Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice About DRM Restrictions?

by
Pamela Samuelson & Jason Schultz*

Introduction

Advances in digital technologies have made many things possible, including cheap and easy copying and distribution of commercially valuable digital content, such as sound recordings and motion pictures, via global digital networks.[1] Although some technologists believe that digital information can no more be made uncopyable than water can be made unwet,[2] other technologists have taken on the challenge of doing just that, after recognizing the emergence of a new market opportunity for innovative digital technologies capable of counteracting the ease of copying and dissemination of digital content.

Frustrated and fearful at the prospect of losing control over their digital content, copyright owners have become avid adopters of these technical protection measure (or TPM, sometimes referred to as "digital rights management" or "DRM") technologies which can be used to control or inhibit unauthorized access to and uses of digital content in mass-market products and services.[3] One British copyright lawyer has optimistically opined that "[t]he answer to the machine is the machine."[4] Many copyright owners, particularly those in the entertainment industry, regard TPMs as essential to the creation of viable global markets.[5]

For some of the very same reasons that copyright owners find TPMs attractive, consumers of digital products may find TPMs unattractive, or worse, frustrating, annoying, and harmful. TPMs often inhibit playful and creative uses of digital works and

---

* Pamela Samuelson is the Richard M. Sherman Distinguished Professor of Law at Boalt Hall School of Law; Jason Schultz is a Staff Attorney at the Electronic Frontier Foundation.

[1] See, e.g., NATIONAL RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 23-75 (2000) (discussing advances in digital technologies that have given rise to difficulties of enforcing copyright protections).

[2] Bruce Schneier, CryptoGram Newsletter, May 15, 2001, available at http://www.schneier.com/crypto-gram-0105.html#3.

[3] We will use the term "technical protection measures" and the acronym "TPM" to refer to technologies that other commentators refer to as digital rights management and DRM technologies, except when we are quoting from sources that use the latter. See, e.g., Pamela Samuelson, *Digital Rights Management {and, or, vs.} the Law*, 46 Comm. ACM 41 (April 2003) (discussing the complex intersection of legal rights and technical measures).

[4] Richard Poynder, "The Answer to the Machine is the Machine" (April 2001), available at http://scientific.thomson.com/free/ipmatters/ipprobs/8204398/ (quoting Charles Clark, General Counsel to the International Publishers Copyright Council)

[5] See, e.g., WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 10-13 (Sept. 1995) (expressing concern about infringements made possible by the Internet and digital technologies and the importance of technical measures to inhibit infringements).

other non-infringing uses of the content, such as time- or platform-shifting. Consumers do not much like having to pay more for TPM'd products that have lesser utility than their non-TPM'd counterparts. Consumers are especially likely to be frustrated and upset when they purchase technically restricted content without having advance notice about what TPMs will disable or otherwise do that they don't expect. This article will demonstrate that copyright owners are generally failing to give adequate and effective notice of TPM restrictions. This lack of transparency about TPMs is causing consumers not only frustration but several different kinds of harm. We believe that some regulatory action is necessary to address the notice problems that TPMs have brought about and can do so without undermining the goals of content protection that many copyright owners desire.

Part I of this article demonstrates that consumers have many expectations about what they should be able to do with digital content. In general, they expect to be able to do at least as much with digital content as they could with copies of copyrighted works in the traditional analog world; indeed, they often expect to be able to do even more with digital content than with analog works. When TPMs interfere with consumers' ability to engage in such uses, as indeed many are programmed to do, consumers are likely to be and have become frustrated and upset, especially if they purchased this product without notice of the restrictions.

Part II observes that copyright owners who employ TPMs to protect digital content products often do not give adequate and effective notice about technical restrictions on the usability of that digital content. Sometimes copyright owners give no notice at all about the technical restrictions, while other times, notice is inadequate or ineffective. Part II identifies six categories of harm that consumers have experienced as a result of the failure to give adequate and effective notice of TPM restrictions.

Part III discusses various studies and reports that have characterized the lack of notice of technical restrictions on digital content as a consumer protection issue warranting attention. While European commentators have been more active in analyzing transparency and other consumer protection issues arising from TPM'd content, American policymakers and commentators have become aware of these issues, particularly after the "magnificent disaster" of the Sony-BMG rootkit incident.[6]

Part IV considers several policy options for addressing the inadequacy of notice problem discussed in Parts II and III. The least interventionist strategy on the policy spectrum is to trust the market to produce an appropriate degree of notice of technical restrictions in digital content products and services. For reasons explained in Part IV, we are skeptical that the market has or will fix the notice problem with TPM'd content. The most interventionist strategy would not only require notice of technical restrictions but would consider substantive regulations about what digital content providers should be able to do (and not do) with TPMs in restricting consumer uses of digital content.

---

[6] Deirdre Mulligan & Aaron Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 Berkeley Tech. L.J. (forthcoming 2007).

In the middle of the policy spectrum lie alternatives that envision a role for the Federal Trade Commission (FTC) in studying the notice problem with TPM'd content and developing standards for adequate and effective notice of TPM restrictions on digital content. This article recommends that the FTC should conduct a thorough empirical investigation of TPM'd digital content, with special attention to the adequacy and effectiveness of notice of technical restrictions, and should report to Congress about whether legislation to mandate notice is necessary to protect reasonable consumer expectations as to technically protected digital content.

I. Consumer Expectations as to Digital Content and TPMs

Consumer expectations about permissible uses of digital media products have partly been shaped by personal use patterns arising from experiences with traditional media. After purchasing long-playing (LP) recordings of musical works back in the olden days, for example, consumers felt free to make personal use copies to play on other platforms (e.g., making tapes of the LPs to play in their cars) or as backups in case the LPs got scratched.[7] When the commercial medium for recorded music shifted to compact discs (CDs), consumers similarly felt free to make personal use copies (e.g., loading the music onto the hard-drives of their computers) of the music. When Sony introduced its Betamax video tape recording device into the market in the mid-1970's, purchasers widely used them to make time-shift copies of broadcast television programming, among other things.[8] Courts have generally regarded time-, space-, and platform-shifting to be fair uses of copyrighted works, seemingly conforming the law on this question with consumer expectations.[9]

It is thus not surprising that consumers expect to be able to time-, place-, space-, and platform-shift as to digital media products, as well as to make backup copies.[10] Because digital technologies enable new flexibilities in ways to use and consume digital information, consumers have come to expect to be able to do more with digital media

---

[7] See U.S. Congress, Office of Technology Assessment, *Copyright and Home Copying: Technology Challenges the Law* 11-14 (1989), available at http://www.wws.princeton.edu/ota/disk1/1989/8910_n.html (reporting on surveys about personal use copying).

[8] Id. at 11-12.

[9] See Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442-43 (1984)(time-shift copying of broadcast television programming is fair use); In re Aimster, 334 F.3d 643, 652-53 (7th Cir. 2003) (noting space-shifting as a possible fair use); Recording Industry Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1079 (9th Cir. 1999)(space-shift copying "is a paradigmatic noncommercial personal use."); S. Rep. 102-294 at 86 (1992) ("[t]he purpose of [the Audio Home Recording Act] is to ensure the right of consumers to make analog or digital audio recordings of copyrighted music for their private, noncommercial use."). But see A&M Records, Inc. v. Napster, Inc., 114 F. Supp.2d 896, 915-16 (N.D. Cal. 2000) (rejecting argument that space-shifting through use of Napster's network was a fair use for purposes of assessing whether Napster had or was capable of substantial non-infringing uses). The implications of *Sony* for various forms of personal use copying are explored in Pamela Samuelson, *The Generativity of* Sony v. Universal: *The Intellectual Property Legacy of Justice Stevens*, 74 Fordham L. Rev. 1831 (2006).

[10] See, e.g., Technology Consumer Bill of Rights, available at http://digitalconsumer.org/bill.html; 17 U.S.C. § 117 (authorizing owners of software programs to make backup copies); Vault Corp. v. Quaid Software Ltd., 847 F.2d, 255, 266-67 (5th Cir. 1988) (affirming the making of software backup copies as a non-infringing use of copyrighted materials).

products than they could do with analog media products.[11] Consumers may, for example, want to link works together, format-shift, annotate them, tinker with them, remix, and mashup existing digital content and share their new creations with others.[12]

The use of TPMs often impairs personal uses that consumers expect to be able to make of digital content.[13] Copy-protected CDs, for example, may prevent platform-shifting and backup copying.[14] Nor can backup copies easily be made of DVD movies.[15] DVD movies, moreover, may not be playable on all DVD devices, insofar as region-coding interferes with this.[16] Even technical sophisticates may have difficulty playing DVD movies on computers which use Linux operating systems.[17] "Ripping" movies from DVDs to store them on computer hard-drives or to make mashups or remixes can likewise be thwarted by TPMs.[18] Online music stores may use TPMs to prohibit personal use sharing of music.[19] Consumer experiences with online music stores have often been confusing and dismaying because of the mismatch between personal use expectations and what the services enable and disable through TPMs.[20]

Consumer expectations about flexible uses of digital content are, moreover, not static; they evolve as advances in digital technologies and user innovations open up new possibilities for use.[21] One recent report has observed that consumers want and expect "flexible personal use—the ability to read, listen to, play, or watch a lawfully acquired

---

[11] See, e.g., Natali Helberger, et al., Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations 21 (Dec. 2004), available at http://www.indicare.org (giving examples of a wide array of personal uses that consumers expect to be able to make of digital media products).

