SHOULD COPYRIGHT OWNERS HAVE TO GIVE NOTICE OF THEIR USE OF TECHNICAL PROTECTION MEASURES?

PAMELA SAMUELSON & JASON SCHULTZ*

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

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] To counteract this easy copying, some copyright owners have adopted technical protection measures (or "TPMs", sometimes also referred to as "digital rights management" or "DRM" technologies) to control unauthorized access to and uses of digital content in mass-market products and services.[2] Copyright owners in the entertainment industry regard TPMs as essential to the creation of viable global markets for digital content.[3]

Consumers of digital products, however, often find TPMs frustrating, annoying, and harmful. TPMs may inhibit playful and creative uses of digital works and other non-infringing uses of the content, such as time- or platform-shifting. Consumers are especially likely to be frustrated and upset when they purchase technically restricted content without being given advance notice about what TPMs will disable or otherwise do that they do not expect. This article will demonstrate that many copyright owners are failing to give adequate and effective notice of TPM restrictions. This lack of transparency about TPMs has caused consumers several different kinds of harm. We believe that some regulatory action is necessary to address the notice problems that TPMs have brought about, and that this can be done without undermining the content protection goals that copyright owners have in using TPMs.

Part I of this article demonstrates that consumers have many expectations about what they should be able to do with digital content.

1. *See, e.g.*, NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 23-75 (Nat'l Academy of Sciences 2000) (discussing advances in digital technologies that have given rise to difficulties of enforcing copyright protections).

2. We will generally use the term "technical protection measures" and the acronym "TPM" to refer to technical locks that other commentators refer to as "digital rights management" or "DRM" technologies, except when we are quoting from sources that use the latter term. We regard TPM as a more neutral term than DRM that avoids resolving the ambiguity about whose "rights" matter in the context of DRM. *See, e.g.*, Pamela Samuelson, *Digital Rights Management {and, or, vs.} the Law*, COMM. ACM, Apr. 2003, at 41 (discussing the complex intersection of legal rights and technical measures).

3. *See, e.g.*, WORKING GROUP ON INTELLECTUAL PROP. RIGHTS, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 10-13 (1995) (expressing concern about infringements made possible by the Internet and digital technologies and the importance of technical measures to inhibit infringements). One British copyright lawyer has optimistically opined that "[t]he answer to the machine is in the machine." *See* Charles Clark, *The Answer to the Machine is the Machine*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 139 (P. Bernt Hugenholtz ed., 1996).

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 many TPMs are programmed to do, consumers are likely to be frustrated and upset, especially if they purchased this product without notice of the restrictions.

Part II observes that many copyright owners who employ TPMs to protect digital content products 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 several studies and reports that have characterized the lack of notice of technical restrictions on digital content as a consumer protection issue warranting attention from policymakers. While European commentators have been more active in analyzing transparency and other consumer protection issues arising from TPM'd content, American policymakers and commentators are becoming more aware of these issues, particularly after the "magnificent disaster" of the Sony-BMG rootkit incident.[4]

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 also impose substantive restrictions on what digital content providers can do (and not do) with TPMs in restricting consumer uses of digital content.

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

4. Deirdre Mulligan & Aaron Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. (forthcoming 2007).

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 content have been shaped in part 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.[5] When the commercial medium for recorded music shifted to compact discs ("CDs"), consumers similarly felt free to make personal use copies of the music (e.g., loading it onto the hard-drives of their computers). When Sony introduced Betamax video tape recorders into the market in the mid-1970's, purchasers used them to make time-shift copies of broadcast television programming, among other things.[6] Courts have generally regarded time-, space-, and platform-shifting to be fair uses of copyrighted works, seemingly conforming the law with consumer expectations.[7]

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.[8] Because digital technologies enable new

5. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, COPYRIGHT AND HOME COPYING: TECHNOLOGY CHALLENGES THE LAW 11-14 (1989), *available at* http://govinfo.library.unt.edu/ota/Ota_2/DATA/1989/8910.PDF (reporting on surveys about personal use copying).

6. *Id*. at 11-12.

