMI AND THE FREEDOM TO TINKER

As music companies saw the other side to the DVD's cautionary tale, the Secure Digital Music Initiative (SDMI) group proposed "to develop the voluntary, open framework for playing, storing, and distributing digital music necessary to enable a new market to emerge."[175] Responding to "analog hole" and redigitization concerns, SDMI proposed an ecosystem of devices that would recognize an embedded watermark and refuse to play watermarked content if it appeared outside of a licensed context. Within this ecosystem, watermarks would prevent copying or uses without permission.[176]

---

175. SDMI Fact Sheet, http://web.archive.org/web/20040213143259/www.sdmi.org/who_we_are.htm (Jan. 27, 2004) (accessed by searching for sdmi.org in the Internet Archive index).

176. Watermarks are one response to the "analog hole" redigitization problem. By marking content as protected-origin, they can indicate that the content was originally restricted. If the initial restrictions never allow the content to be exchanged in unencrypted form, then compliant devices might be programmed to refuse to play unencrypted watermarked content. Of course non-compliant devices might simply ignore the watermark. Other proposals from SDMI suggested that they intended to use these watermarks to indicate that an audio track had not been subjected to compression since application of the watermark. *See* CRAVER ET AL., READING BETWEEN THE LINES: LESSONS FROM THE SDMI CHALLENGE (2001), *available at* http://www.usenix.org/events/sec01/craver.pdf. SDMI

Audio watermarks must serve two potentially conflicting goals: they must not interfere perceptibly with the sound of the music in which they are embedded, yet they must be detectable mechanically.[177] Thus someone determined to thwart the watermark would aim to remove it without changing the track's listening quality, so that both devices and listeners were satisfied with it.

On September 6, 2000, SDMI identified four watermarking technologies as possible elements of its music-protection strategy and issued an "Open Letter to the Digital Community," inviting people to "attack" the proposed watermarks.[178] A team of computer scientists and electrical engineers took up the challenge, downloading the provided samples and analyzing them using signal processing methods to determine how the watermarks had been applied and how they might be removed imperceptibly. This attack analysis

---

invited participation by "companies that have significant direct activity in digital music or digital music technology. These companies must express their commitment to SDMI by agreeing to abide by its Terms of Participation and paying a $20,000 annual membership fee." SDMI.org, Frequently Asked Questions, http://web.archive.org/web/20020924131640/www.sdmi.org/FAQ.htm (originally available at http://www.sdmi.org/FAQ.htm).

177. *See* CRAVER ET AL., *supra* note 176, at 3.

> [W]atermarking technologies [are those] in which subtle modifications are made to an audio file to encode information without perceptible change in how the file sounds. Watermarks can be either *robust* or *fragile*: robust watermarks are designed to survive common transformations like digital-to-audio conversion, compression and decompression, and the addition of small amounts of noise to the file; whereas fragile watermarks do not survive such transformations, and are used to indicate modification of the file.

*Id.*

178. Leonardo Chiariglione, An Open Letter to the Digital Community, http://web.archive.org/web/20040216013811/http://www.sdmi.org/pr/OL_Sept_6_2000.htm (Sept. 6, 2000) (accessed by searching for sdmi.org in the Internet Archive index).

> Here's an invitation to show off your skills, make some money, and help shape the future of the online digital music economy.
>
> The Secure Digital Music Initiative is a multi-industry initiative working to develop a secure framework for the digital distribution of music. SDMI protected content will be embedded with an inaudible, robust watermark or use other technology that is designed to prevent the unauthorized copying, sharing, and use of digital music.
>
> We are now in the process of testing the technologies that will allow these protections. The proposed technologies must pass several stringent tests: they must be inaudible, robust, and run efficiently on various platforms, including PCs. They should also be tested by *you*.
>
> So here's the invitation: Attack the proposed technologies. Crack them.
>
> By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt.

*Id.*

was not merely invited by SDMI, it is a standard part of computer security research. The peer review of technologies is critical to assessing their strength and improving their security.[179] Before copyright holders, device manufacturers, and public purchasers bought into the SDMI scheme, they might want to know how effective it would be at meeting its stated aims.

Edward Felten's team successfully broke all four watermark technologies, creating new samples from watermarked tests that were audibly indistinguishable from unwatermarked originals and bore no detectable trace of the watermark.[180] The team chose to present their work as an academic paper, securing its acceptance to the peer-reviewed Fourth International Information Hiding Workshop.[181] Before they could present the paper, however, Felten received a letter from the Recording Industry Association of America (RIAA), threatening suit under the DMCA.

> [A]ny disclosure of information gained from participating in the Public Challenge would be outside the scope of activities permitted by the Agreement and could subject you and your research team to actions under the Digital Millennium Copyright Act ("DMCA").
>
> Unfortunately, the disclosure that you are contemplating could result in significantly broader consequences and could directly lead to the illegal distribution of copyrighted material. Such disclosure is not authorized in the Agreement, would constitute a violation of the Agreement and would subject your research team to enforcement actions under the DMCA and possibly other federal laws. . . .
>
> In addition, because public disclosure of your research would be outside the limited authorization of the Agreement, you could be subject to enforcement actions under federal law, including the DMCA. The Agreement specifically reserves any rights that proponents of the technology being attacked may have "under any applicable law, including, without limitation, the U.S. Digital Millennium Copyright Act, for any acts not expressly authorized by their Agreement." The Agreement simply does not "expressly authorize" participants to disclose information and research

179. *See* Declaration of Ed Lazowska, Felten v. Recording Indus. Ass'n Am., No. CV-01-2669 (D.N.J. Aug. 13, 2001), *available at* http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cra_decl.html. *See generally* SCHNEIER, *supra* note 5 (discussing computer security).

180. CRAVER ET AL., *supra* note 176, at 12.

181. *See* Janelle Brown, *Is the RIAA running scared?*, SALON, Apr. 26, 2001, http://www.salon1999.com/technology/log/2001/04/26/felten/index.html; Reading Between the Lines: Lessons from the SDMI Challenge, http://www.cs.princeton.edu/sip/sdmi/ (last visited Mar. 30, 2010).

> developed through participating in the Public Challenge and thus such disclosure could be the subject of a DMCA action.[182]

The researchers and conference organizers were concerned enough by the legal threats that Felten and his team withdrew the paper from the April 2001 conference. The RIAA promptly issued a press release claiming that the organization had never intended to sue. Nonetheless, the researchers felt severe enough chill as they prepared to present their work in future papers and conference presentations that they filed suit seeking a declaratory judgment that their work did not violate the DMCA.[183]

The incident demonstrated the chills of the DMCA's broad prohibition on dissemination of technology and "components." While the researchers did ultimately publish and present their work, the RIAA and SDMI were able to use DMCA claims to delay it by half a year, and might well have scared off entirely researchers not backed by a university professor and pro bono legal assistance. Anticircumvention law, thus, blocks the scientific and educational examination of technology, including interoperation anticircumvention.

And to what end? The research that demonstrated flaws in these watermarks points to gaps in the ultimate strategy. If even the best watermarks SDMI could design were vulnerable to analysis and removal, it is unlikely that these disclosure-oriented researchers were the only ones who could do so. Among the music sharers targeted by the technological restrictions would be others able to skirt their controls, and who having done so, could share the resulting cleared files with others.

Since the breaking of its watermark technologies, the SDMI initiative has faded into insignificance as a technological force. A note on its now-defunct website indicated that the "SDMI Forum is on hiatus as of June 2001, and is not accepting new members."[184] Meanwhile, Felten's research has been cited by others in both computer security and copyright protection research.[185]

---

182. Letter from Matthew Oppenheim, Secretary, SDMI Foundation, to Edward Felten, April 9, 2001, *available at* http://cryptome.org/sdmi-attack.htm (last visited Mar. 25, 2010).