[12] See, e.g., LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2003).

[13] See, e.g., Deirdre Mulligan, Aaron J. Burstein, & John Han, *How DRM-based Content Delivery Systems Disrupt Expectations of 'Personal Use,'* PROCEEDINGS OF THE 2003 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2004).

[14] Center for Democracy & Technology, Evaluating DRM: Building a Marketplace in a Convergent World 4 (Sept. 2006) (cited hereinafter as "CDT Report").

[15] Id. at 3.

[16] See, e.g., id.; Helberger et al., supra note xx, at 21.

[17] See, e.g., Declan McCullough, Teen Hacking Idol Hits New York, WIRED (July 20, 2000), available at http://www.wired.com/culture/lifestyle/news/2000/07/37650 (noting inability to play DVDs on Linux systems).

[18] CDT Report, supra note xx, at 3. In truth, the widespread availability of DeCSS has enabled many consumers to be able to make mashups from DVD movies, notwithstanding the ruling in Universal City Studios, Inc. v. Reimerdes, 111 F. Supp.2d 294 (S.D.N.Y. 2000)(holding DeCSS to be an unlawful tool under U.S. anticircumvention rules). See The Trailer Mash, http://www.thetrailermash.com/; Fabienne Serriere, *How-To: Convert a DVD for your iPod (with video) in Windows*, ENGADGET, October 14, 2005, http://www.engadget.com/2005/10/14/how-to-convert-a-dvd-for-your-ipod-with-video-in-windows/.

[19] CDT Report, supra note xx, at 8.

[20] Mulligan et al., supra note xx. Ken Fisher, *Musicload: 75% of customer service problems caused by DRM*, ars technical, March 18, 2007, http://arstechnica.com/news.ars/post/20070318-75-percent-customer-problems-caused-by-drm.html (noting tat Deutsche Telekom's Musicload, one of the largest online music stores in Europe, has come out strongly against DRM on account of its effects on the marketplace and its customers).

[21] CDT Report, supra note xx, at 7.

work in a manner and sequence of the consumer's own choosing."[22] This report recommends that "[a]s much as possible, DRM solutions should seek to allow users to interact with, excerpt, and expand on existing works in ways that are consistent with copyright law,"[23] although it recognizes that TPM systems used in commercially distributed digital content are thus far "not well adapted to the task of facilitating end user creation."[24]

Consumers of digital media products have other legitimate expectations as well, including expectations that their privacy and security interests will be respected. In the analog world, it was almost never possible for authors, publishers, and other commercial distributors of content to monitor consumer usage of copyrighted works. Once a consumer bought a book, an LP, or a videocassette of a movie, he or she could take it home to read, listen to, or watch free from surveillance by the content's developer.[25] Nor did consumers have any reason to fear that such products would impact their security from external attacks when they used such products in the privacy of their homes or offices. Although consumer expectations about privacy and security continue to be reasonable, it has become technically possible for these expectations to be thwarted through the embedding of technical measures that monitor usage of digital media products and/or render users' computers vulnerable to attack.[26] Privacy and security risks are, unfortunately, not the only unanticipated negative impacts that TPM systems may have for consumers.[27]

II. Consumer Harms Resulting From the Lack of Effective Notice of TPM Restrictions

The disparity between consumer expectations for digital media and the limitations imposed by TPMs presents a significant tension for the technology and entertainment marketplaces to mediate. This tension is further exacerbated when the marketplace suffers from imperfect information, namely when copyright owners or TPM vendors fail to adequately and effectively disclose the existence of the TPMs and the limits they impose.[28] This practice has resulted in various harms to the public that can generally be

---

[22] Id.
[23] Id. at 9.
[24] Id.
[25] See, e.g., Julie E. Cohen, *The Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 Conn. L. Rev. 981 (1996).
[26] CDT Report, supra note xx, at 10.
[27] Id. at 10 ("DRM may drain battery or processing power" or "modify[] the operation of device drivers for DVD burners").
[28] *Digital Media Consumer Rights Act of 2003*, 108th Cong., HR 107, 2003 (Committee Hearing) (Testimony of Hon. Rick Boucher) at 12. See also http://www.the-inquirer.com/default.aspx?article=27568; *Consumers, Schools and Libraries DRM Awareness Act of 2003*, 108th Cong., S 1621, 2003 (Sen. Brownback Floor Statements); *Consumers, Schools and Libraries DRM Awareness Act of 2003*, 108th Cong., S 1621, 2003 at 2 (noting increased confusion among industry, educational institutions, libraries, and consumers as access controls become more prevalent in the marketplace.). See also Julian Bajkowski, *Intel Quietly Adds DRM to New Chips*, DIGITAL ARTS, May 27, 2005, http://www.digitalartsonline.co.uk/news/index.cfm?NewsID=4915.

categorized into six areas: interoperability, privacy, security, lockout, anti-circumvention liability risks, and unforeseen changes and discontinuation of service.

A. Interoperability

One of the primary concerns arising from widespread use of TPM technology is the potential damage it can inflict on device and service interoperability. It is well documented that many of the advantages we enjoy from the networked economy result from compatibility between devices, formats, platforms, and applications.[29] These "network effects" increase the value of the overall network for each individual user. However, in order to maintain and exploit this value, devices and systems on the network must be sufficiently compatible to allow high quality data exchanges and high rates of information transfer at low transaction costs. TPMs, at their core, are designed to thwart information transactions by erecting barriers to data exchange. Thus, the tension between TPMs and the value of interoperable networks has proven to be a long-standing one with significant implications for technology law and policy.

This tension is exacerbated when notice of TPM restrictions is inadequate or insufficient. For example, Apple, Inc. has designed its iTunes Music Store ("iTMS") and iPod music player with proprietary TPM technology so that songs from iTMS will only play on the iPod and not on other portable digital music devices. In addition, it has designed the iPod so that it will only accept music files from the iTunes store, or in the non-TPM MP3 format. For vendors of other music devices and other TPM-encoded music files, this presents a problem of interoperability. Users of iTMS and the iPod are precluded from interoperating with other digital music devices and vendors. Yet nowhere on Apple's website or on its products is there any indication to the purchaser of such restrictions or the exact limitations they impose.[30] This lack of notice, and the lack of interoperability it causes, has lead to several public inquiries into the issue with a strong focus on consumer protection.[31]

Another example occurred in 2005 when Sony BMG Music distributed thousands of musical CDs that contained TPM software designed to embed itself in the Windows Operating System where it could monitor and restrict use of the musical files from the CD.[32] While the CDs were labeled with a short "Copy Protected" notification, there was

---

[29] See Samuelson and Scotchmer, The Law and Economics of Reverse Engineering; Lemley and McGowen, The Law and Economics of Internet Norms (discussing positive influence of norms on Internet network effects).

[30] See http://www.apple.com/legal/itunes/us/service.html and http://www.apple.com/legal/itunes/us/sales.html (noting that use of the iTMS requires "a compatible device" and may require the use of an "authorized digital player" but does not specify or define that term). Compare http://www.apple.com/legal/itunes/us/sales.html (noting that in regard to iPod Games, the Games "are compatible only with 5th generation (video) iPods. The Games will not function on any other device, including your personal computer.").

[31] See Stephen Withers, *Europe continues push for iTunes interoperability*, ITWire, March 12, 2007, http://www.itwire.com.au/content/view/10368/53/; Jo Best, Law to make iTunes compatible with Microsoft?, Silicon.com, April 7, 2005, http://management.silicon.com/government/0,39024677,39129365,00.htm.

[32] See Mulligan & Perzanowski, supra note 6; http://www.eff.org/IP/DRM/Sony-BMG/guide.php.

little clarification as to what this term meant, especially in terms of exactly what uses were restricted and how. For example, on the back of the "XCP" protected CDs, it would often list which platforms one could play the music on, but not which applications or devices would play them. It also simply summarized the user's right to make backups or mixed playlists as "limited copies" without any explanation of how many copies, on what media, and what other computers would be able to play them.[33] Again, because this notice was inadequate, users were denied sufficient information to understand the limits on interoperability that Sony BMG had imposed upon them with its XCP protected CDs.