7. *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 Copyright Litig., 334 F.3d 643, 652-53 (7th Cir. 2003) (noting space-shifting as a possible fair use); Recording Indus. 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. NO. 102-294, at 30 (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), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) (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).

8. *See, e.g.*, 17 U.S.C. § 117 (2000) (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); DigitalConsumer.org, Consumer Technology Bill of Rights, http://digitalconsumer.org/bill.html (last visited Nov. 1, 2007).

flexibilities in ways to use and consume digital information, consumers have come to expect to be able to do more with digital media products than they could do with analog media products.[9] Consumers may, for example, expect to be able to link works together, format-shift, annotate them, tinker with them, remix and mashup existing digital content, and share their new creations with others.[10]

The use of TPMs may impair personal uses that consumers expect to be able to make of digital content.[11] Copy-protected CDs, for example, may prevent platform-shifting and backup copying.[12] One cannot easily make backup copies of DVD movies because of TPMs.[13] DVD movies, moreover, may not be playable on all DVD devices, insofar as region-coding interferes with this ability.[14] Even technical sophisticates may have difficulty playing DVD movies on computers which use the Linux operating system.[15] "Ripping" movies from DVDs to store them on computer hard-drives or to make mashups or remixes can likewise be thwarted by TPMs.[16] Online music stores may use TPMs to prohibit personal use sharing of music.[17] Consumer experiences with online music stores have often been confusing and dismaying because of the mismatch between personal use expectations of users and what the services enable and disable through TPMs.[18]

---

9. *See, e.g.*, NATALI HELBERGER ET AL., DIGITAL RIGHTS MANAGEMENT AND CONSUMER ACCEPTABILITY: A MULTI-DISCIPLINARY DISCUSSION OF CONSUMER CONCERNS AND EXPECTATIONS 21 (2004), *available at* http://www.indicare.org/tiki-download_file.php?fileId=111 (giving examples of a wide array of personal uses that consumers expect to be able to make of digital media products).

10. *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

11. *See, e.g.*, Deirdre Mulligan, Aaron J. Burstein & John Han, *How DRM-based Content Delivery Systems Disrupt Expectations of 'Personal Use,'* PROC. OF THE 2003 ACM WORKSHOP ON DIGITAL RIGHTS MGMT. 77 (2003).

12. CTR. FOR DEMOCRACY & TECH., EVALUATING DRM: BUILDING A MARKETPLACE FOR THE CONVERGENT WORLD 7-8 (2006) [hereinafter CDT REPORT], *available at* http://www.cdt.org/copyright/20060907drm.pdf.

13. *Id.* at 4.

14. *See, e.g., id.*; HELBERGER ET AL., *supra* note 9, at 21.

15. *See, e.g.*, Declan McCullough, *Teen Hacking Idol Hits Big Apple*, WIRED, July 20, 2000, http://www.wired.com/culture/lifestyle/news/2000/07/37650 (noting inability to play DVDs on Linux systems).

16. CDT REPORT, *supra* note 12, at 3. Yet, 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. anti-circumvention rules). *See* Posting of Fabienne Serriere to Engadget, How-To: Convert a DVD for Your iPod (with Video) in Windows, http://www.engadget.com/2005/10/14/how-to-convert-a-dvd-for-your-ipod-with-video-in-windows/ (Oct. 14, 2005).

17. CDT REPORT, *supra* note 12, at 9.

18. Mulligan et al., *supra* note 11; Ken Fisher, *Musicload: 75% of Customer Service Problems Caused by DRM*, ARS TECHNICAL, Mar. 18, 2007, http://arstechnica.com/news.ars/post/20070318-75-percent-customer-problems-caused-by-

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.[19] One recent report has observed that consumers want and expect "[f]lexible personal use—the ability to read, listen to, play, or watch a lawfully acquired work in a manner and sequence of the consumer's own choosing."[20] 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,"[21] 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."[22]

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 or to take actions that would make their customers insecure. 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 or control by the content's commercial distributors.[23] Consumers had no reason to fear that their use of these products in the privacy of their homes or offices would undermine their security from external attacks. Consumer expectations about privacy and security continue to be reasonable, but 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.[24] TPMs may, moreover, cause other unanticipated negative impacts on consumers.[25]

II. CONSUMER HARMS RESULTING FROM THE LACK OF EFFECTIVE NOTICE OF TPM RESTRICTIONS

The disparity between consumer expectations about flexible uses of

drm.html (noting that "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").