183. *See* First Amended Complaint, Felten v. Recording Indus. Ass'n Am., No. CV-01-2669 (D.N.J. June 26, 2001), *available at* http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010626_eff_felten_amended_complaint.html. The lawsuit was dismissed for lack of standing. Felten v. Recording Indus. Ass'n Am., No. 01-CV-2669 (D.N.J. Nov. 30, 2001) (docket report on file).

184. SDMI.org, Frequently Asked Questions, http://web.archive.org/web/20040213073219/www.sdmi.org/FAQ.htm (Jan. 27, 2004) (accessed by searching for sdmi.org in the Internet Archive index).

185. *E.g.*, Alin C. Popescu & Hany Farid, *Statistical Tools for Digital Forensics*, *in* INFORMATION HIDING 128, 128 (Jessica J. Freidrich, ed., 2004) (security research); J. ALEX HALDERMANN & EDWARD W. FELTEN, LESSONS FROM THE SONY CD DRM EPISODE

SDMI-like expansion is not the only alternative. Technological responses to law need not be pushed to the illogical extreme, but can leave room for independent development if they forego the legal backing for their tamper-proofing. Adobe's deployment of a limited technological control in its PDF (portable document format) authoring software illustrates that option and pinpoints the spots where legally-enforced technology could block open development, as well as the advantages of calling off the DMCA's hounds.

### C. AN ALTERNATIVE: NON-ROBUST ADVISORY MEASURES

Document authors using high-end versions of Acrobat, Adobe's PDF-authoring application, can choose to control initial *access*, encrypting and password-protecting documents; and to control *use*, by restricting printing, text selection, and even usage of screen reader applications.[186] The differing implementations of the two branches—and their interactions with open source and with anticircumvention law—give a glimpse of the way the law affects independent development.

PDF's access control is provided by encryption using modern, public algorithms. All can be given an encrypted blob, which only those who have been given the decryption key can decrypt. But 'access' is binary: on or off. Once the reader has decrypted the document, he or she has the decrypted document in its full digital glory, with the potential to print, save, and resend.

This encryption is robust: even implemented in open source, fully modifiable software, it gives access to the document only to those who enter the correct password or certificate. The strength of the encryption is independent of the implementation's publicity—indeed, public algorithms and implementations that have been subject to testing are likely to be stronger than privately developed alternatives.[187] With a key space sufficiently large to stymie brute-force attacks, an author can be relatively confident that her documents will be accessible only to those with the password. She can create a separate pass-key for each user and document, or use public-key infrastructure to encrypt to a recipient's existing private key.

As she wants to share a document more widely, however, the author may worry whether one authorized recipient will share it with another, make extra

---

(2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf (copyright protections).

186. *See* Adobe, Adobe Acrobat Pro Extended: Features, http://www.adobe.com/products/acrobatproextended/features/ (last visited Mar. 20, 2010).

187. *See* Bruce Schneier, *The Ethics of Vulnerability Research,* INFO, SECURITY MAG., May 2008, http://www.schneier.com/essay-211.html ("Anyone can design a security system that he cannot break.").

copies, or leave printouts lying around. By itself, encryption does not address those concerns.

In Adobe's system, some of these *use* controls are provided by flags marking restrictions on what the Adobe software will do with document. Adobe's reader software enforces the restrictions, so the recipient who uses Acrobat to open a document flagged "Printing: Not Allowed, Selection: Not Allowed" will find the usual print and text selection options greyed-out and unavailable. In Adobe's reader, such a document can be viewed on-screen but not printed, excerpted, or converted to other formats. The file itself can be copied infinitely many times, but each copy will have these same flags set.[188]

The PDF specification is publicly disclosed[189] and has been implemented in other applications including Apple's Preview and the GPL-licensed xpdf.[190] Preview, the Apple Macintosh's default PDF reader, responds to a "do not print" flag by disallowing printing and prompting for a document-authoring password. It likewise disallows selection of text in a document whose author has set that flag.

As distributed, xpdf behaves similarly, complying with the flags as well. Attempts to print flagged documents from an unmodified copy of xpdf are met with the error message: "Printing this document is not allowed." But the xpdf implementation is not 'robust.' Since xpdf's source is available to those who want to modify it, users frustrated by the flagged recommendations of a PDF document can compile their own versions. Among other customizations, they can tell modified-xpdf to ignore the flags of the program—by removing a check in five simple lines of code.[191]

---

188. The document may be encrypted, but the user who gets view-only privileges does not need to enter a key, it must therefore be one that is held by the program itself—and shared by every copy of the program. So the effect is only that of a flag.

189. *See* Adobe, PDF Reference, http://www.adobe.com/devnet/pdf/pdf_reference.html (last visited Mar. 20, 2010).

190. *See* Apple, What is Mac OS X—Graphics and Media, http://www.apple.com/macosx/what-is-macosx/graphics-media.html (last visited Mar. 20, 2010); Xpdf, Home, http://www.foolabs.com/xpdf/home.html (last visited Mar. 20, 2010).

191. Even to those without knowledge of C, this source code is fairly straightforward:

```
if (! doc->okToPrint()) {
error(-1, "Printing this document is not allowed.");
    exitCode = 3;
goto err1;
}
```

In English: If the document has no okToPrint indication, send an error message and abort, otherwise, continue with the user's request. A user who wanted to print a "printing disallowed" document could simply remove this conditional block;

```
// if (! doc->okToPrint()) {
```

Xpdf's code could have been obfuscated to make the check harder to find, but that would just mean a bit more work for the would-be-printer. Whether or not printing is allowed, the software must have access to the document to render it for on-screen display. At that point, the format relies on the software to enforce its restrictions, and software can be changed to ignore a simple flag and redirect the plaintext output to a printer as well as to a screen.[192]

The PDF specification's openness contributes to its popularity as a standard display and exchange format. Even before Adobe provided applications for most platforms, users could read and create PDFs on Unix and GNU/Linux systems as well as on Macintosh and Windows. Apple could decide at low overhead to build PDF support into its OS X operating system. Users of GNU/Linux operating systems such as Ubuntu can choose among Adobe's reader, xpdf, and ghostview, among others.[193] Independent developers can add features to the open-source xpdf or incorporate its functionality into new programs such as the pdf2html text–webpage generator. Users can create full-text indices of PDF files, facilitating better search, or independent programs to annotate PDF documents. Screen-reader applications can read the text aloud. Google and other search engines can parse the PDF files to include their text in search. Meanwhile, Adobe benefits from this ecosystem through royalties from additional sales of its enhanced PDF-reader and PDF-writer applications. Document authors benefit from the wide availability of tools, lowering the barriers to reading the works they make available. Adobe's open DRM format is successful

---

```
// error(-1, "Printing this document is not allowed.");
//   exitCode = 3;
// goto err1;
// }
```

If you don't check for the presence or value of okToPrint, a flagged document prints as easily as it displays.

This Author had to compile a print-friendly version of xpdf when, as a former editor of the Harvard Journal on Law & Technology (JOLT), she was contacted by one of that Journal's authors. That author had created a PDF version of his own article with the "Printing Not Allowed" and "Text Selection Not Allowed" flags set. After JOLT had published the article on its website, the JOLT author lost the original and wanted to recover the text. A modified xpdf enabled him to do this. This Author understands that similar functionality is now available in commercial programs.

192. It is likely that even if the reader were available only in binary form, it could still be reverse engineered, decompiled and edited to remove the flag check. Binary or obfuscated code would serve as just a minor obstacle to the determined flag-ignorer.

193. *See, e.g.*, Ubuntu Linux, Details of Package Pdf-viewer in Karmic, http://packages.ubuntu.com/karmic/virtual/pdf-viewer/ (last visited Mar. 20, 2010) (listing seven open source pdf viewers).

because Adobe does not insist on making it robust. Contrast this minimal advisory DRM format with other more robust DRM strategies, including Adobe's own eBook format. These tie the two branches of the strategy together, using encryption and § 1201, to force the authorized reader to use a particular application and obey the strictures of that application.