These types of restrictions often surprise, frustrate, and confuse consumers, especially when they are applied to media consumers expect to come without such limits. In such circumstances, TPMs place unwarranted burdens on consumers as well as on retailers and manufacturers of computers or consumer electronics devices to whom consumers may complain about frustrations arising from use of TPM products or services without realizing that the restriction had been imposed by the maker of the digital media product or service rather than the manufacturer or seller of the equipment in which the product or service was being played.

Another example is DVD region codes. Under the technological system designed by the DVD Copy Control Association, the industry coalition that controls the standards for DVD production and playback, DVDs are often encoded with a numerical identifier that corresponds to a specific geographic region in which that the DVD is authorized to play. So, for example, if one were to purchase a DVD with a European Region Code (2) while on vacation in France, that DVD would not play on most U.S. manufactured DVD players, which only play DVDs with a U.S. Region Code (1). While pervasive, most DVD manufacturers fail to adequately disclose this restriction to consumers, either at the point of sale, or in the accompanying literature for the DVD. Consumers who then travel or move from one region to another risk unfair surprise in finding that media they have legitimately purchased does not work with equipment in their new home.[34] Again, without proper notice, consumer may believe that this is a problem with the DVD they bought or their DVD player instead of a TPM restriction imposed on them by the copyright holder in conjunction with the DVD Copy Control Association.

Such problems have also extended beyond DRM and into other TPM arenas. For example, Hewlett-Packard has started "region coding" its printers to match only certain printer cartridges bought in the same region of the world as the printer.[35] If the "wrong" cartridge is inserted, the printer refuses to print, even though it is functionally identical to the "approved" cartridges.[36]

---

[33] Id.

[34] A similar problem exists within the iTunes Music Store TPMs as well. There have been reports of Apple using TPMs to limit access to particular music files based on a user's country of origin without adequate and effective notice to users of these limitations. *See* Paul Collins, *jTunes: The Insanely Great Songs Apple Won't Let You Hear*, SLATE, http://www.slate.com/id/2158151/.

[35] David Pringle and Steve Stecklow, Electronics With Borders: Some Work Only in the U.S., Wall Street Journal, January 17, 2005; Page B1.

[36] Id.

B. Privacy

In addition to a lack of disclosure about use restrictions, Some TPM-protected products and services have been designed to monitor consumer usage. These activities often happen at a very deep technical level of the consumer device or product and thus consumers may not be aware of the existence or extent of such monitoring or of uses that may be made of personal data collected through such monitoring.[37] This poses the harm of invading users' privacy interests and exposing them to unwanted surveillance or profiling.

For example, Blizzard Entertainment makes a very popular online videogame called "World of Warcraft"[38] in which millions of users log in to Blizzard's servers and interact. In an effort to control cheating and "hacks," Blizzard distributed an "update" to all of its users to install on their personal machines that included a TPM called "The Warden."[39] This TPM monitored each user's computer, including any active window, to make sure no "unauthorized programs" were running while the game was in play.[40] If any such programs are detected, The Warden presumably shuts down the World of Warcraft application and notifies Blizzard corporate headquarters to suspend the user's account.[41]

While many users were happy that this kept other players from cheating in the game, others were upset by the failure of Blizzard to disclose the privacy implications of the TPM, which included sometimes scanning email addresses and website URLs.[42] While Blizzard does disclose some general details about The Warden in its End User License Agreement, there are very few specifics about how and what programs are restricted from running and what information is actually collected and/or sent back to Blizzard.[43] Similar complaints were lodged against Sony BMG after evidence emerged that its CD Protection software also sent information about consumer usage over the Internet back to the company that made the TPM for Sony[44] and about the now-defunct Digital Video Express (Divx) format, which allegedly collected information on every movie a user would watch.[45]

These examples represent just the tip of the iceberg to come for potential privacy-invasive TPMs.[46] Makers of digital media products or services who deploy such systems

---

[37] See Bajkowski, supra note 28.
[38] www.worldofwarcraft.com
[39] http://news.bbc.co.uk/1/hi/technology/4385050.stm
[40] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019240; http://www.schneier.com/blog/archives/2005/10/blizzard_entert.html.
[41] Id.
[42] Id.
[43] http://www.worldofwarcraft.com/legal/eula.html (Section 5: Consent to Monitor).
[44] http://www.freedom-to-tinker.com/?p=925.
[45] Dan Fost, "Divx's Death Pleases Opponents", San Francisco Chronicle, June 18, 1999.
[46] See generally Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Lee A. Bygrave, "Digital Rights Management and Privacy - Legal Aspects in the European Union" in Eberhard Becker et al., eds., Digital Rights Management - Technological, Economic, Legal and Political Aspects (New York:

must give consumers effective notice of any such monitoring and of uses that they intend to make of such data. Fair information practices should also be followed in collection and processing of such data.[47]

C. Security

Another category of TPM harm is security. When TPMs exert control over computers and devices to limit access or functionality to users, they are in essence overriding the user's choices and decisions about how to operate their technology.[48] Users who have some moderate level of technical skill may seek to disable these TPMs, so many TPM makers seek to create measures that are "resistant" to user tampering or that hide themselves from the user so that the user cannot locate or disable them. This design approach, however, opens up the TPM to certain kinds of exploitation. Namely, makers of malicious software such as viruses, spyware, or spam-generating programs may seek to use these attributes of the TPM to hide their own programs from the user or to thwart the user's ability to seek out and remove dangerous files from their systems.

This was the case with the Sony XCP Copy Protection program. In order to avoid detection (and subsequent removal) by users, the XCP TPM used a well-known computer exploit technique called "a rootkit" to hid itself in the registry files of the Windows Operating system, pretending to be one of the thousands of essential components that Windows needs to operate correctly.[49] By doing so, it sought to evade most attempts to detect it and thus be allowed to monitor use of the digital music files on the Sony CDs without interference from the user. However, because of certain design flaws, XCP was also susceptible to being taken over by various malicious programs. These programs then used XCP's evasion methodology to avoid detection by anti-virus and anti-spyware programs running on most Windows operating systems. The malicious software could then, in turn, be used to infect the host computer where the Sony CD had been inserted and spread to other computers via network connections undetected.

By failing to disclose (and, in fact, actively concealing) the existence of the XCP TPM, Sony not only mislead its customers about the limits and restrictions of the copyrighted content they purchased but also exposed them to significantly increased risks regarding malicious software and computer security. Adequate and effective disclosure of these risks would not have necessarily prevented the full extent of the harm consumers suffered, but it would certainly have helped cautious consumers avoid installing the software in the first instance. We fear that this example is just the beginning of what is

---

Springer, 2003); Ian Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" 2 Info., Comm. & Ethics in Society 87 (2004).

[47] See European Commission's Data Protection Working Party Report (noting "an increasing gap between the protection of individuals in the off-line and on-line worlds, especially considering the generalised tracing and profiling of individuals.")

[48] http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

[49] See Mulligan & Perzanowski, supra note 6.

sure to be a pattern of security-induced problems for users stemming from TPM technology.[50]

D. Lockout

Another area of harm is lockout. Similar to the concerns expressed over interoperability, lockout concerns arise when TPMs are used to prevent users from purchasing alternative replacement parts or using independent service vendors other than those associated with the original TPM-encoded product. There have been numerous cases of this in recent years. For example, in the case of *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004), a garage door opener ("GDO") manufacturing company attempted to use a TPM (and Section 1201 of the DMCA, discussed *infra*) to ensure that its customers could only use its proprietary electronic GDO remotes to open their garage doors. This was accomplished via a set of rolling codes that were synchronized between the remotes and the openers. At the time of purchase, however, Chamberlain failed to disclose the extent of this technological lock-in to its customers. It was, ironically, only after an after-market GDO remote competitor, Skylink, reverse engineered the code system and offered a competing universal GDO remote, that Chamberlain disclosed the existence of the TPM and its restrictions via a lawsuit filed against Skylink under Section 1201 of the DMCA. Such use of TPMs significantly raises the switching costs for consumers, thus creating inefficiencies in the marketplace for such technologies and putting consumers are risk of being stuck with inadequate or debilitating purchases. Similar situations have also arises in the context of printers and printer ink cartridges,[51] magnetic tape library storage systems,[52] car repair diagnostic software, online videogame servers[53] and digital cameras film files.[54]

a. Legal Risks

In addition to the problems that lurk for consumers and competitors regarding interoperability, privacy, security, and lockout, there are also legal risks associated with inadequate notice of TPMs. While there are clearly cases where people are on notice that TPMs are employed and thus, presumptively aware that Section 1201 of the DMCA protects against circumvention of those technologies, the history of DMCA enforcement efforts also shows that there are many gray areas where such clarity is not present.[55] Such

---

[50] http://www.theregister.co.uk/2005/01/13/drm_trojan/

[51] Lexmark v. Static Control Corp.