19. CDT REPORT, supra note 12, at 14.

20. *Id.*

21. *Id.* at 17.

22. *Id.*

23. *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).

24. CDT REPORT, *supra* note 12, at 10.

25. *Id.* at 20 ("DRM may drain battery or processing power" or "modify[] the operation of . . . device drivers for DVD burners.").

digital media and limitations imposed by TPMs gives rise to significant tensions for the technology and entertainment marketplaces to mediate. Copyright owners may be aware that TPMs will not be popular with customers, and this creates incentives not to disclose their use in advance. When copyright owners or TPM vendors fail to adequately and effectively disclose the existence of the TPMs and the limits they impose, however, it exacerbates the tension mentioned above because the marketplace is operating on imperfect information.[26] The failure to give adequate and effective notice of TPM restrictions has resulted in six types of harms to the public: 1) lack of expected interoperability, 2) privacy intrusions, 3) security vulnerabilities, 4) anti-competitive lockouts, 5) risks of unforeseen anti-circumvention liability, and 6) unanticipated and unconsented to changes in or discontinuation of service.

A. Lack of Expected Interoperability

Among the most widespread concerns arising from 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 consumers enjoy from the digital networked economy result from compatibility between devices, formats, platforms, and applications.[27] 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, tend to be designed to thwart information transactions by erecting barriers to data exchange. Thus, the tension between TPMs and the value of

26. *Digital Media Consumer Rights Act of 2003: Hearing on H.R. 107 Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. 12 (2003) (testimony of Rep. Rick Boucher); *see also* 149 CONG. REC. S11571 (2003) (statement of Sen. Sam Brownback introducing S. 1621, titled the Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, to the Senate); Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, S. 1621, 108th Cong. § 2(2) (noting increased confusion among industry, educational institutions, libraries, and consumers as access controls become more prevalent in the marketplace); Julian Bajkowski, *Intel Quietly Adds DRM to New Chips*, DIGITAL ARTS, May 27, 2005, http://www.digitalartsonline.co.uk/news/index.cfm?NewsID=4915; Marc McEntegart, *No Pre-Owned Games to be Allowed for Playstation 3*, INQUIRER, Nov. 9, 2005, http://www.the-inquirer.com/default.aspx?article=27568.

27. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575 (2002); Mark A. Lemley, *The Law and Economics of Internet Norms* 29-30 (Berkeley Program in Law & Econ., Working Paper Series, Paper No. 132, 1999), *available at* http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1131&context=blewp (discussing positive influence of norms on Internet network effects).

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 ineffective. 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 various non-TPM formats such as MP3. 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.[28] This lack of notice, and the lack of interoperability the Apple TPM causes, has led to several public policy inquiries focused on consumer protection implications.[29]

In 2005, moreover, Sony BMG Music distributed thousands of sound recordings in 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.[30] While the CDs were labeled with a short "Copy Protected" notification, the notice did not clarify what this term meant, nor what uses were restricted and how. On the back of XCP protected CDs, there was a list of certain platforms on which one could play the music, but not which applications or devices would play them. The notice 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.[31] Because of the inadequacies of this notice, users lacked sufficient information to understand the limits on interoperability

28. *See* Apple Inc., iTunes Store – Terms of Service, http://www.apple.com/legal/itunes/us/service.html (last visited Oct. 22, 2007) (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* Apple Inc., iTunes Store – Terms of Sale, http://www.apple.com/legal/itunes/us/sales.html (last visited Oct. 22, 2007) (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.").