Advisory anti-copying features may have a place, especially if they do not invoke the DMCA. But Adobe's attitude toward breaks of the PDF anti-printing feature contrasts with DMCA prosecution it instigated against Elcomsoft after Dmitry Sklyarov broke the encryption on its eBook format. Sklyarov, a Russian Ph.D. student, was in the country for a computer security conference at which he gave a presentation on the insecurity of Adobe's eBook encryption technology. Following the presentation, he was arrested and charged with trafficking in a product designed to circumvent copyright protection, in criminal violation of the DMCA, based on his employer's sale of a software program to read encrypted eBooks.[194] Adobe had encouraged the prosecution, but then encouraged the government to drop charges against Sklyarov individually after widespread public protest. A federal jury ultimately rejected DMCA charges against the company.[195]

For many companies, the DMCA inclines them toward behavior like Adobe's close guarding of its eBook format rather than its openness around the PDF specification, to the detriment of open-source and user-accessible technology. With these examples in mind, this Article considers the implications of anticircumvention's foreclosure of open development more deeply through the lenses of economic and legal research on distributed innovation.

## V. NEW CRITIQUE: ANTICIRCUMVENTION TAXES OPEN DEVELOPMENT AND USER INNOVATION

Beyond fair use, the DMCA extracts costs by foreclosing an entire mode of development. The DMCA, and the contractual ties built around its anticircumvention regime, foreclose open source development of media software and open hardware because it is impossible to build the secrecy DRM requires into a product designed for user-modification and collaborative development. This foreclosure adds yet another set of weights

194. Criminal Complaint, U.S. v. Sklyarov, No. 5-01-257 (N.D. Cal. July 17, 2001); *see also* Press Release, Dep't of Justice, First Indictment Under Digital Millennium Copyright Act Returned Against Russian National, Company, in San Jose, California (Aug. 28, 2001), *available at* http://www.cybercrime.gov/Sklyarovindictment.htm.

195. Lisa M. Bowman, *ElcomSoft Verdict: Not Guilty*, CNET NEWS.COM, (Dec. 17, 2002), http://news.cnet.com/2100-1023_3-978176.html.

to the structural balance described by Tim Wu and Yochai Benkler[196]: the costs not only of centralizing creation and innovation, but of locking users—those most familiar with their technology needs and wants—out of the design process. Perversely, anticircumvention exerts this development-closing effect just as legal scholars, as well as economists and management scholars, are recognizing the significant contributions from open source development, user innovation, and peer production.[197]

The particular impact of anticircumvention-induced closure may have been overlooked in a tallying of the costs of DRM because it has not been recognized, or because the mode-of-development tax has not been distinguished from the overall impact of DRM on innovation. While this problem shares many of the elements with generalized harm to innovation, it is distinctly deeper-rooted; it is not one that can be designed around within the framework of anticircumvention. Even were DRM designers to follow the urging of academics and try to make room for innovation, they would ultimately face an irreconcilable gap between DRM and openness.

This Article thus adds to the literature an analysis of the mode-of-development tax. Earlier Sections described the progression by which digital rights management, supported by anticircumvention law, is driven towards ever higher degrees of lock-out. Each reaction to a perceived threat (whether to media control or profitability) drives the locking attempts deeper into the core of product design: from simplistic devices to hinder copying, to more complicated designs, to "robust" mechanisms to protect those devices and assure they operate as intended, and finally to architectural mandates and forced incompatibility. This Part will now explore the cost of such a lock-out. Changing not only *who* can innovate but also *how* they may do so severely limits the scope of development and its zone of potential. Characterizing anticircumvention as a mode-of-development barrier explains why the law is problematic even when the DRM it supports is chosen by private inter-industry standard-setting rather than by government mandate. Anticircumvention provides the hook by which to demand *some* DRM, and no matter how open the process by which the DRM standard was developed, devices implementing it will have to be closed.[198]

---

196. *See generally* Yochai Benkler, *Freedom in the Commons, Towards a Political Economy of Information*, 52 DUKE L.J. 1245 (2003); Wu, *Intellectual Property, Innovation, and Decentralized Decisions*, *supra* note 154.

197. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2007); ERIC VON HIPPEL, DEMOCRATIZING INNOVATION (2005); Karim R. Lakhani & Eric von Hippel, *How Open Source Software Works: "Free" User-to-User Assistance*, 32 RES. POL'Y 923 (2003); Josh Lerner & Jean Tirole, *Some Simple Economics of Open Source*, 50 J. INDUS. ECON, 197 (2002).

198. This is the flaw in the purportedly "open source" model behind Sun's DReAM

While DRM is ineffective against mass redistribution,[199] it imposes several costs on every would-be developer of interoperable devices: either licensing costs or the costs of circumventing the requested license, including the costs of breaking DRM (or finding an existing break); costs of assuring that other users will also be able to use the fix if developing for more than personal use; and costs of legal uncertainty. Law-backed DRM limits the potential upside to innovation because if a developer hopes to commercialize

---

platform. Even if anyone can build an implementation of the specification, it would win "authorization" to play protected content only after proving its un-modifiability by others as a prerequisite to obtaining permission. Developers writing such code would be unable to comply with the downstream "freedom to modify" condition of the Free Software Foundation GPL. *Cf.* Gerard Fernando, Tom Jacobs & Vishy Swaminathan, PROJECT DREAM, AN ARCHITECTURAL OVERVIEW (2005), http://www.openmediacommons.org/collateral/DReaM-Overview.pdf.

199. So long as DRM is trying to protect mass-distributed content, it faces an asymmetric challenge of adversaries as widely distributed as the interest in what it protects. *See* Stephen Lewis, *How Much Is Stronger DRM Worth?*, *in* ECONOMICS OF INFORMATION SECURITY 53, 54 (L. Jean Camp & Stephen Lewis eds., 2004).

> Even with the strongest DRM mechanisms we have today, the BORA (break once run anywhere) principle still holds. Once content is retrieved from a DRM system, and re-encoded in a non-DRM protected form, the duplication of that content is as easy as moving the bits around. This means that the cost of breaking the DRM on a particular piece of content need only be borne once. The marginal costs of the duplication to the consumer who can obtain the content are near-zero, and furthermore the consumer need not expend any resources in breaking the DRM.

*Id.*; *see also* Stuart E. Schechter et al., *Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment* (May 2003), http://www.eecs.harvard.edu/~stuart/papers/eis03.pdf (describing the cost of pirated goods as a function of one-time extraction costs (or first-copy costs) and per-copy distribution costs).

So why is DRM not equally ineffectual against innovation? A different kind of hacking is needed for distribution of the extracted original versus innovation around uses of that original. To stop Darknet-enabled mass copying and redistribution, you need to stop every would-be copyist, because once one copy is out, it can be shared with others at much lower cost. Whereas to stop user innovation, you can throw up barriers that stop a group from reaching critical mass—such that each person needs to overcome the barrier. Of course, some breaks, in software that is not individualized, can be shared rather than having to be recreated. *See, e.g.*, Adam Pash, Jailbreak Your iPhone or iPod Touch with One Click, LIFEHACKER (Oct. 29, 2007), http://lifehacker.com/316287/jailbreak-your-iphone-or-ipod-touch-with-one-click/. It may also be easier to break than to interoperate—finding a buffer overflow versus actually understanding the obfuscated code.

