Loyola of Los Angeles Entertainment Law Review

Volume 24
Number 4 *Symposium: Protecting Content in the Digital Environment*

Article 4

12-1-2004

Measuring the Digital Millennium against the Darknet: Implications for the Regulation of Technological Protection Measures

Fred von Lohmann

MEASURING THE DIGITAL MILLENNIUM COPYRIGHT ACT AGAINST THE DARKNET: IMPLICATIONS FOR THE REGULATION OF TECHNOLOGICAL PROTECTION MEASURES

*Fred von Lohmann**

Has the regulation of "technological protection measures" implemented by the Digital Millennium Copyright Act ("DMCA") been a success?[1]

When enacted in 1998, the DMCA represented a serious break from American copyright law and tradition.[2] Rather than regulating the reproduction, performance, display and distribution of copyrighted works—the traditional focus of copyright law—the DMCA focused on the "technological protection measures" ("TPMs") used to control access to, and use of, copyrighted works.[3] Enacted in section 1201 of the Copyright Act, these anti-circumvention provisions of the DMCA essentially shifted the spotlight from the copyrighted work to the "digital locks" used by copyright owners to protect the work.[4]

Curiously, five years after its enactment, few have paused to evaluate whether section 1201 has been a success or failure when measured on its own terms.[5] Has this section delivered on the policy justifications offered

---

* The author is a senior staff attorney with the Electronic Frontier Foundation, a nonprofit public interest organization devoted to the protection of civil liberties and free expression in the digital realm. For additional information, see http://www.eff.org.

1. The DMCA was an omnibus measure that included a number of distinct provisions. This paper is concerned with the anti-circumvention provisions of the DMCA, contained in Title I of the Copyright Act, and codified at 17 U.S.C. § 1201. References to the DMCA should be understood to refer to these provisions of the Act unless otherwise noted.

2. *See* Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1, 78–81 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); 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, 417–29 (1999).

3. *See* Samuelson, *supra* note 2, at 534.

4. *Id.*

5. *See* Electronic Frontier Foundation, *Unintended Consequences: Five Years Under the DMCA*, EFF.ORG, *at* http://www.eff.org/IP/DRM/DMCA/unintended_consequences.php. (last

by its supporters? Many criticized the DMCA as bad policy, arguing that it was unnecessary, and that it upset the traditional balance between copyright owners and the public interest.[6] Others extensively cataloged the unintended consequences that dogged the measure almost from its outset, specifically that of inflicting collateral damage on other public values, such as free speech, competition, and innovation.[7] However, few have questioned whether the DMCA succeeds or fails when measured against the policy rationales offered by its proponents five years earlier.[8]

The question is of particular relevance now.[9] A number of nations are considering whether and how they should follow the lead of the United States in implementing legal protections for copyright owners who employ TPMs.[10] At the same time, the United States is vigorously pressing its trading partners to adopt laws modeled on the DMCA as part of bilateral and multilateral trade agreements.[11]

This paper argues that the DMCA fails in light of its stated goal—namely, reducing the threat of copyright infringement in the digital age.[12] Trends in digital distribution technologies, moreover, indicate that *any* regulatory regime focused on TPMs as a solution to this problem may be doomed to fail.[13] In short, the developments of the last five years suggest that policy-makers should reevaluate whether legal prohibitions against the circumvention of TPMs represent the best regulatory lever for addressing

---

visited Mar. 9, 2004).

6. *Id.*

7. *See* Electronic Frontier Foundation, *supra* note 5.

8. *See id.*

9. The European Union issued a directive in May 2001 mandating that its member states provide legal protections to copyright owners who employ TPMs. Member states are in the process of crafting and implementing legislation. *See* Ross Anderson, *The Draft IPR Enforcement Directive—A Threat to Competition and to Liberty,* FIPR.ORG, *at* http://www.fipr.org/copyright/draft-ipr-enforce.htrml (last visited Mar. 9, 2004). New Zealand, Australia, and Canada are among the other countries considering the proper scope of TPM provisions. *See* Ministry of Economic Development, *Response to the Discussion Paper, at* http://www.med.govt.nz/buslt/int_prop/performers/cabinet/cabinet-03.html (last visited Mar. 10, 2004).

10. *See* Anderson, *supra* note 9.