[52] StorageTek v. CHE (Fed. Cir.)

[53] See Davidson v. Internet Gateway (using undisclosed TPM to lock videogames into vendor's proprietary servers); MDL Industries v. Blizzard, Inc. (Declaratory Judgment Action against videogame company Blizzard for legal threats over undisclosed TPM that prohibits the running of third-party client-side applications); Ed Foster, *Steaming about DRM*, http://www.infoworld.com/weblog/foster/2005/01/04.html (describing videogame company Valve's attempt to restrict use of videogame to a single computer using undisclosed TPM).

[54] *See* Digital Photography Review, *Nikon responds to RAW WB concerns*, http://www.dpreview.com/news/0504/05042203nikonnefresponse.asp (discussing allegations that Nikon encrypts certain "white balance" data when a user takes a picture with its camera but does not allow that data to be transferred when the user converts the RAW image file to a competing format).

[55] See Generally R. Anthony Reese, Symposium: The Law and Technology of Digital Rights

ambiguity and obfuscation help neither those who wish to legitimately prevent circumvention of copyright-protecting TPMs nor customers and competitors who wish to expand legitimate functionality and usage without running afoul of Section 1201's prohibitions.

For instance, in Lexmark v. Static Control Corp., a printer manufacturer sued a competing maker of aftermarket ink cartridges under the DMCA because it claimed that by using trafficking in unauthorized cartridges that activated the printer engine software program inside Lexmark printers, the defendant was circumventing protections on accessing that program under the DMCA. While the appellate court eventually reversed a lower court order and ruled against Lexmark for, among other things, failing to "effectively control access" to the printer program (for example by encrypting it), [56] this was a clear example of a situation where the defendant had no notion that Lexmark sought to protect its printer program in this way, let alone that it would seek to use Section 1201 to enforce prohibitions against accessing the program. It is also worth noting that while this case concerned the trafficking provision of 1201(a)(2), Lexmark's theory of circumventing its TPM could have just as easily been brought against printer owners who had purchased and used Static Control cartridges in their Lexmark printers.

A similar lack of clarity emerged in the case of *Chamberlain v. Skylink*. As noted above, in that case, the maker of a GDO device sued a manufacturer of universal GDO remotes under Section 1201 for trafficking in devices that allowed legitimate purchasers of Chamberlain GDOs to program the remotes for compatibility with Chaimberlain devices. This theory was premised on the notion that since the opener ran a software program when the remote activated it, the code used by the opener was a TPM that controlled access to the code and which the defendant's remote circumvented. In both the lower court and at the appellate level, the judges reviewing the case expressed serious concerns over what the TPM at issue was and how the DMCA applied to it. What did it mean to "access" the software program at issue? What did the program protect? Was opening the garage door an unauthorized access of a copyrighted work (the software program) even though the user might be completely unaware of the program's existence? The Federal Circuit Court of Appeals eventually ruled that because there was no "nexus" between the user's actions and any potential copyright infringement, there was no Section 1201 violation, but the opinion suggests that issues of notice and fundamental unfairness supported its reasoning for limiting the DMCA's application in this case.

In the case of Princeton Computer Science Professor Ed Felten v. the Recording Industry Association of America, similar ambiguity and uncertainty reigned, this time with a chilling effect on First Amendment speech. In that case, Professor Felten and his students entered an authorized challenge to "crack" a new version of DRM for music files

---

Management: Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?, 18 Berkeley Tech. L.J. 619 (2003)

[56] Note that Judge Merritt's concurrence suggests that there should never be an instance where the DMCA should prevent competition in such a market while the majority only ruled against Lexmark under the current facts.

[58] See. e.g., Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 Science 2028 (Sept. 2001).

called "SDMI." After doing so and scheduling to present a paper on the implication of their work, Felten received a threat letter from the RIAA claiming that by publishing his results, he would be trafficking in a circumvention device under Section 1201.[58] After Felten filed for a declaratory judgment of non-circumvention, the RIAA mooted the suit. However, the uncertainty of whether and how future scientific research could violate the DMCA remained.

In the case of Davidson & Associates v. Jung, the parent company of Blizzard Entertainment sued a group of open source developers for creating an interoperable game server (called the "BNETD" server) to play with Blizzard's Warcraft, Starcraft, and Diablo videogames. In creating the BNETD server, the programmers specifically avoided any encryption protocols or authentication mechanisms that the client tried to send to the server in an effort to avoid Section 1201 liability. However, both the district court and the appellate court found that, notwithstanding this intent, the developers had in fact made themselves liable under 1201 because they did not respond to the encrypted data appropriately. The data, as it turns out, contained a unique serial number intended to prevent unauthorized copying. By ignoring this valuable information, even in good faith, both courts found the developers were circumventing Blizzard's TPM and thus liable even though they had no intention of furthering infringement of Blizzard games. Notably, there was no indication in the Blizzard End User License Agreement or Terms of Use that the TPM existed or what limitations, either technologically or legally, it was meant to impose.

Yet another example of potential legal liability from unclear TPM notice arose in the case of the Sony Aibo robotic dog. In 1999, Sony released the metal programmable pet into the market. Sooner thereafter, an enterprising group of computer coders discovered how one could reprogram the dog to do any number of creative (albeit unauthorized) maneuvers, e.g., jazz-inspired dance sequences.[59] In 2001, Sony sent a cease-and-desist letter to a website called "aibohack.com" demanding that it stop distributing code that was retrieved by bypassing the copy prevention mechanisms of the robot.[60] After much protest, Sony backed off from this position and allowed non-commercial reprogramming of the robot by its customers; however, the lack of clarity surrounding the limits of the Aibo TPM and the associated legal risks left their mark.

Finally *Techmo v. Ninja Hacker* was yet another example of unintentional legal exposure resulting from inadequate TPM notice.[61] In that suit, Techmo sued the users and host of a forum where players of popular Techmo games traded "skins" – graphical outfits used by the players in the games to designate skin color, uniforms, and other attire. In its complaint, Techmo alleged that in order to access and modify the skins, users needed to modify their Microsoft Xbox systems to allow interaction with an external computer hard drive. According to Techmo, this "unauthorized access" circumvented the

---

[59] Sony Uses DMCA to Shut Down Aibo Hack Website, Slashdot, Oct. 27, 2001, available at http://yro.slashdot.org/article.pl?sid=01/10/28/005233.

[60] Id.

[61] Kevin Poulsen, Hackers Sued for Tinkering with Xbox Games, Security Focus, Feb. 9, 2005, available at http://www.securityfocus.com/news/10466.

protections on the game and violated Section 1201. Because the case settled soon after filing, there is no way to know how a court would have ruled on the legal merits of this claim, but it is fair to surmise that neither the users nor the host of the forum had adequate notice that Techmo was using the XBOX hardware as a TPM to restrict access to its game skins.

F. Changing Terms and Discontinued Service

Additional harms occur when consumers discover that TPM-protected products or services they have purchased have been programmed to enable alteration of functionality without notice of the changes or an opportunity to object or to obtain a remedy for the lower value of the altered product or service.

For example, in 2003, Intuit offered an "activation feature" to purchasers of its popular TurboTax software product that required users to register the product with a specific computer prior to activation.[62] Once registered, the software refused to let the user print their tax return or file it with the IRS electronically from any other computer without the purchase of another license or reactivation of the software.[63] Needless to say, this caused severe frustration for consumers who were not aware of the feature when they purchased the software product.

Apple Computer has instituted similar practices in its iTMS DRM, changing the number of copies and accessible computers available to past, present, and future users at least three times since they launched the program in 2001. In fact, according to the iTunes Store Terms of Service, Apple expressly reserves the right to change the "Usage Rules" and other limits on the music purchased from the service at any time without prior notice to consumers.[64] This has also been the case with personal video recorders like TiVo as a result of deals these companies have made with TPM providers like Macrovision and content providers like HBO.[65]

Such situations are even more troublesome when companies that tether their content to TPMs discontinue service or go out of business. For example, when the Divx video disc format was available, one could purchase access to various movie titles for limited periods of time, such as 48 hours. One could also purchase lifetime access for significantly more money. When the company that ran Divx went out of business, [66] however, it was unclear what would happen to those "lifetime" purchases. Would they be honored? Or would consumers lose access to the content even though they had paid past the lifetime of the company?

---

[62] http://www.pcmag.com/article2/0,1895,821308,00.asp

[63] Id. See also Ed Foster, Steaming About DRM, InfoWorld, January 4, 2005 (noting personal problems activating Christmas video game gift for his eight-year-old son).

[64] See http://www.apple.com/legal/itunes/us/service.html. Notably, this practice has been objected to by at least one European Consumer Ombudsman. See http://www.forbrukerombudet.no/index.gan?id=11032467&subid=0.