While Paul Ohm's *Myth of the Superuser* makes a persuasive argument against the focus of computer crime laws on the "superuser," in the DRM context it takes only one moderately-super user to make unencrypted content available to all. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1348 (2008). Fred von Lohmann refers to this as Mike Godwin's "smart cow" problem. Fred von Lohmann, *Licensing in the Digital Age: The Future of Digital Rights Management*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1009, 1042 (2005).

a product, she can predict having to seek a license, and expect that even if successful in obtaining that license, she will have to share the rents from innovation.[200]

Even if the usage rules posed no *practical* use restriction, such as that a device "must permit fewer than six billion copies," the robustness rules, mandating their implementation by technological fiat, would still bind the hands of developers. To build a system capable of *assuring* that it makes no more than 5,999,999,999 reproductions, the builder must lock it down, forbidding the end-user from tampering with the system and voiding those guarantees. For a "trusted system" to be reliable, it must be hardened against its users.[201]

The same challenge meets those who would design systems to adjudicate fair use or to check with a third-party arbiter before permitting new uses.[202] Even if the arbitration is perfect, the judge attuned to all the nuances of free expression, the *system* must be hardened to be capable of enforcing those determinations robustly. Technology's users must still be forbidden from modifying the core of their playback devices. Likewise, standardizing the DRM infrastructure might do away with custom DRM, making interoperation *among licensees* and marketing of works for the platform easier, but the standard would still bar user modification.

It is not possible to harden technical protection measures without closing devices to user development.[203] Trusted computing proposes a closed core

200. The potential for holdup is similar to that of blocking patents supported by injunctions. *Cf.* Mark A Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 2010 (2006) (arguing that patent injunctions "encourage rent seeking by patent trolls and discourage innovation by firms that design and manufacture complex products").

201. *See* SETH DAVID SCHOEN, TRUSTED COMPUTING, PROMISE AND RISK 10–11 (2005), http://www.eff.org/files/20031001_tc.pdf.

202. *See supra* Section III.B.

203. *See* Reid & Caelli, *supra* note 46, at 1. Reid and Caelli state:

> Once dissociated from its protection, the content can be freely copied, played, modified and redistributed, albeit in violation of the license terms. Consequently, to reliably enforce typical DRM policies, it must not be possible for the platform user to access the plaintext bits that represent the content, despite the practical reality that the platform is under the user's direct control. This is an access control problem that cannot be solved purely by cryptography. On open computing platforms that can run arbitrary software, it is a difficult problem to which there is currently no practical, deployed solution, particularly in terms of 'software-only' techniques. Recent trusted computing initiatives, namely Microsoft's Next Generation Secure Computing Base (NGSCB) and the Trusted Computing Group (TCG) specification, formerly known as TCPA aim in part, to address this issue through both hardware and software based methods.

with open interfaces. A system that offered users access to various features, while keeping the media decoding stream hidden, might be better than nothing, but it is not open source. It essentially lets users change the faceplates on their car radios, but not fix the tuners. In that mode, where users cannot manipulate the media stream directly, they are barred from implementing deeper features, such as modulating the audio to match sped-up video or adding echo cancellation.[204]

The copyright holders want a setup that cannot be made to leak the work, except through authorized outputs. They would prefer to have assurances up the viewer's eyeballs and eardrums, but if implants are impossible, they demand at least encrypted and signed pathways up to the analog output point of screen and speakers. While closed software and hardware can engage in the arms race, *appearing* secure until a smarter hacker comes along, open source software and user-modifiable hardware cannot even play the game. Their secrets are *intentionally* disclosed. Trusted computing, offered as the next generation solution for media on general-purpose hardware, does not allow for greater openness; it just pushes the closure into "trusted platform modules" and "remote attestation," and still forecloses open development of media software and hardware.[205] Moreover, trusted computing would not permit open source hardware, as Peter Gutmann notes in his catalog of the costs of Windows Vista content

> The goal of trusted computing is to deliver systems that are highly resistant to subversion by malicious adversaries, allowing them to operate reliably and predictably in almost any circumstance. Trusted computing is an important ingredient in DRM because it provides a sound basis for license enforcement. Given the way the NGSCB and TCG initiatives have been promoted, one could be forgiven for thinking that trusted computing is an entirely new concept. As we discuss in Section 3.1, trusted computing actually has a long history but the lessons this history can teach have been largely ignored over the last 20 years, particularly in the design of mainstream PC operating systems. As a consequence, such systems are fundamentally ill equipped to provide the level of protection that a robust DRM system demands.

*Id.* at 1–2 (internal citations omitted).

204. *See generally* Seltzer, *supra* note 9; PETER GUTMANN, A COST ANALYSIS OF WINDOWS VISTA CONTENT PROTECTION (2007), http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html.

205. Trusted computing provides a trusted platform, authenticated to be in a secure state with secure inputs and output paths, and audited source code that could "attest" to its integrity, checking in with a remote service for real-time verification before running with media input. *See* SCHOEN, *supra* note 201, at 4–5. In this case, the source code for this application could be delivered, but since a modified version would not pass the check-in, and thus would not actually be capable of functioning. Such tethered code would not pass the Open Source or Free Software definitions. *See id.*

protection.[206] Neither software nor hardware in a trusted computing platform is actually open and modifiable, even if its parts are visible under glass. This kind of one-way translucency would not support the vibrant innovation environment we see around genuinely open software and hardware. Openness is foreclosed by the design rules of DRM.

### A. THE HIDDEN COSTS OF DRM

Beyond impeding fair use, anticircumvention's restrictions are troublesome because they explicitly bar a particular mode of development—the public mode of free and open source software development—that has been increasingly successful in both commercial and non-commercial production.[207] Anticircumvention forecloses end-user tinkering and innovation and cements a centralized industrial structure, just at the time when technology offers us the means and networked opportunity to do more from the distributed edges of the Internet.[208]

While large incumbent firms have many economic advantages over smaller competitors, including operating at large scales and minimizing transaction costs, recent research suggests that a diversity of sources can more effectively foster innovation.[209] Non-incumbent firms and individual user-innovators may be better positioned to stretch limits, pursuing avenues that might not have been explored by the dominant industry players. Thus companies without a base of existing customers may be more likely than incumbents to produce disruptive innovations that find support outside an established customer base; though the disruptive innovations fail at first to serve existing customers, they may ultimately improve to meet the demands of both old and new customers better.[210] Meanwhile, users themselves may adapt or innovate upon products, using information and motivation more readily available to them than to corporate manufacturers.[211] Under an anticircumvention regime, however, any innovator who would challenge the incumbent media industry is precluded by law that centralizes the "permission to innovate" with the copyright owner.

---

206. *See* GUTMANN, *supra* note 204.

207. *See generally* Lerner & Tirole, *supra* note 197.

208. *See generally* BENKLER, *supra* note 197; CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS (2008); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006).

209. *See infra* Section V.B.

210. For the leading exponent of disruptive innovation, see CLAYTON M. CHRISTENSEN, THE INNOVATOR'S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL 79–81, 132–34 (1997).

211. The leader in user innovation research is Eric von Hippel. *See* VON HIPPEL, *supra* note 197, at 19–22.

Anticircumvention affects different kinds of innovators differentially. Disruptive innovation by commercial-scale firms may still be possible in limited circumstances—if the would-be disrupter can obtain permission in advance. A newcomer to digital media who is an established player in another field might have the clout to negotiate authorization with sufficient relevant copyright holders, and by such authorization convert its actions to non-circumvention; individual users are unlikely to be able to do so. Even in an un-concentrated, uncoordinated media market, neither companies nor users will be able to obtain "permission to tinker" or to offer general-use media-access products modifiable by other users, because such access to the underlying media stream is precisely what DRM is designed to prevent. In a concentrated, coordinated market, a few privileged participants may get access to the bulk of media, but even then, they will be unable to offer open user-modifiable products.