11. Anti-circumvention obligations have been included in bilateral free trade agreements concluded between the United States and Chile, Singapore, Australia, Morrocco and Jordan. Similar provisions have been proposed as part of the multilateral Free Trade in the Americas Agreement (FTAA) and Central American Free Trade Agreement (CAFTA) negotiations, *at* http://www.fataa-alca.org/ftaadrafts_e.asp and *at* www.ustr.gov/new/fta/cafta.htm.

12. *See* Samuelson, *supra* note 2, at 520–23.

13. *See* COMMITTEE ON INTELLECTUAL PROPERTY RIGHTS, COMPUTER SCIENCE & TELECOMMUNICATIONS BOARD, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE (National Academy Press) (2000), *at* http://www.nap.edu/html/digital_dilemma/exec_summ.html [hereinafter DIGITAL DILEMMA].

what has come to be known as copyright's "digital dilemma."[14]

The discussion proceeds in four parts. First, this article reviews the development of the DMCA and the policy rationales offered by its proponents. Part II suggests that the arrival of new digital distribution technologies have created what some describe as the "darknet," a development that has undermined the DMCA's core policy rationale.[15] Part III briefly considers whether alternative policy mechanisms might better address copyright's digital dilemma. Finally, this article closes by touching on the costs imposed on the public by the DMCA and contrasting those costs with the DMCA's failure to generate the countervailing benefit—the reduction in the number of individuals engaged in infringing conduct—predicted by its supporters.

I. DEVELOPMENT OF, AND RATIONALES FOR, THE DMCA'S TPM PROVISIONS.

The DMCA's origins can be traced back to 1993, with the formation of an inter-agency federal working group known as the Information Infrastructure Task Force ("IITF").[16] In 1995, the IITF issued what became known as the "White Paper," which proposed that new legislation be introduced to target those TPMs used to protect copyrighted works.[17] In 1996, receiving a cool reception in Congress, the Clinton Administration took the TPM issue to the international arena, raising it with the World Intellectual Property Organization ("WIPO").[18] At the urging of the U.S.

---

14. The moniker is derived from the title of a comprehensive report published by the National Academy of Sciences in 2000 addressing the policy implications of new information technologies on intellectual property law. *See id.*

15. The "darknet" is defined as "[t]he collection of networks and other technologies that enable people to illegally share copyrighted digital files with little or no fear of detection. *The Word Spy*, THE WORD SPY.COM, *at* http://www.wordspy.com/words/darknet.asp (last visited Mar. 9, 2004) (defining "darknet" as a noun).

16. The Digital Millennium Copyright Act, S. REP. NO. 105–190, at 2 (1998) (giving an abbreviated view of the DMCA's legislative history); *see also* JESSICA LITMAN, DIGITAL COPYRIGHT 122–45 (2001); David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909 (2002) (giving a more comprehensive view of the DMCA's legislative history).

17. INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 230 (1995) *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf [hereinafter IITF WHITE PAPER]. *See also* Arnold P. Lutzker, *Primer on the Digital Millennium: What the Digital Millennium Copyright Act and the Copyright Term Extension Act mean for the Library Community, at* http://www.arl.org/info/frn/copy/primer.html (last visited Mar. 9, 2004).

18. Pamela Samuelson, *The Digital Agenda of the World Intellectual Property Organization: Principal Paper: The U.S. Agenda at WIPO*, 37 VA. J. INT'L L. at 369–75 (1997).

delegates, WIPO ultimately included general language that required "adequate legal protection and effective legal remedies against the circumvention of effective technological measures" in the 1996 Copyright Treaty.[19] The entire course of the DMCA's five-year gestation was marked by intensive lobbying and negotiation between copyright industries, information technology companies, and a variety of other major stakeholders.[20]

So what was the policy rationale for the TPM provisions of the DMCA? The answer is relatively simple. According to DMCA proponents, copyright owners faced a particularly serious threat of piracy in the digital context, since digital technologies allowed perfect copies to be easily made and inexpensively distributed.[21] Copyright owners, in turn, would not be willing to make their works available in the online environment absent some ability to prevent widespread online piracy.[22]

Legislators intended the DMCA to encourage copyright owners to employ TPMs such as "digital rights management" technologies to protect their works, by giving copyright owners legal recourse against those who circumvented these "digital locks" and those who made circumvention tools available to consumers.[23]