[65] http://www.wired.com/wired/archive/12.11/view.html?pg=3

[66] See, e.g., Stephanie Miles, CNET News, Behind the Death of DivX Were Angry Customers, available at http://news.com.com/2100-1040-227248.html.

A similar situation recently arose involving Sony BMG's "Sony Connect" service. When the service launched in 2006, it included TPMs that monitored user usage to ensure compliance with certain rules about access and availability of songs. However, recently, there was a news report that suggested Sony would be shutting down the service, potentially leaving thousands of music fans and customers without access to the content they have legitimately downloaded.[67] Other subscription services such as Rhapsody and Napster raise the same issues about consumer rights.

III. The Notice Problem Posed by TPMs Has Been Noticed

Several European reports have emphasized the need for transparency when technical restrictions are embedded in mass-marketed digital content.[68] An especially thorough report on transparency and other consumer protection issues posed by TPM'd digital content is a report entitled "Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations," published by a multi-institutional study group known as "The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe" (aka INDICARE).[69] The INDICARE Report considers five major categories of consumer protection concerns posed by these technologies: "(1) fair conditions of use and access to digital content, (2) privacy, (3) interoperability, (4) transparency, and (5) various aspects of consumer friendliness."[70] This report discusses several EU directives that have a bearing on disclosure of TPM restrictions,[71] as well as German legislation and French caselaw that require content owners to give consumers adequate notice about TPM restrictions.[72]

Another European report on DRM technologies was issued in the UK by the All Party Parliamentary Internet Group (APIG); it states that the group had reached "considerable consensus on the principle that consumers should be aware of what they are purchasing."[73] More specifically, there was agreement that "all CDs should in the future come with a prominent label saying 'you are not permitted to make any copies of this CD for any reason'" before selling copy-protected CDs.[74] Full disclosure should also be given, says APIG, if technically protected CDs will not play on all devices, will not be

---

[67] http://www.paidcontent.org/entry/419-sony-connect-to-close-music-video-services-focus-on-servicing-playstati

[68] See, e.g., All Party Parliamentary Internet Group, Digital Rights Management: Report of an Inquiry by the All Party Internet Group (June 2006) (cited hereinafter as "AIPG Report"); European Consumer Law Group, Copyright Law and Consumer Protection, ECLG/035/05 (Feb. 2005), available at http://www.europeanconsumerlawgroup.org (cited hereinafter as "ECLG Report"); and The Gower Review of Intellectual Property (Dec. 2006), available at http://www.hm-treasury.gov/uk/media/583/91/pbr06_gowers_report_755.pdf (cited hereinafter as "Gower Report").

[69] Helberger, supra note xx.

[70] Id. at vi.

[71] Id. at 51-55.

[72] Id. at 53 (discussing German labeling requirement for TPM'd content), 55 (discussing a French judicial decision finding the lack of labeling of a copy-protected CD as a misleading practice).

[73] AIPG, supra note xx, at 15.

[74] Id.

playable if the users' device breaks or is stolen, and will record identity information about users.[75] It went on to recommend that the British Office of Fair Trading (OFT) "bring forward appropriate labeling regulations so that it will become crystal clear to consumers what they will and will not be able to do with digital content that they purchase."[76] A second British report, The Gower Review of Intellectual Property, similarly recommended labeling of technically restricted digital content to protect legitimate consumer interests and expressed concern about the risks that TPMs could be used for socially undesirable purposes.[77]

The first American policy initiative aimed at addressing consumer concerns about inadequacy of notice as to TPM-protected copyrighted works was Rep. Rick Boucher's bill, H.R. 107, introduced in January 2003, which would have amended the FTC Act to give the agency authority to regulate labeling of copy-protected CDs of recorded music.[78] Among its proposed "findings" was that the introduction of copy-protected CDs "has caused consumer confusion and placed increased, unwarranted burdens on retailers, consumer electronics manufacturers, and personal computer manufacturers responding to consumer complaints."[79] If the recording industry was going to use copy-protection systems for CDs, it needed to be "responsible for providing adequate notice to consumers about restrictions on the playability and recordability of 'copy-protected compact discs.'"[80] The bill proposed to authorize the FTC to develop standards for appropriate labeling of such CDs.[81] After promulgation of these standards, recording companies would be required to comply with those standards.[82] Thereafter, it would be an unfair trade practices for firms to introduce into the market un- or mislabeled copy-protected CDs or to advertise such CDs unless the copy-protection feature was disclosed.[83] The bill would have also required the FTC to submit a report to Congress about the effects of the legislation.[84]

Senators Brownback and Wyden introduced similar legislation, although their bills were more general in addressing disclosure issues as to technically protected digital media products.[85] The Brownback bill would have authorized the FTC to establish an advisory committee to inform the Commission "about the ways in which access control technology may affect consumer, educational institution, and library use of digital media

---

[75] Id.
[76] Id.
[77] Gower Report, supra note xx, Recommendation 16 (need for labeling), sec. 4.8 (harmful uses of TPMs). "In the event that companies use DRMs to create market power, damage users' software or invade their privacy, the Review recommends that the Office of Fair Trading undertake investigations." Id. at sec. 4.107.
[78] H.R. 107, 108th Cong., 1st Sess. (2003).
[79] Id., sec. 2(1).
[80] Id., sec. 2(2).
[81] Id., sec. 3 (subsec. (d) of proposed sec. 24A of the FTC Act).
[82] Id., (subsec. (b) of proposed sec. 24A of the FTC Act).
[83] Id.
[84] Id., sec. 4.
[85] S. 692, 108th Cong., 1st Sess. (2003)(Wyden bill); S. 1621, 108th Cong., 1st Sess. (2003)(Brownback bill).

products based on their legal and customary uses of such products," as well as about consumer awareness about the use of such technologies in digital media products.[86]

A year after the effective date of the legislation, the Brownback bill would have charged the FTC with promulgating regulations to require notice about technically protected digital media products unless their makers had "established [and implemented] voluntary rules for notice and labeling of access controlled or redistribution controlled digital media products" insofar as these technologies would affect "their legal, expected, and customary uses" of these products.[87] Thereafter it would be illegal to sell technically restricted digital media products without "clear and conspicuous notice" that "identifies any restrictions the access control technology or redistribution control technology used in or with that digital media product is intended or could reasonably be foreseen to have on the consumers', educational institutions', or libraries' use of the product."[88] The FTC would also be required to report to Congress on the deployment of technically protected digital media products, on the extent to which such products allowed customers to engage in lawful uses, and the extent to which notices of technical restrictions were being effective.[89]

The Wyden bill had the same goal as the Brownback bill—to give consumers effective notice about technical restrictions built into digital media products[90]—but had a broader perspective on the use of TPMs and sought to accomplish the goal somewhat differently. It recognized that media firms were embedding TPMs in digital media products in order to protect these products from illegal copying and that deployment of TPMs "could help promote a competitive digital marketplace in which consumers have a broad range of choices and media businesses can pursue a variety of business models."[91] However, it also recognized the legitimacy of consumer expectations about their ability to use and manipulate digital content "for reasonable, personal, and noncommercial purposes."[92]

The Wyden bill identified three significant risks posed by deployment of TPMs in digital media products: (1) that TPMs "could have the side effect of restricting consumers' flexibility to use and manipulate such content for reasonable, personal and noncommercial purposes," (2) that use of TPMs "could unfairly surprise consumers by frustrating their expectations concerning how they may use and manipulate digital content they have legally acquired," and (3) that deployment of TPMs "could result in greater market power for the holders of exclusive rights and reduce competition, by limiting the ability of unaffiliated entities to engage in lawful secondhand sale or distribution of such products."[93]

---

[86] Id., sec. 4(a).
[87] Id., sec. 4(d).
[88] Id., sec. 4(c).
[89] Id., sec. 7.
[90] The short title of the Wyden bill was the "Digital Consumer Right to Know Act." S. 692, supra note xx, sec. 1.
[91] Id., sec. 2(a)(2)-(3).
[92] Id., sec. 2(a)(1).
[93] Id., sec. 2(a)(4)-(6).