29. *See* Stephen Withers, *Europe Continues to Push for iTunes Interoperability*, ITWIRE, Mar. 12, 2007, http://www.itwire.com.au/content/view/10368/53/; Jo Best, *Law to Make iTunes Compatible with Microsoft?*, SILICON.COM, Apr. 7, 2005, http://management.silicon.com/government/0,39024677,39129365,00.htm.

30. *See* Mulligan & Perzanowski, *supra* note 4; Electronic Frontier Foundation, A Spotter's Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Oct. 22, 2007).

31. Electronic Frontier Foundation, A Spotter's Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Oct. 22, 2007).

that Sony BMG had imposed upon them with its XCP protected CDs.

Technical restrictions like these often surprise, frustrate, and confuse consumers, especially when they are applied to media such as CDs that consumers have come to expect to be available without such limits. TPMs may place unwarranted burdens not only on consumers, but also on retailers and manufacturers of computers or consumer electronics devices. This is because consumers may complain to the retailers or manufacturers about their frustrations with TPM products or services. It is often not obvious to the complaining consumers that the technical restriction was imposed by the maker of the digital media product or service, not the manufacturer or seller of the equipment on which consumers choose to render the digital media product or service.

A third example of TPM-induced non-interoperability 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 the DVD is authorized to be distributed. If, for example, someone purchased a DVD with a European Region Code (Region 2) while on vacation in France, he or she could not play that DVD on most U.S. manufactured DVD players because they are encoded to play only DVDs having a U.S. Region Code (Region 1). Notwithstanding the pervasiveness of DVDs, most DVDs do not disclose region code restrictions to consumers, either at the point of sale, or in the accompanying literature for the DVD. Consumers who 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 hotel or new home.[32] Without proper notice, consumers may believe that this is a problem with the DVD they bought or with their DVD player instead of a TPM restriction imposed on them by the copyright holder in conjunction with the DVD Copy Control Association.

TPM-induced non-interoperability problems are not limited to digital content. Hewlett-Packard, for example, has started "region coding" its printers and printer cartridges so that consumers must buy the latter in the same region of the world as they bought the printer.[33] If the "wrong" cartridge is inserted, HP equipment will not print documents, even though the cartridge is, except for the difference in the region code,

32. A similar problem exists within the iTunes Music Store TPMs. Apple has reportedly been 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, *iTunes: The Insanely Great Songs Apple Won't Let You Hear*, SLATE, Jan. 23, 2007, http://www.slate.com/id/2158151/.

33. David Pringle & Steve Stecklow, *Electronics With Borders: Some Work Only in the U.S.*, WALL ST. J., Jan. 17, 2005, at B1.

functionally identical to the "right" region-coded cartridge.[34]

B. Privacy Invasions

Some TPM-protected products and services have been designed to monitor consumer usage and report back about it to the owners of copyrights in the TPM-protected works or to their agents. This monitoring often happens at a very deep technical level of the consumer device or product. Ordinary consumers are unlikely to be aware of the existence or extent of such monitoring or of uses that may be made of personal data collected through such monitoring.[35] This poses the harm of invading users' privacy interests and exposing them to unwanted surveillance or profiling.

Blizzard Entertainment, for example, has deployed a privacy-intrusive TPM in software associated with its very popular online videogame called "World of Warcraft"[36] in which millions of users log in to Blizzard's servers and interact. Blizzard conceived of this privacy-invasive TPM as a strategy for controlling cheating and "hacks." An "update" of its software included a TPM monitor called "The Warden," which users installed on their personal machines.[37] The Warden TPM monitored each user's computer, including any active window, to make sure no unauthorized programs were running while the game was in play.[38] Upon detecting any such program, The Warden was designed to investigate the user's gaming activities; based on the results of the investigation, Blizzard may take steps including suspending the user's account.[39]

While some users did not object to the Warden because it kept some 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.[40] While Blizzard does disclose some general information about The Warden in its

34. *Id.*

35. *See* Bajkowski, *supra* note 26; *see also* CANADIAN INTERNET POLICY AND PUBLIC INT. CLINIC, DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES AND CONSUMER PRIVACY (2007), *available at* http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf.