Proponents of the DMCA's anti-circumvention provisions were not naïve about the technological infallibility of TPMs. They admitted that no technology would be foolproof against every hacker bent on compromising it. The proponents were under no illusion that the copyright owners could track down and enforce the ban on acts of circumvention against every person on the planet who might outwit a TPM, any more than they were able to enforce their rights against every copyright infringer in the pre-digital era.[24]

Instead, these proponents envisioned that TPMs would be robust enough to prevent the average consumer from evading them, while the legal ban on circumvention tools and services kept user-friendly

19. World Intellectual Property Organization Copyright Treaty, Dec. 2–20, 1996, art. 11, *at* http://www.wipo.int/documents/en/diplconf/distrib/94dc.htm. For a general overview of the U.S. involvement in the development of Article 11, *see* Samuelson, *supra* note 18, at 369; *see also* Pamela Samuelson and John Browning, *Confab Clips Copyright Cartel*, WIRED 5.03 (Mar. 1997), *available at* http://www.wired.com/wired/5.03/netizen.html.

20. *See generally* LITMAN, *supra* note 16, at 89–150 (describing the legislative history and the rise of the information superhighway between 1992 and 1996).

21. *See* S. REP. NO. 105–190, at 8 (1998).

22. *Id.*

23. *See* IITF WHITE PAPER, *supra* note 17, at 230.

24. *See* Samuelson, *supra* note 2, at 519.

circumvention tools out of the mainstream marketplace.[25] Entertainment industry lobbyists are fond of expressing this notion as "keeping honest people honest," although it is more accurate to characterize the mechanism as "keeping technically unsophisticated people honest."[26] Another favorite is the "speed bump" metaphor—TPMs may not be impervious to technically sophisticated attackers, but would be enough of a "speed bump" to deter the average American couch potato from any unauthorized uses of a protected work.[27] Ultimately, it was hoped, the DMCA would restrain copyright infringement and encourage entertainment industries to make their wares available in the digital world.

Has it worked? Even a cursory review of the present state of digital media online suggests that the DMCA has, thus far, proven to be a conspicuous failure at its stated goal.[28] Despite the use of TPMs by copyright owners, it is evident that online copyright infringement has become a global and epidemic problem in part *because* of such uses.[29] Since the entertainment industries have been slow to make their wares available online, this has further fueled consumer demand for copyrighted works which are ultimately obtained from unauthorized sources.[30]

Where did the DMCA fail? It may be that the focus on TPMs as the best place to apply the lever of regulation by the DMCA was simply premature.[31] The negotiations that led to the DMCA began in 1993, at a time when relatively few Americans were using email, the World Wide Web had not yet been invented, the DVD was still on the drawing board, and the term "broadband residential Internet access" had not yet been coined.[32] The digital rights management technologies that the DMCA was intended to buttress were still in their infancy.[33]

While lobbyists and policy-makers crafted the DMCA, by 1998 the

---

25. *See* Electronic Frontier Foundation, *Digital Rights Management: The Skeptics' View*, EFF.ORG, *at* http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.php [hereinafter *DRM: The Skeptics View*] (last visited Mar. 3, 2004).

26. *See, e.g.*, Dean S. Marks & Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*, 46 J. COPYRIGHT SOC'Y U.S.A. 563, 567 (1999).

27. *See* Amy Harmon, *Studios Using Digital Armor To Fight Piracy*, N.Y. TIMES, Jan. 5, 2003, § 1, at 1 (quoting head of the Motion Picture Association of America, Jack Valenti, saying "[w]e need to put in speed bumps to keep people honest").

28. Samuelson, *supra* note 2, at 519.

29. *See* discussion *infra* Part IV.

30. *See* DIGITAL DILEMMA, *supra* note 13.

31. *See* Lutzker, *supra* note 17.

32. *Id.*

33. *See id.*

advancement of these technologies led to their widespread availability.[34] Nevertheless, subsequent technological developments revealed that the DMCA's drafters failed to anticipate developments in the digital storage and digital distribution technologies that today challenge the workability of the entire enterprise of using TPMs to protect copyrighted works online.