To guard against unfair surprise, the Wyden bill called for the FTC to develop rules to implement the following disclosure requirement:

> If a producer or distributor of copyrighted digital content sells such content or access to such content subject to technological features that limit the practical ability of the purchaser to play, copy, transmit, or transfer such content on, to, or between devices or classes of devices that consumers commonly use with respect to that type of content, the producer or distributor shall disclose the nature of such limitations to the purchaser in a clear and conspicuous manner prior to such sale.[94]

The bill proposed to authorize the FTC to "prescribe different manners of disclosure for different types of content and different distribution channels,"[95] and also to make exceptions to the notice requirement as to uses of TPMs "that are sufficient unusual or uncommon that the burdens of prior disclosure would outweigh the utility to consumers" or "that have no significant application for lawful purposes."[96]

The Wyden bill gave examples of TPM limitations that should trigger the disclosure requirement, including limits on users' ability to make time-shifting or space-shifting copies of audio or video content, to make back-up copies or excerpts for such purposes as criticism or commentary, and to transfer one's copy to others.[97] It would have required the FTC to issue an annual report to Congress to review the effectiveness of its notice regulations and to advise Congress about "whether changes in technology or in consumer practices have led to new, legitimate consumer expectations concerning specific uses of digital information or entertainment content that would result in consumers' suffering unfair surprise if a technology were to limit those uses without prior notice."[98]

The Wyden bill was explicit about its purposes: to ensure that consumers would have sufficient notice of technical restrictions so that they could "factor this information into their purchasing decisions" and to ensure there was a "strong market-based incentive for the development of technologies that address the problem of unlawful reproduction and distribution of content in ways that still preserve the maximum possible flexibility for consumers to use and manipulate such content for lawful and reasonable purposes."[99]

Even without such legislation, the FTC has authority to regulate unfair and deceptive practices, such as those that may arise from the misuse of TPMs in digital media products. The FTC charged Sony BMG with violating the FTC Act because of its

---

[94] Id., sec. 3(b)(1).
[95] Id., sec. (b)(2).
[96] Id., sec. (d).
[97] Id., sec. (c)
[98] Id., sec. (e).
[99] Id., sec. (b).

copy-protected CDs covert installed software on purchasers' computers[100] Sony BMG's failure to give proper notice of the installation of this software was one of the key problems requiring a regulatory response.[101] The FTC's settlement agreement with Sony BMG requires it to give "clear and conspicuous notice" before installing software on user hard-drives or limiting the usability of the digital content on users' computers. [102]

In a recent address discussing the role of consumer protection in regulating TPMs, FTC Commissioner Thomas Rosch observed that the Commission "has long insisted that consumers be given adequate notice of the terms on which goods or services are being made available to them, including any material limitations."[103] The FTC had, for example, taken action against the makers of certain wireless devices to require them to inform consumers that purchasing such devices would not provide access to the Internet, and that they had to buy additional products or services to obtain such access.[104] "Likewise, with DRM, *any material limitations of use rights* (including, but not limited to, technological limitations such as an inability to use the media on another platform) *must be clearly and conspicuously disclosed* before a sale of these media is made."[105] This suggests that Sony BMG may only be the first, but by no means the last, deployer of technically protected digital content whose disclosure practices vis-a-vis TPMs will be subjected to regulatory scrutiny by the FTC.

While not expressly calling for regulation to require disclosure of TPMs, a recent report issued by the Center for Democracy and Technology (CDT) emphasizes the importance of transparency concerning the use of TPMs in mass-marketed digital media products and devices.[106] "With sufficient information, competition between different DRM offerings can help promote a marketplace for digital media products that is diverse and responsive to reasonable consumer expectations."[107] Among the questions it poses as to transparency are these: "Are users given fair notice of product characteristics that may be relevant to them? Is notice provided in a manner that is sufficiently prominent and understandable?...Is notice provided at appropriate times?"[108] Disclosure is most necessary "where DRM-equipped products will not work with certain devices or in

---

[100] Complaint, In the Matter of Sony BMG Music Entertainment, available at http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf.

[101] See J. Thomas Rosch, *A Different Perspective on DRM*, 22 Berkeley Tech. L.J. (forthcoming 2007).

[102] In re Sony BMG Music Entertainment, FTC File No. 062 3019 (posted for public comment Jan. 30, 2007)(consent decree), available at http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf

[103] Rosch, supra note xx, at [3].

[104] Id., at [3-4] (citing to three consent orders in such cases).

[105] Id. at [4] (emphasis added). In his view, consumers of CDs "have the right to expect that their CDs come without copying limitations and to expect that the music on those CDs will play on any device." Id. at [3]. In accordance with this view, Sony BMG could have been charged with unfair and deceptive practices for selling copy-protected CDs without notice, even if it had not also caused rootkit software to be installed on users' computers.

[106] CDT Report, supra note xx, at 2. This report offers four metrics for evaluating DRM products and services: transparency, effects on use, collateral impacts, and purpose and consumer benefit. Id.

[107] Id. at 1.

[108] Id. at 6. Notice may need to be given not only at the time of the user's first encounter with the product, but also at later times as the user interacts with the product or services related to it. Id. This is especially important if the rights holders offer consumers "upgrades" that, for example, impair compatibility or if the terms of service change in a material way. Id. at 7.

certain configurations,"[109] but is always warranted "when DRM will cause a product's function to deviate significantly from mainstream consumer expectations."[110]

The CDT report recognizes that transparency will be thwarted if content producers bury material information about TPM restrictions deep in long license documents that are available to consumers only after they have purchased the product.[111] The report also points to some potential negative impacts of TPMs in digital media products, such as harms to user privacy and anonymity interests insofar as the TPM is programmed to "phone-home" usage information and harms to competition insofar as TPMs are used to lock users into a particular family of products.[112] CDT urges "[p]roduct reviewers, consumer advocates, and computer security experts [to] be alert for DRM behaviors that pose security risks" such as those caused by the Sony BMG rootkit software.[113]

The notice problem with TPMs having thus been noticed on both sides of the Atlantic, it is time to consider in greater detail the policy options for addressing this problem.

IV. A Spectrum of Policy Options to Address the Notice Problem

While Part III identified some of the policy options for addressing the problems posed by inadequate or no notice of TPMs that frustrate consumer expectations, we think it is most useful to consider a range of options along a spectrum from least to most regulatory in character, and then to assess the pros and cons of each option.

The least regulatory option is to trust, as we believe copyright industry groups will prefer, that the market can effectively respond to consumer needs for disclosure of TPMs in digital media products. A second, and next lightest, regulatory option would be for the FTC or other consumer protection agencies at the state level to work with copyright industry groups and those concerned about the adequacy of notice as to TPMs so that the industry undertakes to develop self-regulatory measures to address the TPM notice problem. It is consistent with these first two options for the FTC and similar agencies at the state level to act promptly and decisively when deployers of TPMs deceive consumers or treat them unfairly, as happened in response to the Sony rootkit incident.[114]

A third option is for the FTC to undertake a thorough investigation about the uses of TPMs in digital content and the extent to which content owners are disclosing (or not) the capabilities of TPMs that are relevant to consumer decision-making. This investigation would likely produce a report that would recommend whatever legislative

---

[109] Id. Region-coding restrictions in DVDs, for example, should be disclosed to consumers before they purchase copies that may not work on their machines. Id.
[110] Id.
[111] Id. at 7.
[112] Id. at 9-10.
[113] Id. at 10.
[114] Mulligan & Perzanowski, supra note xx.

or administrative or self-regulatory measures that the investigating agency thought were warranted.

A fourth option would be for Congress to enact legislation akin to the Wyden bill that mandates disclosure of TPMs and gives guidance about some of the functional characteristics (e.g., interoperability across devices) that are of particular legislative concern. As with the Wyden bill, it could leave to the considered judgment of the FTC the decision about what notice should be given in what form as to what products.

A fifth option would be to mandate not only that notice must be given about TPM restrictions or other relevant technical features, but would also regulate concerning certain features in TPM systems, such as the monitoring of usage. In order to give content developers meaningful incentives to comply with notice requirements, Congress might condition the ability of digital media firms to take advantage of the anti-circumvention rules that protect TPMs used by copyright owners to protect their rights in digital works on their willingness to comply with notice and/or substantive requirements as to TPMs.

Each of these options is discussed below.

A. Trust the Market

Americans generally believe that the market is, or at least can be, an effective means of protecting consumers, especially when there is clear and conspicuous information disclosure and competition among vendors of particular products. If products made by vendor A do not comport with consumer expectations or embody defects likely to harm consumers, vendors B and C will generally be able to lure customers away from A toward their more superior or more consumer-friendly products. Comparative advertising, consumer product ratings services, and news media coverage of consumer product issues are among the institutional mechanisms of American markets that contribute to consumer awareness about products and their feature sets. These mechanisms are especially important as to product features that are difficult to discern from pre-purchase visual inspections of the products.

However, consumers of digital media products cannot generally detect TPMs by looking at these products prior to purchasing them; indeed, they may not even learn of the TPMs in the course of ordinary use of the product.[115] Vendors of digital content have incentives to make the technologies complex, difficult to reverse engineer, and highly proprietary trade secrets in order to inhibit circumventions of the TPMs that would undo the protections they provide.[116] Content owners are also understandably reluctant to

[115] The packaging of DVD movies, for example, does not mention that encryption software installed on the DVD disks prevents backup copying, extraction of fair use snippets, and skipping through commercials. Consumers may only find out about the TPM restrictions when they try to use the DVD movie in a different way than merely playing it to watch the movie. CDT Report, supra note xx, at 3.