### B. DRM LIMITS DISRUPTIVE INNOVATION

Numerous industries have been dramatically reconfigured by "disruptive innovations," non-linear developments that benefit the public through greater productivity, efficiency, or choice. As Clayton Christensen describes, disruptive technologies are often initially dismissed as inferior by those in the industry, but they soon catch up to and outpace the old ones.[212] These technologies have two key characteristics: "[f]irst, they typically present a different package of performance attributes—ones that, at least at the outset, are not valued by existing customers. Second, the performance attributes that existing customers do value improve at such a rapid rate that the new technology can later invade those established markets."[213] Typically, Christensen finds, disruptive innovations are overlooked or cast aside by existing producers, even in "good" companies.[214] A company's strengths at listening to existing customer demands ("sustaining" innovations) can deafen it to the appeals of a new product with different characteristics and initial targets.[215] Hence in industry after industry, competitors have usurped the spots of prior giants.[216]

Disruptive products or services appear at first to be inferior alternatives for mainstream customers. The market applications these products might fit

212. *See* CHRISTENSEN, *supra* note 210, at 79–86.

213. Joseph L. Bower et al., *Disruptive Technologies: Catching the Wave*, HARV. BUS. REV., Jan.–Feb. 1995, at 44.

214. CHRISTENSEN, *supra* note 210, at 207.

215. *Id.* at 20.

216. *See* CLAYTON M. CHRISTENSEN & MICHAEL E. RAYNOR, THE INNOVATOR'S SOLUTION: CREATING AND SUSTAINING SUCCESSFUL GROWTH at 34–43 (2003).

offer lower profit margins, making them less attractive diversions of attention for an established company. A newcomer facing a different set of opportunity costs may be willing to experiment, however, selling to the lower-margin customer segments.[217] As it does so, it improves its competing product. The "disruption" occurs when some of these improved competitors attract mainstream attention, migrating from the sidelines to overtake the prior standard.[218] The erstwhile market leader is left to regret not focusing more attention on smaller, once-inferior disk drives or minicomputers.[219]

Christensen suggests that incumbents can learn to innovate disruptively,[220] but the sheer numbers and risk appetite of competitors make it likely more radical change will come from outside. An incumbent who recognizes this pattern of disruptive innovation but is unable to identify the potentially successful disruptive technology (and grab the profits for itself) may prefer to block new technology altogether. If the incumbent can do so using intellectual property, it can preserve its own position for a bit longer at the expense of a public denied the opportunities of technological improvement. It takes less foresight to seek stability by blocking others from innovating than to innovate for oneself.

The VCR and MP3 could both be considered disruptive technologies. The initial recording capacity and quality of the Betamax made it poorly suited for television broadcasters or movie studios to use in-house, but to television viewers with no other option for recording shows, poor quality was better than nothing.[221] As the quality was shown to be good enough, and the capacity improved, a virtual network of VCR-owners developed, providing opportunities for the rental of pre-recorded movies as well.[222] Similarly, the MP3's compressed audio was dismissed by audiophiles as inferior for music-listening, but its smaller file size made it popular with fans, who could "rip" MP3s to music players and trade them over even slow Internet connections.[223] In time, of course, both found sizeable audiences.

---

217. CHRISTENSEN, *supra* note 210, at 26.

218. *Id.* at 77–95.

219. *Id.* at 134–38 .

220. *See* CHRISTENSEN & RAYNOR, *supra* note 216, at 33–35.

221. *See* JAMES LARDNER, FAST FORWARD: HOLLYWOOD, THE JAPANESE, AND THE ONSLAUGHT OF THE VCR 95–97 (1987). This argument, which considers Betamax and VHS together, is distinct from the ongoing debate about whether the triumph of VHS over Beta illustrates path dependence. *See generally* S.J. Liebowitz, & Stephen E. Margolis, *Path Dependence, Lock-in, and History*, 11 J.L. ECON. & ORG. 205 (1995).

222. *See* LARDNER, *supra* note 221, at 312–20. On network effects of technology, see CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 183 (1998).

223. *See* STEVEN LEVY, THE PERFECT THING: HOW THE IPOD SHUFFLES COMMERCE,

The entertainment companies' response to both VCR and MP3 as they became popular was similar to their reaction to newer technologies under the DMCA: attempt to sue them away.[224] None of the existing copyright laws gave them traction, however. The Supreme Court ruled that Sony was not liable for enabling a combination of non-infringing, fair, and possibly infringing uses of its Betamax. Instead, the Court held that a device "capable of substantial non-infringing use," including that of "time-shifting" broadcast programming, was lawful to sell.[225]

The Diamond Rio, introduced in 1998, offered users portable storage for an hour's worth of MP3-encoded music, imported from a computer.[226] The Recording Industry Association of America sued, claiming that the device violated the Audio Home Recording Act (AHRA).[227] The Ninth Circuit rejected the argument on statutory grounds: The AHRA requires that "digital audio recording devices" contain serial copyright management features to bar second-generation copying, but because the Rio obtained its music through a personal computer (not primarily a music copying device) it was out of scope of the AHRA's mandate.[228] The decision properly found the AHRA's scope limited to special-purpose digital audio recorders (effectively rendering it irrelevant), rather than requiring every general-purpose computer to be restricted to watch for and respond to anti-copying watermarks. The *Diamond* court found that the Rio's space-shifting was likely non-infringing: "In fact, the Rio's operation is entirely consistent with the Act's main purpose—the facilitation of personal use."[229] Pre-DMCA copyright holders could not claim a right to control or bill for personal uses, even if those uses incidentally required copying.

These technologies disrupted existing entertainment production-and-distribution business models, while providing the public more access to art and entertainment. Under prior copyright law, companies in the entertainment business had to adapt or fail. But what pre-existing copyright

---

CULTURE, AND COOLNESS 144–55 (2006); Robert Levine, *The Death of High Fidelity*, ROLLINGSTONE.COM, Dec. 27, 2007, http://www.rollingstone.com/news/story/17777619/the_death_of_high_fidelity/print/.

224. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Recording Industry Ass'n of Am. v. Diamond Multimedia Sys., Inc. 180 F. 3d 1072 (9th Cir., 1999).

225. *Sony*, 464 U.S. at 456.

226. LEVY, *supra* note 223, at 27.

227. *Diamond*, 180 F. 3d at 1075.

228. *Id.* at 1078.

229. *Id.* at 1079.

law failed to control, the anticircumvention laws give new ammunition against.

Although music can still be accessed from unencrypted CDs, unburdened by technical protection measures, innovation upon and around other kinds of content has become harder. The difference the DMCA made was apparent from the first case decided under the new law in 2000: *Real Networks v. Streambox*.[230] Streambox developed the "Streambox VCR," a bit of software to play Real video streams, the then-dominant format of streaming video, and save them. Real sued for circumvention and won. To receive RealNetworks video, the Streambox VCR had to mimic the "Secret Handshake" of the RealPlayer client, a move the district court found to be circumvention.

> [A]t least a part of the Streambox VCR circumvents the technological measures RealNetworks affords to copyright owners. Where a RealMedia file is stored on a RealServer, the VCR "bypasses" the Secret Handshake to gain access to the file. The VCR then circumvents the Copy Switch, enabling a user to make a copy of a file that the copyright owner has sought to protect.[231]

By contrast to the pre-DMCA world, when movie studios lost their bid to stop the Betamax,[232] now it sufficed for Real to say that its Secret Handshake (not so secret, since every streaming client knew it) and Copy Switch were "technological measures" for it to win an injunction against the Streambox VCR's further production or distribution.[233] Users who wanted to time-shift online video—and the companies who wanted to offer them that and other options beyond those of Real's product—were out of luck.[234]

Other disruptive innovators have managed to negotiate with those who control entertainment copyrights—Apple's iTunes music store became the first commercially successful music store after various music companies had tried and failed.[235] Apple could secure copyright licenses and then, using the

---

230. RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

231. *Id.* at *20.