36. World of Warcraft, http://www.worldofwarcraft.com (last visited Oct. 22, 2007).

37. Mark Ward, *Warcraft Game Maker in Spying Row*, BBC NEWS, Oct. 31, 2005, http://news.bbc.co.uk/1/hi/technology/4385050.stm.

38. Jon Espenschied, *No Security Reprieve from Blizzard's Warden: Two Good Reasons to Pass on MMORPGs in the Office*, COMPUTERWORLD, May 13, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019240; Schneier on Security, Blizzard Entertainment Uses Spyware to Verify EULA Compliance, http://www.schneier.com/blog/archives/2005/10/blizzard_entert.html (Oct. 13, 2005).

39. *Id.*

40. *Id.*

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.[41]

Similar concerns about TPM privacy invasiveness were lodged against Sony BMG after it became known that its TPM system for copy-protecting CDs sent information about consumer usage over the Internet back to the company that made the TPM for Sony[42] and against the now-defunct Digital Video Express (Divx) system, which reportedly collected information on every movie a user would watch.[43]

Copyright owners have incentives to embed privacy-invasive monitoring and reporting features in their TPMs. As with the Blizzard software, monitors can aid in the detection of infringing copies of copyrighted works; they can also facilitate price discrimination and profiling about customers that will allow rights holders to offer new products and services to them or to sell user profiles to other firms. If experience thus far is any guide, deployers of TPM monitoring software are unlikely to give adequate and effective notice of the monitoring capabilities and what the monitoring firm plans to do with the information collected by the TPM system. We worry that that the privacy-invasive TPMs of the present may augur further such systems in the future.[44] We believe that firms that distribute digital media products or services that monitor consumer uses should be required to give their customers 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 collecting and processing of such data.[45]

C. Security Vulnerabilities

Certain kinds of TPMs may also make consumers' computers

41. World of Warcraft, End User License Agreement § 5 http://www.worldofwarcraft.com/legal/eula.html (last visited Oct. 22, 2007).

42. Posting of J. Alex Halderman to Freedom to Tinker, Sony Shipping Spyware from SunnComm, Too, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005).

43. Dan Fost, *Divx's Death Pleases Opponents*, S.F. CHRON., June 18, 1999, *available at* http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/06/18/BU89741.DTL.

44. *See generally* Lee A. Bygrave, *Digital Rights Management and Privacy - Legal Aspects in the European Union in* DIGITAL RIGHTS MANAGEMENT - TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 418 (Eberhard Becker et al. eds., 2003); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Ian Kerr & Jane Bailey, *The Implications of Digital Rights Management for Privacy and Freedom of Expression*, 2 J. INFO. COMM. & ETHICS SOC'Y 87 (2004).

45. *See generally* ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO INTELLECTUAL PROPERTY RIGHTS (2005), *available at*, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf (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").

vulnerable to security problems. When TPMs exert control over computers and other devices to limit access or functionality to users, they are, in essence, technically overriding the users' default configurations and decisions about how to operate their technology.[46] Anticipating that some users with technical skills may try to disable TPMs, TPM makers have developed ways to make the TPMs "resistant" to user tampering or to hide the TPM software so that the user cannot locate or disable the TPM. This design approach, however, is likely to make users' computers vulnerable to certain kinds of unanticipated exploitations. Makers of malicious software, such as viruses, spyware, or spam-generating programs, for example, can take advantage of certain attributes of TPM "resistant" design 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.

In order to avoid detection (and subsequent removal) by users, for example, the Sony BMG XCP TPM used a well-known computer exploit technique called "a rootkit" to hide itself in the registry files of the Windows operating system by pretending to be one of the thousands of essential components that Windows needs to operate correctly.[47] The XCP software was designed to evade most attempts to detect it so it could monitor use of the digital music files on the Sony BMG CDs without interference from the user. However, because of certain design flaws, the XCP software made users' computers susceptible to being taken over by malicious programs. The malicious programs were able to use XCP's evasion feature to avoid detection by anti-virus and anti-spyware programs typically installed on computers running Windows. This malicious software could then, in turn, be used to infect the host computer when the Sony BMG CD had been inserted and spread itself undetected to other computers via network connections.