II. THE DARKNET INSIGHT.

In November 2002, four senior Microsoft security engineers took a fresh look at copyright's digital dilemma in an influential paper entitled *The Darknet and the Future of Content Distribution*.[35] The insights in that paper may serve to explain why the DMCA has thus far failed to deliver under its policy rationale.[36] Moreover, the paper suggests that efforts to solve copyright's digital dilemma with regulations focused on TPMs may be doomed to failure in the future.[37]

The Darknet paper is based on three assumptions about the modern digital environment:

1. Any widely distributed object will be available to some fraction of users in a form that permits copying.

2. Users will copy objects if it is possible and interesting to do so.

3. Users are connected by high-bandwidth channels.

The Darknet is the distribution network that emerges from the injection of objects according to assumption one and the distribution of those objects according to assumptions two and three.[38]

The first assumption is simply another way of saying that no TPM has yet been developed, nor is one likely to be developed, that is invulnerable against an expert attacker.[39] History has certainly demonstrated this time and time again as TPMs designed to protect mass-media products have

---

34. *See* DIGITAL DILEMMA, *supra* note 13.

35. Peter Biddle, Paul England, Marcus Peinado & Bryan Willman, *The Darknet and the Future of Content Distribution* (2002), *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc (last visited Sept. 26, 2004). In the months since its publication, Microsoft has been at pains to explain that the views expressed in the paper represent those of the authors, not Microsoft. *See* FREEDOM-TO-TINKER.COM *at* http://www.freedom-to-tinker.com/archives/000206.html (last visited Mar. 10, 2004).

36. *See* Biddle et al., *supra* note 35.

37. *See id.* § 1.1.

38. *Id.*

39. The darknet paper points out that this assumption is limited to mass market media, where a popular work is distributed to thousands or millions of users and is in demand by many more. The situation would be different where the object were distributed to a more limited group of individuals and contained content (like the medical records of one person) that would not be in high demand. *Id.*

been swiftly defeated.[40]

The remaining assumptions imply that, once compromised by a sophisticated attacker, a TPM is effectively useless at further restricting the widespread redistribution since users have the desire and capability to rapidly duplicate and propagate the formerly protected work. In other words, in light of modern digital distribution technologies, all it takes is "one leak" to neutralize a TPM entirely—and all TPMs leak (see assumption number 1).[41]

These insights, taken together, render obsolete the "keeping honest people honest" and "speed bump" mechanisms on which the efficacy of the DMCA depends.[42] So long as the average user has access to sufficiently effective darknet channels, the need to access circumvention tools does not exist. In effect, once a sophisticated user has broken the "digital lock" and extracted the content, there is no "speed bump" impeding subsequent unsophisticated users from gaining unauthorized access.[43]

Peer-to-peer file-sharing networks comprise the most widely-used and discussed darknet in existence today. Most estimates set the number of global file-sharers using programs like Kazaa and Morpheus in the hundreds of millions, with estimates in the United States ranging between 18 and 60 million.[44] There is credible evidence to suggest that the number of users continues to grow, despite lawsuits against individuals aimed at deterring further use of such software.[45]

---

40. For example, tools to circumvent the TPM used to secure DVDs, known as CSS, have been widely available for several years. *See* 321 Studios v. Metro-Goldwyn-Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004); Universal City Studios v. Corley, 273 F.3d 429, 436–37 (2d Cir. 2001). Copy protection technologies deployed on audio CDs have fared little better. *See* John Borland, *Student Faces Suit Over Key to CD Locks*, CNET NEWS (Oct. 9, 2003), *available at* http://news.com.com/2100-1025-5089168.html.

41. *See* Biddle et al., *supra* note 35.

42. *DRM: The Skeptics View*, *supra* note 25.

43. There are other "speed bumps" that may continue to have some force with many consumers, including moral suasion and a fear of being caught and punished. *But see, e.g.*, Dennis Michael, *Win or Lose, Napster Has Changed Internet*, CNN.COM (2000), *at* http://edition.cnn.com/2000/SHOWBIZ/Music/10/02/napster/index.html (suggesting that file sharers do not perceive downloading music as wrong). For purposes of this paper, it is enough to note that none of these alternative "speed bumps" rely on TPMs or the legal innovations introduced in the DMCA.

44. *See* Press Release, Ipsos-Reid, Americans Continue To Embrace Potential Of Digital Music (Dec. 4, 2002), *available at* http://www.ipsos-na.com/news/pressrelease.cfm?id=1685 (setting number of U.S. file-sharers at 60 million); Pew Internet & American Life Project, *Sharp decline in music file swappers: Data memo from PIP and comScore Media Metrix* (Jan. 4 2004), *available at* http://www.pewinternet.org/reports/toc.asp?Report=109 (estimating number of U.S. file sharers at 18 million).