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

233. *RealNetworks*, 2000 U.S. Dist. LEXIS 1889, at *18–*19.

234. The *Streambox* court held that the DMCA eliminated *Sony*'s "substantial non-infringing use" defense. "Streambox's primary defense to Plaintiff's DMCA claims is that the VCR has legitimate uses . . . [but] 'equipment manufacturers in the twenty-first century will need to vet their products for compliance with Section 1201 in order to avoid a circumvention claim, rather than under Sony to negate a copyright claim.' " *Id.* at *21–*23 (quoting DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.18[B] (1999 Supp.)).

235. LEVY, *supra* note 223, at 168–70.

DMCA, create a format with which others were forbidden from interoperating.[236] With that combination, Apple could use the music to sell its iPod music players, the only ones with "authorization" to decode the encrypted AAC tracks, and then lock out other innovators from that piece of the market.[237]

While disruption is painful to those whose businesses are leapfrogged, it generally benefits end-users. Through competition, they get access to a wider range of products, better tailored to their needs in feature selection or price.[238] Customers who cannot attract the attention of a major producer, on whose scale they would be just a speck, may be able to find a supplier elsewhere who sees them as opportunities to break in to a new market. Some would-be disruptors fail, of course, but the larger number of innovators who can try when barriers to entry are lower gives more opportunities for unexpected successes.[239]

Armed with anticirumvention law, however, media companies can barricade themselves against disruption by such upstarts. By denying the critical "authorization" to anyone who would operate differently, the incumbents can lock out challengers. Fewer authorized innovators means fewer entrepreneurs free to pursue their own experiments around what the markets and public might support. The requirement of advance permission—and the possibility that permission will be denied or conditioned—imposes a hurdle that will stop many. Particularly around media where many are frustrated by the slow pace of entertainment companies' technology adoption, the public loses when competitors are forbidden from experimentation.

---

236. *See* Peter Burrows, *DoubleTwist is Dancing in Dangerous Legal Territory*, BUSINESS WEEK, Feb. 19, 2008, http://www.businessweek.com/technology/ByteOfTheApple/blog/archives/2008/02/doubletwist_is.html/.

237. Apple's recent decision to drop the DRM from its iTunes store does not contradict this story. DRM served to lock users into the Apple ecosystem early, as the iPod was taking off, but now annoys those same users as they try to move tracks among a growing number of Apple products. Meanwhile, compatibility with custom-designed software and peripherals can now serve to perpetuate the lock-in. *See* Brad Stone, *Want to Copy iTunes Music? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 7, 2009, at B1.

238. *See generally* W. KIP VISCUSI, JOSEPH E. HARRINGTON & JOHN M. VERNON, ECONOMICS OF REGULATION AND ANTITRUST (4th ed. 2005).

239. Distributed innovation thus functions like a diversified portfolio of options, giving more chances to succeed in the face of uncertainty. Some might argue that the incentives to compete are lower when the potential gain is a smaller, more rapidly disputed monopoly. However, as we see, *infra* Part V, the motivations to innovate are more varied than just the size of the profit pot, suggesting that innovation and entrepreneurship will continue to flourish even if not assured a winner-take-all outcome.

Yet if the circumstances are bad for would-be disruptive companies, they are worse for individuals or those seeking to enable end-user innovation. While innovation is still possible by those who can convince incumbents that they will share the profits, *end-user* innovation is precluded entirely in the domains where TPMs are in force. Robustness rules lock out open-source or user-accessible design.

### C. DRM LIMITS USER INNOVATION

Eric von Hippel has led the field in describing the ways in which users—and not just manufacturers—improve upon and innovate the products they use.[240] Because they are closer to their problems and benefit directly from their solutions, end-users often have better information and greater motivation to improve products than manufacturers. As von Hippel finds, from ten to forty percent of users across a range of fields engage in developing or modifying products, rather than merely "consuming" them.[241]

By innovating for themselves, end-users can obtain products not available commercially, products that may be unavailable because manufacturers have not gotten there yet or because it is not economical for manufacturers to offer the variety of items that would include all of their users' distinct individual preferences. Once lead-users have demonstrated the value of innovations and their commercial potential, however, manufacturers or a user community may develop it on a larger scale. Von Hippel and colleagues have found this user innovation pattern in business and consumer products alike, in fields from scientific and medical instruments to mountain bikes and rodeo kayaks.[242]

The current technology environment is particularly fertile for user innovation around consumer products, particularly in digital media. The Internet reduces costs of communication, enabling user communities to share information and development more cheaply and rapidly.[243] Where the product is bits, the Internet also reduces to near-zero the cost of distribution. End-users can get involved with little start-up capital. We have seen "DIY culture" reinvigorated as people learn to manage the complexity of computer technology and leverage it to their own ends: user innovation is enabled and

240. *See generally* VON HIPPEL, *supra* note 197; ERIC VON HIPPEL, SOURCES OF INNOVATION (1988).

241. VON HIPPEL, *supra* note 197, at 20 (2005).

242. *See* VON HIPPEL, SOURCES OF INNOVATION, *supra* note 240, at 11; Christoph Hienerth, *The Commercialization of User Innovations: The Development of the Rodeo Kayak Industry*, 36 RES. & DEV. MGMT. 273 (2006); Christian Lüthje, Cornelius Herstatt & Eric von Hippel, *User-innovators and "Local" Information: The Case of Mountain Biking,* 34 RES. POL'Y 951 (2005).

243. *See* Zittrain, *supra* note 208, at 1988.

manifested in do-it-yourself electronics and mechanical projects, from Make Magazine and its Maker Faires to Lego Mindstorms.[244] Online, the World Wide Web has accelerated the development of expression, software, and mashups (blogging, scripting, photography, videography, and mapping, to name a few).[245] Yochai Benkler suggests that these conditions for decentralized decision-making enable commons-based peer-production to improve upon market-based or hierarchical organization.[246]

The rising popularity of free and open source software both reflects the interest in user-accessible products and provides toolkits for it. With the source code available and freely modifiable, users can reconfigure software products or hire independent consultants to do so for them, even when their modification demands do not rise to the scale or expected profitability sufficient to interest a commercial supplier. Both hobbyists and commercial vendors have been willing to share their software's source code, often collaborating on the same project. While their motives may differ, user-producers of both types recognize value from enabling end-user investigation and modification.[247]

User innovation is not merely an interesting alternate source of products, it enhances social value. Joachim Henkel and Eric von Hippel "conclude that an innovation system where user innovation is present is welfare superior to one where it is not."[248] Even assessing only aggregate value—a society's total income and not its distribution—user-innovated products tend to suit their users more precisely, leaving less deadweight loss in the usual mismatch between product and function.[249] User innovation is less subject to the "consumer surplus effects" that can limit manufacturers' incentives to innovate when they feel they will be unable to capture the total value of new

244. *See* Tim O'Reilly, *Where Real Innovation Happens*, FORBES.COM, Feb. 2, 2009, http://www.forbes.com/2009/02/03/innovation-tim-oreilly-technology-breakthroughs_0203oreilly.html ("[A]lpha geeks exercise an idea or a gadget, push[] it past its current limits, reinvent[] it and eventually pav[e] the way for entrepreneurs who figure out how to create mainstream versions of their novel ideas."); Makezine.com, About MAKE, http://makezine.com/about/ (last visited Feb. 22, 2010).

245. *See* Zittrain, *supra* note 208, at 1994.

246. *See* Yochai Benkler, *Coase's Penguin, or Linux and The* Nature of the Firm, 112 YALE L.J. 369, 375 (2002).

247. *See* Karim Lakhani & Robert Wolf, *Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects*, *in* PERSPECTIVES ON FREE AND OPEN SOURCE SOFTWARE 12, 12–15 (Joseph Feller et al. eds., 2005); Josh Lerner & Jean Tirole, *Some Simple Economics of Open Source*, 50 J. INDUS. ECON. 197, 212–15 (2002).