[116] See, e.g., Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 Hastings L.J. 777, xx (2007) (discussing the complex licensing regime that the DVD Copy Control Ass'n has used to maintain secrecy for encryption keys used to protect DVD movies).

disclose TPM restrictions, such as the copy-protection software embedded in some CDs, because consumers do not particularly like TPMs.[117] Consumers who have a choice among digital products, some of which have TPMs and some of which do not, are likely, all other things being equal, to choose the non-TPM'd product.[118] Similarly, consumers are likely to prefer less restrictive TPMs over more restrictive ones, given information relevant to this choice, which helps to explain why Apple's iTunes service has been more successful with consumers than the highly restrictive digital music services offered by major recording industry firms.[119]

In addition to the invisibility of TPMs, their complexities, their proprietary nature, and other factors that make vendors reluctant to disclose them, members of the public, consumer product reporting services, and news reporters, as well as policymakers, are largely ignorant about TPMs and relatively inexperienced in dealing with them. There are, moreover, no established metrics for informing consumers about TPM systems that will affect their usage of digital media products. Although CDT has recently proposed some criteria for metrics to evaluate TPMs,[120] this has yet to take hold as a meaningful market constraint on the deployment of TPMs. It is true that market mechanisms induced some recording industry firms to recalibrate their copy-protection systems to be more consumer-friendly,[121] but disclosure of TPM restrictions and capabilities among digital media products remains woefully thin. As Part II has shown, the lack of disclosure has brought about numerous harms to consumers. For these reasons, we are skeptical that market mechanisms alone will bring about sufficient disclosures about TPMs.

B. Trust Self-Regulation

We are tempted to limit our discussion of the industry self-regulation policy option to a single statement: Self-regulation is unlikely to provide meaningful disclosure about TPM restrictions or capabilities by digital content industry sectors in the absence of significant nudges from governmental actors (on which more in subsection C). However,

---

[117] Disincentives for content developers to disclose TPM restrictions may also arise from concentration in some copyright industry sectors, as in the recording industry. The more concentrated the industry, the less competitiveness firms may be about key product issues, such as TPMs. Moreover, even in a more deconcentrated industry sector, firms may not want to compete about TPMs because of concerns about fragmentation of the market that might happen during standards wars.

[118] Efforts by leading firms in the software industry in the 1980's to use copy-protection technologies were unsuccessful, as TPM restrictions were competed away. See, e.g., Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 Mich. L. Rev. 462 (1998)(discussing this history). See also Don Jeffrey, "EMI cashes in on unprotected music sales", Bloomberg News, June 15, 2007 (noting that DRM-free versions of songs from EMI were selling at a rate of 200-300% higher than DRM versions).

[119] See, e.g., Jon Healey, *Sony Dis-Connects*, L.A. Times, June 18, 2007 (discussing the demise of Sony Connect as attributable in part to restrictive TPMs, contrasting this service with Apple's); Yuri Kageyama, Sony exec admits mistakes, says company is 'growing up', Associated Press, January 20, 2005 (quoting president of Sony Computer Entertainment admitting that it was overly proprietary in its approach to TPMs and missed out on the unprotected MP3 market).

[120] CDT Report, supra note xx, at 1-2.

[121] Id. at 4.

because this option is often preferred to governmental regulation in the American policy quiver, we will give it somewhat greater attention than it may genuinely deserve.

Self-regulation is often used as an alternative to government regulation in the U.S. This is mainly because firms in an industry are likely to have a more grounded sense about the viability of certain policy options than government regulators would have. They are in a better position to assess the costs and benefits of various approaches and to identify a range of possible implementations for accomplishing the overall goals. Through self-regulation, firms can apply their expertise to addressing problems in a flexible manner that is responsive to societal expectations.[122] In the course of developing and then implementing "best practices" guidelines or codes of conduct, industry leaders not only internalize the norms that reflect societal values, but also set examples that other firms are likely to follow. Insofar as firms deviate from established self-regulatory norms, there may be both formal and informal means of chastising the deviants and reinforcing the normative heft of the self-regulatory infrastructure.

So why are we skeptical that industry self-regulation is likely to lead to effective disclosure of TPM restrictions and other capabilities affecting consumers? For one thing, it has not happened, or even begun to happen, in the past decade. The lack of self-regulatory initiatives is notable, given how common incidents of consumer difficulties with TPMs have been, as shown in Part II. Second, the same disincentives to meaningful disclosure that make us skeptical of a trust-the-market approach exist to undermine our confidence in a self-regulatory approach. Third, a self-regulatory regime is unlikely to succeed because the producers of digital content generally do not construct the TPM systems they use, and each firm has different interests and incentives for paying attention to consumer impacts.[123] Fourth, the most ardent proponents of TPMs, that is, the entertainment industry, has yet to accept that the notice problems identified in this article exist and are in need of attention.[124] This industry does not believe that consumers have "rights" to make backup copies or fair uses of copyrighted content; consumers only have "expectations," and the industry believes that these expectations can be managed by means of the TPMs they build into the digital products and services they make available in the marketplace.

The factor most likely to induce industry self-regulation of TPMs in the U.S. is the adoption of disclosure requirements for TPMs by other nations, such as the U.K. Because markets for digital media products are global, disclosure regulations in even one country with a sizeable market may well affect industry behavior worldwide. However, it is also quite possible that the industry will choose to segment the market by selling products with notices in places that require them and products without notice where transparency is not required.

---

[122] See, e.g., Joseph J. Oliver, The Public Interest in Self-Regulation (2001), available at http://www.ida.ca/Files/Media/AnnualConf/2001/Speeches/2001OpenAddress_en.pdf.

[123] See, e.g., Mulligan & Perzanowski, supra note xx.

[124] See, e.g., Remarks of Preston Padden of Disney Co. at Silicon Flatirons Conference, Boulder, Co., February 11, 2007 (endorsing a trust-the-market approach). Other industry sectors that use TPMs, such as the videogame industry, without giving notice about TPM restrictions have yet to feel any public pressure to provide meaningful notice.

C. An FTC Investigation and Report

By bringing a claim against Sony BMG in response to the rootkit software incident, the FTC has demonstrated that it already has authority to regulate abusive uses of TPMs in mass-market products. Lack of meaningful disclosure was a key element of this case, and to settle this lawsuit, Sony BMG pledged to disclose material features of TPM systems in audio CDs in the future.[125]

The broader implication of the *Sony BMG* case, however, is apparent from Commissioner Rosch's affirmation that failure to reveal relevant technical restrictions to consumers prior to their purchase of technically protected digital media products may be an unfair or deceptive trade practice.[126] As we have shown, Sony BMG is far from the only deployer of TPMs to have given little or no information to consumers about the restrictiveness of their systems.

While the FTC will almost certainly bring additional cases against firms that abusively deploy TPMs in digital products, we believe that the Commission should launch an investigation about the extent (or lack) of transparency about TPMs and consumer harms resulting therefrom and issue a report, akin to those it has written on other new technology consumer protection issues, such as spyware and online information privacy.[127] Part II has given many examples of transparency problems with TPM deployments, which suggests that a broad empirical investigation of industry practices and of the mismatch between consumer expectations and what TPM restrictions and features is warranted. Such a report might recommend legislation or other measures aimed at bringing about greater transparency about TPMs.

It is even conceivable that such a report, or perhaps even the prospect of such a report, will induce those who are regularly deploying TPMs in digital products to commence a conversation about self-regulatory measures that might be undertaken to address the notice problems we have identified here. While we have doubts about how meaningful any such effort would be without the prospect of closer regulatory oversight hanging like a sword of Damocles over their heads, it would be a welcome development for the affected industry groups to begin to address the notice problem in a constructive way.

D. Conditioning Legal Protection for DRM on Adequate and Effective Notice

---

[125] Sony BMG Settlement, supra note xx, at 3-5 (various disclosure requirements).
[126] Rosch, supra note xx, at [4].
[127] See, e.g., Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000), available at http://www.ftc.gov/os/2000/05/index.shtm#22; Federal Trade Commission, Staff Report on Monitoring Software on Your PC: Spyware, Adware, and Other Software, available at http://www.ftc.gov/bcp/edu/microsites/spyware/reports.htm.

Deciding the proper regime for enforcing adequate and effective DRM notice depends on many factors, incentives, and efficiencies. One approach to balancing these factors is delegation to an experiences federal agency such as the FTC, as detailed in Section C above. An alternative approach, however, would be to focus less on government regulation via central agency and more in market incentives tied to legal entitlements.