45. *See* Farhad Manjoo, *Is the War on File Sharing Over?*, SALON.COM (Jan. 15, 2004), *at* http://archive.salon.com/tech/feature/2004/01/15/filesharing_tide_turned/index_np.html; *Did Big*

The authors of the Darknet paper, however, observe that other darknet mechanisms exist, as well. For example, the widespread availability of inexpensive optical storage media, such as CD-R and DVD-R discs, facilitates hand-to-hand exchanges. They also point to interconnected "small-worlds networks," comprised of affinity groups who exchange materials through private networks. Even if the global, public peer-to-peer networks were eliminated through legal or technical means, the Microsoft engineers conclude that these "small worlds networks" would likely provide a mechanism efficient enough to satisfy a large percentage of digital media consumers.[46]

The Darknet paper subsequently discusses several technological and legal strategies copyright owners could use to respond to the challenges posed by unregulated digital distribution networks. The copyright owners, for their part, have both seeded file-sharing networks with "spoofs"—decoys intended to significantly increase search costs for file sharers—and taken other self-help measures to reduce the efficiency of darknet channels for users seeking unauthorized content.

Whether these or other counter-measures can effectively impede the efficiency of darknet channels remains to be seen. But the insights contained in the Darknet paper make one thing clear—the use of digital rights management and other TPMs to control unauthorized reproduction and distribution of digital content is largely a waste of time and resources. As discussed above, TPMs are inevitably far from foolproof. Once compromised, TPMs are effectively eliminated from the equation.

If the authors of the Darknet paper are correct, then copyright owners are left with two alternatives. They can either strive for perfect enforcement of the legal prohibitions against acts of circumvention by the sophisticated users that break TPMs, or they can instead respond to the threat posed by digital distribution technologies. The former course seems unlikely to succeed, given the global nature of the problem and the difficulty in tracking down every potential adversary. Relying on the darknet assumptions, however, anything less than total success will dictate total failure—TPMs, once broken, are no longer effective at restricting subsequent infringements.

In fact, the use of TPMs by copyright owners may be worse than

---

Music Really Sink the Pirates?, BUSINESS WEEK (Jan. 16, 2004), *available at* http://www.businessweek.com/technology/content/jan2004/tc20040116_9177_tc024.htm; Thomas Karagiannis et al., *Is P2P Dying Or Just Hiding?* (Sept. 9, 2004), *available at* http://www.caida.org/outreach/papers/2004/p2p-dying/p2p-dying.pdf (evaluating trends in file-sharing and concluding that it has not declined since the RIAA lawsuit campaign began).

46. Biddle et al., *supra* note 35, §§ 2.1, 2.5.

useless; it may be counter-productive. Where alternative channels exist, customers of legitimate services will respond to restrictions imposed by TPMs by seeking out darknet channels. In the words of the Darknet paper's authors:

> [I]ncreased security (e.g. stronger DRM systems) may act as a *disincentive* to legal commerce. Consider an MP3 file sold on a web site: this costs money, but the purchased object is as useful as a version acquired from the darknet. However, a securely DRM-wrapped song is strictly *less* attractive: although the industry is striving for flexible licensing rules, customers *will* be restricted in their actions if the system is to provide meaningful security. This means that a vendor will probably make more money by selling unprotected objects than protected objects. In short, if you are competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security.[47]

To take an example, imagine a customer who buys a CD and discovers that it is "copy-protected," thereby frustrating any desire to transfer the music to her iPod. Such copy protection gives that paying customer an incentive to install Kazaa to download unencumbered versions of the music available on her CD. Once the user has invested the time to find, install, and learn how to use Kazaa, she may be tempted to download additional music she has not purchased. And that person may be affected in such a way that he or she may no longer buy CDs—why buy the cow, when you can get the milk for free?[48] In this way, ironically, CD copy-protection technology effectively drives legitimate customers into the arms of unauthorized darknet alternatives, to the long-term detriment of copyright owners.

III. DARKNET'S IMPLICATIONS FOR ENTERTAINMENT INDUSTRIES AND ANTICIRCUMVENTION REGULATIONS.

Concern is appropriate, but alarm perhaps is not. Although this paper focuses on the efficacy of anti-circumvention regulations as a policy tool to

47. *Id.* § 5.2.