248. Joachim Henkel & Eric von Hippel, *Welfare Implications of User Innovation*, 30 J. TECH. TRANSFER 73, 74 (2004).

249. *Id.* at 78.

products; as simultaneous producers and consumers, user innovators do not feel loss from this effect. User innovation thus increases social welfare through several vectors, including better products, better R&D, and, not to be underestimated, the enjoyment of innovation itself.[250]

First, user innovation may produce more valuable products directly. That is, user-innovators may become sources of product, for themselves or for others through non-commercial sharing or commercial entrepreneurship. They contribute new products and better customized versions of existing products, often, products that would not have been created—at least not so early or with the same attributes—if all development were commercial supplier-driven.[251] Users have advantages in development, such as the ability to iterate quickly to improve and respond to changing needs. They have better information about what they need and do not filter those needs through the barriers of cross-discipline communication, nor support the costs of disaggregating "sticky" information.[252]

Eric Raymond, computer programmer and open source advocate, explains why he began developing the fetchmail program:

> I needed a POP3 client. So I went out on the Internet and found one. Actually, I found three or four. I used one of them for a while, but it was missing what seemed an obvious feature, the ability to hack the addresses on fetched mail so replies would work properly. . . . This was clearly something the computer ought to be doing for me. But none of the existing POP clients knew how![253]

Working to "scratch[] [the] developer's personal itch," and soliciting the bug reports and code contributions of other user-developers, Raymond turned his stub of code into a robust mail-delivery program, tailored to the features he and the community needed in practice.[254]

Eric von Hippel tells similar innovation stories, from clinical chemists designing their own assays for research use, to mountain bikers building or modifying their equipment.[255] More than half of experimental results reported in the chemical literature derived from user-designed and -adapted

250. *Id.* at 81–82.

251. *See* VON HIPPEL, SOURCES OF INNOVATION, *supra* note 240, at 14–15.

252. Henkel & von Hippel, *supra* note 248, at 75; Eric von Hippel, *"Sticky Information" and the Locus of Problem Solving: Implications for Innovation*, 40 MGMT. SCI. 429, 430 (1994).

253. ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR 23 (2001).

254. *Id.* at 23–27.

255. VON HIPPEL, SOURCES OF INNOVATION, *supra* note 251, at 11; *see also* Lüthje et al., *supra* note 242, at 951.

tests.[256] Nineteen percent of mountain bike enthusiasts reported developing and building components of their equipment, often using skills from hobby or professional background.[257]

Thus users—whether in their roles as amateur hobbyists, professional scientists, or programmers—often build or adapt tools for their own use, to serve previously unmet needs. Some users become developer–distributors, as Raymond did maintaining the fetchmail client for a growing user base. Their innovations may later be followed by and shared with other similarly situated users.

Second, end-users can contribute to commercial innovation indirectly, serving as research labs for commercial suppliers. Even when the end-users do not themselves produce in large scale, their innovations may be adopted by established firms. As von Hippel describes, this diffusion is facilitated because user-innovators often "freely reveal" their improvements, either because it is more convenient for them to speak openly than to be secretive, or because they gain more from the ease with which other users can contribute than they would from a competitive head start.[258] Especially if they do not themselves plan to produce the product commercially or use it as a key component of a business process, end-users may see no disadvantages to revealing—no advantages to trade secrecy that justify the costs of keeping secrets—and may see benefits to having their small-scale efforts picked up for commercial use.[259] Thus users of open source software often contribute their modifications back as patches to the main source tree.[260] Along with recognition and reputational advantages, contributors can save themselves work, gaining better assurance of continued compatibility with a wider range of possible complementary applications,[261] bringing "more eyes" to their bugs, and, perhaps, improving the fixes further. The clinical chemists' independently developed tests are now available for purchase, pre-packaged, for their developers and the broader research community. Free revealing enables users to get both non-commercial and commercial support and commercial firms to add their expertise in larger-scale manufacture or distribution, using the community of lead users as a test bed or field research lab.

256. VON HIPPEL, SOURCES OF INNOVATION, *supra* note 251, at 11.
257. Lüthje et al., *supra* note 242, at 957, 961–62.
258. VON HIPPEL, *supra* note 197, at 77–91.
259. Lüthje et al., *supra* note 242, at 954.
260. Lakhani & von Hippel, *supra* note 197, at 926.
261. In software, contributing patches to the main codebase saves developers the work of reapplying the patches with each new release.

Further, the *process* of innovation may itself be rewarding to the user–innovator—it offers community, intellectual stimulation and development of new skills, and engagement with technology.[262] Engagement in development may make users happier with results by changing baseline expectations for products: a user may be more satisfied with a self-made product or improvement and more forgiving of its rough edges than if he had obtained the same product commercially.[263]

In addition to differences in the quality and variety of products and services developed, user innovation produces distributional benefits. The distribution of wealth and access may be fairer in a field open to user innovation than in one closed to it. Access may be more democratic, open to those who are time-rich and money-poor (and offering new fields of entrepreneurship by which people may make time into money). Particularly users with niche needs will be better served by self-innovating. Moreover, the user-innovator is empowered to think of him or herself as more than a mere consumer, and perhaps, like the Jeffersonian yeoman farmer, to become more involved in governance of the information environment.[264]

That society as a whole is better off when fields are open to user innovation does not, however, ensure that enough participants have the incentive to provide for it. While some companies recognize the opportunities user innovation provides (IBM, famously, contributes to Linux because better software, widely distributed and open, complements its proprietary hardware),[265] others feel threatened by the potential competition. They may fear losing the first-mover advantage of trade secrecy or prefer licensing revenue to its absence (e.g. licensing a smaller pool of technology rather than manufacturing a part of a big pool or making ancillary revenues).[266] Jonathan Zittrain suggests that even users will react against generatively open platforms if those platforms are more easily overrun by bad actors.[267]

---

262. *See* BENKLER, *supra* note 197, at 122–27; CHRIS DIBONA, SAM OCKMAN & MARK STONE, OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 13 (1999). *See generally* Ed Felten et al., Freedom to Tinker, http://freedom-to-tinker.com/ (last visited Mar. 7, 2010).

263. VON HIPPEL, *supra* note 197, at 33–43.

264. This Author uses governance by reference to ELINOR OSTROM, GOVERNING THE COMMONS (1990), to mean voluntary self-organization to overcome collective action problems and manage common pool resources.

265. *See* David Berlind, *Open Source: IBM's Deadly Weapon*, ZDNET, Apr. 8, 2002, http://news.zdnet.com/2100-10532_22-296366.html.

266. *See* Thomas R. Eisenmann, Geoffrey Parker & Marshall Van Alstyne, *Opening Platforms: How, When and Why?* (Harvard Bus. Sch., Working Paper No. 09-030, 2008), at 5.

267. JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 8

For those reluctant to be innovated against, anticircumvention has proven a powerful means of blocking user innovation, whether deliberately or incidentally. User innovation depends upon openness and accessibility of the underlying product.[268] Christina Raasch describes the impact of technical accessibility in the International Moth racing sailboat. This class is marked by a high degree of user-development, but as the technological complexity of the hull materials increased (in a shift from plywood to fiber-reinforced plastic and then carbon fiber), most users stopped innovating on hull design, although they continued to innovate elsewhere in the boats.[269] Robustness rules similarly increase the barriers to user innovation in media technologies.