By failing to disclose—and, in fact, actively concealing—the existence of the XCP TPM, Sony not only misled its customers about restrictions on the usability of the copyrighted content they had purchased, but also exposed them to significantly increased risks of malicious software undermining 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 may be just the beginning of a

46. *See, e.g.*, SETH SCHOEN, ELEC. FRONTIER FOUND., TRUSTED COMPUTING: PROMISE AND RISK 1, http://www.eff.org/files/20031001_tc.pdf (noting that while "trusted computing" technologies solve some of today's electronic security problems, they may do so "while giving third parties the power to enforce policies on users' computers against the users' wishes").

47. *See* Mulligan & Perzanowski, *supra* note 4.

pattern of security-related problems for users of TPM technology.[48]

D. Anti-Competitive Lock-out

TPMs can also be designed to prevent users from using non-infringing competing products as alternatives to those provided by the TPM content developer or from using independent service vendors other than those affiliated with or licensed by the original TPM-encoded product or service. Consumers suffer harm when TPMs are used to lock-out competitive products and services, especially when they were given no notice of the existence of the lockout system before purchasing the product or service.

An example is the case of *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*,[49] in which the maker of a garage door opener ("GDO") asserted that a competitive GDO manufacturer could not lawfully distribute its GDOs because they bypassed an access control feature of Chamberlain's GDOs in violation of the Digital Millennium Copyright Act ("DMCA") anti-circumvention rules, now codified as Section 1201 of Title 17 of the U.S. Code.[50] Chamberlain had installed a set of rolling codes that were synchronized between the remotes and the openers. It asserted that these rolling codes were access controls protecting its copyrighted software, and bypassing the access controls was illegal under the DMCA.

One of the problems the court perceived with Chamberlain's DMCA claim was that Chamberlain had failed to disclose this technological lock-out feature to its customers when they purchased its GDOs.[51] It was, ironically, only after an after-market GDO remote competitor, Skylink, reverse-engineered Chamberlain's programs and offered a competing universal GDO remote that Chamberlain disclosed the existence of the TPM by the lawsuit it filed against Skylink under Section 1201.

Use of TPMs as lock-out devices significantly raises switching costs for consumers, creates inefficiencies in the marketplace for such technologies, and puts consumers at risk of being stuck with inadequate or debilitating purchases. Other examples of TPMs being used as lock-out mechanisms have arisen in the context of printers and printer ink

48. *See* John Leyden, *Trojans Exploit Windows DRM Loophole*, REG., Jan. 13, 2005, http://www.theregister.co.uk/2005/01/13/drm_trojan/ (reporting that "Trojans and other malware" are able to subvert DRM features in Windows Media Player).

49. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

50. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 and 28 U.S.C. (2006)).

51. *Chamberlain Group*, 381 F.3d at 1187, 1194.

cartridges,[52] magnetic tape library storage systems,[53] car repair diagnostic software,[54] online videogame servers[55] and digital camera film files.[56]

E. Risks of Inadvertent Anti-Circumvention Liability

Inadequate notice of TPMs can also put consumers at risk of inadvertent anti-circumvention liability. There are unquestionably some situations in which people have been aware that copyright owners are using TPMs to protect their works, and hence, presumptively aware that Section 1201 of the DMCA protects rights holders against circumvention of these TPMs. The journalist Eric Corley, for example, was well aware that the DVD Copy Control Association required makers of DVD movies and DVD players to use the Content Scramble System ("CSS") TPM to protect DVD movies from unauthorized copying; Corley also knew that he was running the risk of legal liability under Section 1201 when he posted the source and object code of a program that bypassed CSS on the website of his online magazine.[57]

However, the history of DMCA enforcement efforts thus far suggests that there are significant gray areas as to anti-circumvention liability.[58] Some customers and competitors have been surprised to find themselves charged with Section 1201 violations, in part because the copyright owner did not give adequate or effective notice that it was using a TPM that was subject to Section 1201 strictures.