48. *See* Shawn Langlois, *MusicNet Walks the Cyber-Plank. Web Surfers Hardly Dancing to AOL's Subscription Tune*, CBSMARKETWATCH.COM (Feb. 27, 2003), *at* http://cbs.marketwatch.com/news/story.asp?guid=%7B240F5267-1561-4B9C-AA0B-7B230CC298A1%7D&siteid=google&dist=google. "AOL Time Warner this week became the latest company to attempt to sell the cow to customers who've grown quite accustomed to getting the milk for free." *Id.*

address copyright's digital dilemma, a brief digression may be in order to reassure those who may have concluded that the darknet is fundamentally irreconcilable with intellectual property. That conclusion, however, would be premature.

In a digital world, efficient darknets are easily accessible to most digital media customers. Consequently, copyright owners are effectively left to "compete with free." As daunting as this may sound, numerous large industries have crafted successful businesses in the face of "free." Examples often mentioned include bottled water, private education, and Starbucks coffee.[49]

Perhaps the best example is one drawn from the digital media market itself. Today, virtually every popular movie released on DVD is widely available from unauthorized sources, whether on the public peer-to-peer file sharing networks, through small worlds networks made possible by software like Bit Torrent, or through hand-to-hand DVD-R copying.[50] Nevertheless, DVD sales not only remain robust, but continue to show positively explosive growth.[51] As a result, the motion picture industry is enjoying its most profitable years in history even as peer-to-peer file sharing continues to grow.[52] How is it that DVDs have managed to not only succeed, but in fact thrive, while "competing with free"?

One thing is clear: neither the DMCA anti-circumvention provisions nor the use of TPMs have been of any help.[53] DVDs were among the first mass-market media objects to utilize a TPM system; namely, the CSS

---

49. *See, e.g.*, Symposium, *Copyright's Long Arm: Enforcing U.S. Copyrights Abroad*, 24 LOY. L.A. ENT. L. REV. 1, 72 (2004) (statement of Professor Paul Goldstein noting the shrewd marketing behind bottled water).

50. *See* Richard Menta, *Proof that File Trading Sells DVDs. . .Sort Of*, MP3NEWSWIRE.NET (April 13, 2003), *at* http://www.mp3newswire.net/stories/2003/dvd_sales.html. Some movies are even available through such networks before their official release date, though rarely.

51. *See* Seth Schiesel, *File Sharing's New Face*, N.Y. TIMES (Feb. 12, 2004), *available at* http://www.nytimes.com/2004/02/12/technology/circuits/12shar.html?ex=1081054800&en=c7508929609679f4&ei=5070; Lorenza Muñoz and Jon Healey, *Pirated Movies Flourish Despite Security Measures*, L.A. TIMES (Dec. 4, 2003), *available at* http://www.latimes.com/news/local/la-et-piracy4dec04,1,4016096.story.

52. Entertainment and Electronic Media, INDUSTRYPRO.COM, *at* http://www.industrypro.com/reports/chpt32electronicentertainmentmedia.pdf (last visited Mar. 14, 2004).

53. Movie studios have also been vigilant in using the anti-circumvention provisions of the DMCA to crack down on the availability of products that are able to circumvent the CSS system used on DVDs. *See, e.g.*, Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001); Paramount Pictures Corp. v. 321 Studios, No. 03-CV-8970, 2004 U.S. Dist. LEXIS 3306 (S.D.N.Y., Mar. 4, 2004); 321 Studios v. Metro-Goldwyn-Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004). Despite their unbroken string of successes in court, circumvention tools remain widely available from a variety of darknet sources.

encryption system ("CSS").[54] CSS was readily compromised, and today, free circumvention tools are in wide circulation across the Internet. Most who are interested in unauthorized downloading of movies, however, never require the use of a CSS circumvention tool—the movies available in darknet channels have been "pre-circumvented" by expert users and those versions are often compressed to facilitate further redistribution.[55]

The DVD, however, offers a number of features that make it successful in the face of darknet competition. First, the product is widely perceived as a convenient, high-quality medium.[56] Consumers readily appreciate the improvement over the prior standard of prerecorded VHS cassettes. Second, DVDs have been aggressively priced, with titles frequently available for $10-12 at retail.[57] Moreover, customers have a variety of rental and pay-per-view options that can bring the cost for a single viewing down to as little as $2.[58] In contrast, movies often found through darknet channels suffer from inferior quality, consume a significant amount of time to obtain, and require the viewer to either watch on their computer screen or engage in the cumbersome task of transferring the movie to DVD-R.[59]

By continuing to offer a superior alternative at a competitive price, DVDs prove that the motion picture industry can "compete with free."[60] In addition, the DVD experience suggests that one of the best ways to compete is to provide customers with competitive prices and convenient access to products that cannot be easily delivered via the darknet.[61] For

---

54. *See Universal City Studios v. Corley*, 273 F.3d at 436–37 (describing CSS).