### D. THE OVER-ARCHING COST: DRM CENTRALIZES INNOVATION, OPPOSING COPYRIGHT'S ORIGINAL GOALS

Contrary to the main trunk of copyright, the anticircumvention branch centralizes decision-making authority. Copyright as a whole decentralizes choices about the kinds and quantities of creative works that should be produced. By offering property rights of exclusion, copyright enables markets in creative works despite the basically non-excludable nature of creative expression.[270] Markets decentralize decision making[271]: instead of waiting for the state cultural minister or a wealthy patron to finance a new work of cinematic art, Walt Disney Co. can listen to the demands of millions of princess-favoring kids and their indulgent parents. Traditional copyright thus lets producers of creative works of art, literature, and music self-organize to meet what they perceive to be the interests of their audiences.[272] In a world of imperfect information, decentralization gives us more chances to match consumer interests and a more democratic opportunity to serve

---

(2008). Thus we cannot invoke the invisible hand to ask, "if it's so good, why aren't we there yet?"

268. The characteristics that make a product conducive to user innovation are similar to those Zittrain identifies as key to a technology's "generativity": capacity for leverage, adaptability, ease of mastery, and accessibility. Zittrain, *supra* note 208, at 1981. Where some of the characteristics of generativity, particularly "capacity for leverage," are directed to the creation of something else using the technology, user innovation focuses on changing the technological product directly. *Id.*

269. Christina Raasch, Cornelius Herstatt & Phillip Lock, *The Dynamics of User Innovation*, 12 INT'L J. INNOVATION MGMT. 377, 390 (2008).

270. *See* Wendy Gordon, *Fair Use as Market Failure*, 82 COLUM. L. REV. 1600, 1610–12 (1982).

271. F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 526 (1945).

272. *See* Wu, *Intellectual Property, Innovation, and Decentralized Decisions*, *supra* note 154, 146–47.

them.[273] Tim Wu suggests that intellectual property regimes should be assessed by their effects on the structure of decision making.[274]

Along with the economic benefits of letting markets organize production and enabling disruptive innovation, decentralization has social and cultural value. It helps to produce a democratic information environment, where everyone is a potential creator and consumer,[275] a read–write culture.[276] It lets users self-organize, in the mode Yochai Benkler terms "commons-based peer-production."[277]

While copyright decentralizes independent production, some have also noted that it centralizes control over follow-on expression. Through the exclusive rights over reproduction and derivative works, the initial creator can control use of his work as input if the use exceeds fair use.[278] There, they conclude that the problems get more serious (costs rise against benefits) as copyright's restrictions become more severe, apply to more conduct, and last longer.[279]

Yet if basic copyright, by creating markets, decentralizes at least the independent production of expressive works, the DMCA's anticircumvention provisions centralize control of the technologies that work with them, swapping one set of coordination problems for another. Where we celebrate copyright's "romantic author" and resisted centralized decision making for works of creative expression,[280] we have centralized innovation around the technological means to enjoy the created texts, sounds, and movies.

---

273. Even here, copyright is not costless. Economists discuss the tradeoffs between static costs and dynamic benefits. We accept the inefficiency of monopolies in individual works in exchange for the innovation derived from competition among them over shares of the broader "literature" or "entertainment" markets.

274. Wu, *Intellectual Property, Innovation, and Decentralized* Decisions, *supra* note 154, at 123–24.

275. WILLIAM FISHER, PROMISES TO KEEP 20 (2004).

276. LESSIG, *supra* note 86, at 28.

277. *See* Benkler, *supra* note 246, at 376.

278. *See* JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND (2008); Derek Bambauer, *Faulty Math: The Economics of Legalizing 'The Grey Album,'* 59 ALA. L. REV. 345 (2007); Benkler, *supra* note 129; Mark Nadel, Questioning the Economic Justification for (and thus Constitutionality of) Copyright Law's Prohibition Against Unauthorized Copying: § 106 (2003), AEI-BROOKINGS JOINT CTR., RELATED PUBL'N 3-1 (Jan. 2003), http://www.reg-markets.org/admin/pdffiles/Nadel.pdf.

279. For a fictional treatment of the expanding-derivatives problem, see SPIDER ROBINSON, MELANCHOLY ELEPHANTS (1983), *available at* http://www.spiderrobinson.com/melancholyelephants.html/ (describing a future in which nothing can be composed because everything imagined is too similar to works already under perpetual copyright).

280. *See* ROSEMARY COOMBE, THE CULTURAL LIFE OF INTELLECTUAL PROPERTIES:

Wu makes a similar critique of copyright's "communications policy," interpreting the current Copyright Act as a product of incumbent disseminators' rent-seeking activities to keep upstart challengers out of the market.[281] The pattern fits anticircumvention, helping to explain the expansion of the zone of authorization and control from authors of copyrighted works to developers of technologies of copy-protection. Not only do authors and copyright holders seek to capture all possible rents around their copyrighted works, non-authors try to use others' copyrights as a guarantor of profits. In the centralized marketplace, a few stagnating incumbent media companies[282] can use the continuing market power of back-catalog to prevent technologists or competing independents from inventing new models of media use.

## VI. CONCLUSION

When we grant anticircumvention control to copyright holders, we foreclose a set of possibilities and a solution space for the challenges of cultural exchange and technical productivity.[283] It is hard to quantify what does not yet exist,[284] but comparisons from other, less encumbered fields, and the not-too-distant past of media have suggested several reasons to prefer openness here.

The DMCA's anticircumvention provisions centralize the production of media playback technology, giving copyright holders the right to authorize—or forbid—the interoperation with their copyrighted works. This is a new phenomenon. In the "old world" of copyright, once the copyright holder had exercised his first sale rights, the public gained the ability and opportunity to use the work in a variety of ways that did not implicate copyright.

Anticircumvention closes the frontiers of media innovation. The open frontier is not just specific possibility, but an inspiration, an invitation to explore.[285] Not all the prospectors searching California for gold found that, but their risk-fueled exploration set the stage for commercial development of

---

AUTHORSHIP, APPROPRIATION, AND THE LAW 219 (1998).

281. Wu, *Copyright's Communications Policy*, *supra* note 154, at 325–28.

282. *See* WILLIAM PATRY, COPYRIGHT WARS AND MORAL PANICS 173 (2009).

283. *See* Timothy F. Bresnahan, & Manuel Trajtenberg, *General Purpose Technologies: "Engines of Growth"?*, 65 J. ECONOMETRICS 83, 84 (1995) ("Most [general purpose technologies] play the role or 'enabling technologies,' opening up new opportunities rather than offering complete, final solutions.").

284. And harder still to fund lobbying efforts on behalf of technology yet-to-be-invented.

285. *Cf.* FREDERICK J. TURNER, THE FRONTIER IN AMERICAN HISTORY 25–32 (1921) (attributing democratic success to the availability of a "public domain" of free land).

the American West. In the course of exploration and mapping the space, innovators may make unexpected discoveries and find new sources of value. Even if their hoped-for gold rush does not pan out, their exploration of the space may pave the way for other innovations of great aggregate importance.

Anticircumvention encourages copyright holders to stake out the frontier of technological innovation with "no trespassing" signs, not because they have explored and settled the territory to develop it productively, but because they feel threatened if others do so. Anticircumvention sends a message to developers, both commercial and user-innovators, that certain activities and opportunities are off limits, that even if it is technically feasible to improve interoperation with a wide variety of media, they are forbidden from doing so without advance permission. The vagaries (and transaction costs) of the permission-granting mechanisms deter innovators, as do the prospects of being forced to share the rents.

Anticircumvention serves as public law, enforcing private law, to forbid tinkering and block distributed user innovation. As a matter of regulatory design, this kind of architectural regulation externalizes costs. It lets those who benefit, a set of incumbent copyright holders, pretend that the imperfect DRM is good, while imposing a mode-of-development tax on the entire public. In the full cost–benefit analysis of anticircumvention, the loss to open user innovation outweighs the gains from this imperfect mechanism of copyright enforcement. Treating code literally as law leaves the law with too many harmful side effects.