Section 1201 of the Copyright Act provides a strong legal incentive for firms to incorporate DRM into their products and provides strong intellectual property right-like protection against the circumvention of DRM systems. However, unlike most other intellectual property grants,[128] it does not provide sufficient incentives to give notice of the scope of the associated rights and restrictions it protects. Thus, one option for encouraging firms to take on the obligation to provide meaningful notice in a serious way would be to condition standing to sue under Section 1201 on the requirement that the party intending to sue "provide reasonable and effective notice of all access and/or copy limitations implemented by the technical measure protected under this title." This would ensure that those firms, especially in the entertainment industries, who depend on Section 1201 take the steps necessary to explicitly describe the contours and limitations they wish to protect from circumventing acts and devices.

A second additional incentive would be to require knowledge and/or intent for violations of Section 1201. Again, similar to other systems of intellectual property, giving adequate and effective notice of the meets and bounds of one's property right often serves to trigger "intentional" or "willful" liability for infringement of that right.[129] As noted above in Part II, adequate and effective notice was one of the key concerns for the courts in the *Lexmark* and *Skylink* cases when assessing the appropriateness of Section 1201 liability. In those cases, none of the defendants were on adequate notice that any copyrighted works were even allegedly protected by a TPM, let alone actually protected by one. Thus, even if there had been a violation of Section 1201 in those instances, it would have almost certainly been an unintentional one.

By requiring that the plaintiff in a Section 1201 case prove that the defendant knew they were circumventing or intended to circumvent the known restrictions on access or copying, all potential plaintiffs would have incentives to give clear, adequate, and effective notice of those exact limits in order to make their case as easy as possible to win. Without proper notice, defendants would be able to legitimately respond that they

---

[128] See, e.g., 17 U.S.C. §§ 411(a), 412 (requiring registration of copyrighted materials prior to institution of suit and as prerequisites for statutory damages and attorneys fees and costs); 35 U.S.C. 287 (denying recovery for patent infringement damages prior to the issuance and recording of a patent in the Federal Register unless the patentee has given notice to the public by marking); 15 U.S.C. § 1111 (denying profits and damages for trademark infringement without proper notice of registration); Cal. Civ. Code. § 3426.1(b) (requiring actual or constructive knowledge of trade secrecy or improper acquisition in order to find liability for misappropriation).

[129] See, e.g, 17 U.S.C. § 504(c)(2) (raising ceiling on statutory damages for willful copyright infringement from $30,000 per work to $150,000 per work); Cal. Civ. Code § 3426.3(c) (authorizing exemplary damages up to twice actual damages for willful or malicious trade secret misappropriation); 35 U.S.C. § 284 (authorizing treble damages for willful patent infringement).

had no knowledge or intent to circumvent. With proper notice, such a defense would be unlikely to succeed. To implement this change, all one would have to do is insert the word "knowingly" before the word "circumvent" in Section 1201(a)(1)(A). For the trafficking provisions of 1201(a)(2) and (b)(1), one would insert "knowingly" before the word "manufacture". This would ensure that in order for a defendant to be found liable under Section 1201, they must know of the existence of the access or copy control and know they either their act is circumventing that limitation or that the primary purpose of the device they are trafficking in is to do so. This would negate liability for those innocently caught in the web of undisclosed TPMs like Chamberlain's and Lexmark's but still hold those who intentionally circumvent or assist other in circumventing liable – the actors that Section 1201 was truly intended to reach.

In addition to providing rational incentives for adequate and effective notice practices by DRM vendors and content providers, these proposals also find support in the WIPO Copyright Treaty, the primary international agreement which served as the basis for the United States' implementation of Section 1201.[130] Under that treaty, it was clear that the member countries supported anti-circumvention regulations to deter efforts to defeat lawful access and copy controls that prevent mass infringement. However, it was also clear that the member countries intended to limit the scope of these technological and legal tools from impeding legitimate acts that were permitted by law or otherwise beyond the authority of copyright owners, such as fair use of copyrighted works or unfettered access to public domain works.[131] Adding various notice and/or knowledge and intent requirements to Section 1201 supports this goal, as it would encourage DRM vendors and copyright owners to make sure their technological restrictions are in line with the limits of their rights, else they become subject to public scrutiny, or under the Skylink/STK line of cases, risk forfeiture of Section 1201 enforceability for a lack of nexus with infringement of their rights.[132]

E. Substantive Consumer Protection Laws

Finally, one could consider enacting new consumer protection laws that substantively address the harms identified in Part II above, perhaps even a "software consumer bill of rights." For example, laws could be passed that would outlaw any TPM that substantially impaired the use of any computer in a way unrelated to limitations on access or copying of the associated copyrighted work protected or TPMs that increased the risk of unauthorized access by third parties.[133] One could also outlaw any TPM that

---

[130] See WIPO Copyright Treaty, CRNR/DC/96 (Dec. 20. 1996).

[131] Id., Art. 11. For a discussion of the balance in this provision, see, e.g., J.H. Reichman, Graeme Dinwoodie, & Pamela Samuelson, A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Works, 22 Berkeley Tech. L.J. (forthcoming 2007).

[132] One such conditional requirement is already present in Section 1201(k)(2), which requires copy-control technologies for videocassette recorders to maintain time-shifting of broadcast and some cable television content. It has also been suggested in other contexts for preserving access to material for fair use, see e.g., Burk & Cohen, Fair Use Infrastructure for Rights Management Systems, 15 Harv. J. Law & Tech 1 (2001).

[133] This would be consistent with the European Union's implementation of the WIPO Copyright Treaty which imposes an obligation EU member states to ensure that consumers will be able to exercise

collected non-public data on computer use without independent and explicit consent by each computer user and for each new use of that data. An alternative would be to allow collection and transmission of data but condition these activities on anonymizing the data so that it could not be linked back to any particular user or individual.[134] Finally, one could pass laws enabling users to circumvent TPMs for public interest uses.[135]

Conclusion

There are many reasons why it is socially desirable for producers of digital content to give effective notice about TPMs embedded therein. Such notice is obviously likely to affect decisions about whether to purchase technically protected products at all and may induce shopping for alternatives. Notice will also affect consumers' assessment of the value they will derive from purchasing such products and their satisfaction with them. Notice of TPMs can, moreover, avert imposing unwarranted burdens on retailers, consumer electronics firms, and makers of digital media players whom frustrated consumers may otherwise blame for upsetting experiences with TPMs of which they had no notice.[136] Product reviews by consumer rating services and the news media will also be better able to inform consumers if producers of digital content with TPMs reveal more about product characteristics and limitations.[137]

Requiring firms to give consumers notice about TPMs is more likely to foster meaningful competition among providers of digital products and services than will occur if giving notice about TPMs is not required. Some of this competition will be between TPM and non-TPM products, and some will be between products with more and less restrictive TPMs.[138] Even in the absence of competition, digital media producers may be affected by notice requirements when making decisions about whether to use TPMs or whether to use lighter- or heavier-weight TPM systems. The more notice they have to give about the restrictiveness of their products, the less inclined they may be to adopt highly restrictive systems.

We are not so naïve as to believe that designing effective disclosure rules about TPMs will be easy. The products and services to which notice requirements may apply are so varied, as are the devices on which the content can be rendered as well as the capabilities of TPM systems. Fortunately, the FTC has demonstrated considerable

---

exceptions and limitations even when works are technically protected. See Reichman, et al., supra note xx, Part III.

[134] See, e.g., Julie E. Cohen, *DRM and Privacy*, 18 Berkeley Tech. L.J. 575 (2003).

[135] See Boucher Bill; Reichman et al., supra note xx.

[136] See Proposed Finding (1), H.R. 1201, 109th Cong. (2005).

[137] CDT Report, supra note xx, at 1.

[138] That competition is having an effect on the use of TPMs is evident from the recent decision of one of the major recording labels, EMI, to allow much of its repertoire to be distributed via digital music services in an unprotected MP3 format, instead of being locked down with TPMs. See, e.g., Press Release, EMI Music Launches DRM-Free Superior Sound Quality Downloads Across Its Entire Digital Repertoire, http://www.emigroup.com/Press/2007/press18.htm. Even though the Apple iTunes service currently uses TPMs, Steve Jobs, Apple's CEO, has announced its willingness to drop TPM restrictions on digital music and has urged major labels to agree to this. See, e.g., Steve Jobs, Thoughts on Music, Feb. 6, 2007, available at http://www.apple.com/hotnews/thoughtsonmusic/.

competence in balancing consumer and producer interests in other new technology contexts, and we, like Rep. Boucher and Senators Brownback and Wyden, are confident that the Commission can devise a flexible and adaptable disclosure regime that will yield notices that consumers can understand and that copyright owners can live with.

Nor are we so naïve as to believe that a notice requirement will address all of the consumer protection issues likely to be posed by TPMs in digital content. Although consumer protection laws, such as those administered by the FTC, have proven flexible enough to deal with the first round of TPM consumer protection problems, we foresee the possibility of the need for additional regulation of TPMs over time. Especially likely to be needed is regulation to protect information privacy of users of TPM'd content insofar as the TPMs are part of a monitoring regime affecting consumer intellectual privacy interests.