55. In fact, recent research suggests that most movies available from darknet channels are leaked by movie studio "insiders." *See* Simon Byers, et al., *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process*, ACM WORKSHOP ON DIGITAL RIGHTS MGMT. (2003), *available at* http://portal.acm.org/citation.cfm?doid=947380.947383. Although movie studios have begun employing TPMs in an effort to control this, it appears these TPMs have been no more successful at preventing widespread distribution than CSS.

56. *See, e.g.*, Stephen H. Wildstrom, *A Multimedia Power Surge*, BUSINESSWEEK.COM, *at* http://www.businessweek.com/1996/53/b3508106.htm (last updated June 13, 1997).

57. *See* Michael Booth, *Recording Industry's Missteps*, DENV. POST , Sept. 14, 2003, at F1.

58. *See, e.g.*, Scott Hilyard, *With "On Demand" Cable, Viewers Watch What They Want*, COPLEY NEWS SERVICE, Aug. 9, 2004, LEXIS, Nexis Library, Copley News Service File.

59. *P2P Calls in Air Strikes*, (March 28, 2003), *at* http://blogcritics.org/archives/2003/03/28/081647.php.

60. *See* Anthony Violenti, *Slipped Discs*, BUFF NEWS, July 8, 2003, at D1.

61. Some in the movie industry have claimed that they have been sheltered from the full force of the darknet by the relatively meager bandwidth available in most American homes. *See* Jack Valenti, A Clear Present and Future Danger: The Potential Undoing of America's Greatest Export Trade Prize, Testimony Before the Senate Foreign Relations Committee (Feb. 12, 2002), *available at* http://www.copyrightassembly.org/briefing/test_021202.htm. This is what prevents customers from instantaneously downloading perfect, full-quality copies of DVD movies, or so

example, movie studios could spend less of their time, energy, and resources bickering about the appropriate TPMs for next-generation high-definition DVDs.[62] Instead, they could rush movies to market in the new format that, due to its high resolution and consequent large data payload, will be more resistant to darknet redistribution than today's DVDs—a natural "speed bump" to users that might try to access them through darknet channels. As the Darknet authors point out, when competing with free, the best strategy is not to encumber legitimate customers with technological restrictions, but to offer them a better experience than they can obtain via darknet channels for the same "cost" (whether measured in search costs, download times, or monetary outlay).[63]

Should any particular copyright industry prove unable to effectively "compete with free," there are other policy mechanisms that may serve to mediate the challenges posed by the digital dilemma.[64] Alternative compensation systems have been used in the past to address new technologies that prove difficult for the traditional copyright regime to digest.[65] A number of commentators have recently begun exploring the possibilities presented by compulsory licensing and voluntary collective licensing approaches to the digital dilemma.[66] These deserve additional attention in light of the insights of the Darknet paper.

IV. REGULATING THE WRONG THING, AND IF SO, AT WHAT COST?

To return to the main theme, however, the rapid development of

goes the argument. Even if the rosy predictions of rapid growth in residential broadband capacity were to come true, however, further TPMs on movies are unlikely to impede the Darknet. There may be other policy initiatives that should be considered to address this, should "super-broadband" become widely available and should DVD sales show any signs of slowing, but the anti-circumvention provisions of the DMCA seem plainly unsuited to addressing this possibility for the reasons discussed earlier.

62. *See* Nick Wingfield, John R. Wilke, & Phred Dvorak, *U.S. Probes DVD Industry Group*, WALL ST. J., Jan. 26, 2004, at A3.

63. *See* Biddle et al., *supra* note 35 at § 5.2 "In short, if you are competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security." *Id.*

64. *See, e.g.*, WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT 199–258 (2004); *see also* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003); *see also* Raymond Shi Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 312–15 (2002).

65. *See* Netanel, *supra* note 64; at 31–35.

66. *See, e.g.*, Fisher, *supra* note 64; *see also* Lichtman & Landes, *supra* note 64; Netanel, *supra* note 64; Ku, *supra* note 64.

digital distribution technologies poses a fundamental challenge to regulatory regimes premised on protecting digital media content by prohibiting circumvention of TPMs.[67] To put the matter simply, when enacting section 1201 of the DMCA, it appears that legislators may have chosen to regulate the wrong thing.

The error is particularly grievous in light of the mounting evidence that the anti-circumvention provisions of the DMCA are inflicting serious collateral damage on other public values, including scientific research, free speech, innovation, fair use and competition.[68]

There have been more than a dozen reported incidents involving DMCA threats to researchers, journalists, and hobbyists.[69] Bowing to DMCA liability fears, self-censorship is common: online service providers and bulletin board operators have censored discussions of copy-protection systems; programmers have removed computer security programs from their Web sites; and students, scientists, and security experts have stopped publishing the details of their research.[70]

Legitimate computer security research has been a frequent target of overreaching DMCA claims.[71] In perhaps the best-known example, in September 2000, a multi-industry group known as the Secure Digital Music Initiative (SDMI) issued a public challenge inviting technologists to defeat certain watermarking technologies intended to protect digital music.[72] Princeton University Professor Edward Felten and a team of researchers at Princeton, Rice University, and the Xerox Corporation took up the challenge and succeeded in removing the watermarks.[73]

When the team tried to present their results at an academic conference, however, representatives of SDMI threatened the researchers with litigation under the DMCA.[74] The threat letter was simultaneously delivered to the researchers' employers and the conference organizers.[75] After extensive discussions with counsel, the researchers grudgingly withdrew their paper from the conference.[76] The paper was ultimately

67. *See* Terri Branstetter Cohen, *Anti-Circumvention: Has Technology's Child Turned Against Its Mother?*, 36 VAND. J. TRANSNAT'L L. 961, 973 (2003).

68. *See* Electronic Frontier Foundation, *supra* note 5.

69. *See id.*

70. *See id.* (citing each of the instances detailed in the following examples).

71. *See id.*

72. *Id.*

73. *Id.*

74. Electronic Frontier Foundation, *supra* note 5.

75. *Id.*

76. *Id.*

published at a subsequent conference, but only after the researchers filed a lawsuit of their own against SDMI, resulting in the withdrawal of the DMCA threats.[77] Incidents like this one led White House Cyber Security Chief Richard Clarke in October 2002 to call for DMCA reform, noting his concern that the law had been used to chill important computer security research.[78]

Others have wielded the DMCA to hinder legitimate competition.[79] For example, Lexmark, the second-largest laser printer vendor in the U.S., has invoked the DMCA in an effort to eliminate the secondary market for refilled printer toner cartridges.[80] Similar suits have already been brought in the garage door and video game industries in an effort to eliminate legitimate competition from interoperable products.[81] Some in the auto industry are worried about the use of the DMCA to eliminate the aftermarket for automotive parts.[82]

A comprehensive review of the unintended consequences of the DMCA is beyond the scope of this article. Policy-makers, however, have a responsibility to periodically evaluate the costs and benefits of the policies they enact. Where the anti-circumvention provisions of the DMCA are concerned, the costs appear to be mounting, while the benefits appear never to have materialized.[83]

V. CONCLUSION

It is time to reconsider the wisdom of relying on legal protections for TPMs to address the challenges posed by digital technologies for the copyright industries. Countries that have not yet embarked down this path should refrain from doing so. Policy-makers in the United States, meanwhile, should give serious consideration to repealing the anti-circumvention provisions of the DMCA in favor of allowing a new solution to the digital crisis—preferably, one that works.

---

77. *Id.*

78. *Id.*

79. *See id.*

80. Electronic Frontier Foundation, *supra* note 5 (citing Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003)).

81. *See id.* (citing The Chamberlain Group, Inc. v. Skylink Technologies, Inc., 292 F. Supp. 2d 1023 (N.D. Ill. 2004), *aff'd per curiam*, 381 F.3d 1178 (Fed. Cir. 2004) and Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000)).

82. Frank Ahrens, *Caught By the Act; Digital Copyright Law Ensnaring Businesses, Individuals Over Fair Use*, WASH. POST, Nov. 12, 2003, at E1.

83. *See* discussion *supra* Part I.