Consider, for example, the unwelcome surprise experienced by the

52. *See, e.g.*, Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 528-32 (6th Cir. 2004).

53. *See, e.g.*, Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

54. *See, e.g.*, Auto Inspection Servs., Inc. v. Flint Auto Auction, Inc., No. 06-15100, 2007 WL 674312 (E.D. Mich. Feb. 28, 2007).

55. *See, e.g.*, Davidson & Assoc., Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1167 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Assoc. v. Jung, 422 F.3d 630 (8th Cir. 2005) (using undisclosed TPM to lock videogames into vendor's proprietary servers); The Grip Line Weblog by Ed Foster, Steaming about DRM, http://www.infoworld.com/weblog/foster/2005/01/04.html (Jan. 4, 2005) (describing videogame company Valve Software's attempt to restrict use of videogame to a single computer using undisclosed TPM).

56. *See Nikon Responds to RAW WB Concerns*, DIGITAL PHOTOGRAPHY REV., Apr. 22, 2005, 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).

57. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 324 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (affirming a lower court ruling that Corley was liable for violating Section 1201 of the DMCA by posting DeCSS on his website and linking to sites where DeCSS could be found).

58. *See generally* R. Anthony Reise, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003).

maker of chips designed for use in Lexmark-compatible printer cartridges when Lexmark sued it for violating Section 1201 in the *Lexmark International, Inc. v. Static Control Components, Inc.*, case.[59] Lexmark claimed that Static Control trafficked in unlawful circumvention technologies because its chips contained software that activated printer engine software code inside Lexmark printers, thereby bypassing a TPM that Lexmark had embedded in its software to control access to its copyrighted program.[60] The lower court found Lexmark's logic persuasive and enjoined Static Control from further manufacture of the Lexmark-compatible chips. This ruling was eventually overturned on appeal in part because the court decided that Lexmark had, among other things, failed to "effectively control[] access" to the printer program (for example, by encrypting it).[61] While we think the appellate court reached the right conclusion on 1201 liability, perhaps it should also have considered that Static Control had no reason to anticipate that Lexmark was using a 1201-relevant TPM to protect its printer program, let alone that it would charge Static Controls with 1201 violations for making chips for use in competing cartridges. It is also worth noting that while this case concerned the anti-trafficking provision of 1201(a)(2), Lexmark's conception of 1201 liability would logically lead to holding purchasers of Lexmark-compatible cartridges equally liable for violating this law, even though customers could not have reasonably anticipated being charged with violating Section 1201 based on their purchase of products that competed with Lexmark products.[62]

Lack of adequate notice of potential anti-circumvention liability was also a problem in *Chamberlain v. Skylink*.[63] Chamberlain's theory of liability was premised on the notion that since GDOs ran a software program when the remote activated it, the code used by its GDO was a TPM that controlled access to that code, a TPM that 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

59. Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003), *vacated*, 387 F.3d 522 (6th Cir. 2004).

60. *See Lexmark*, 253 F. Supp. 2d at 947-57.

61. *Lexmark*, 387 F.3d at 551-53 (Merritt, J., concurring) (asserting that Section 1201 claims should not be used to block competition in the products market; the majority ruled only that Lexmark had not made a valid claim on the facts before them).

62. If the Static Control chip was an anti-circumvention tool, then users of printer cartridges embodying this chip would logically be in violation of 17 U.S.C. § 1201(a)(1)(A), which forbids bypassing TPMs that control access to protected works.

63. *Chamberlain Group*, 381 F.3d 1178.

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.[64]

Nor could Princeton Computer Science Professor Ed Felten have reasonably anticipated being charged with violating Section 1201 by the Recording Industry Association of America ("RIAA") when he and his students wrote a paper for presentation at a scientific conference based on their experience undertaking an RIAA-authorized challenge to "crack" recently developed TPMs for recorded music files.[65] RIAA claimed that if Felten et al. published their results, they would be trafficking in a circumvention device under Section 1201.[66] Felten filed for a declaratory judgment that presenting this paper would not violate the anti-circumvention laws, following which the RIAA mooted the suit. However, this threatened lawsuit created uncertainty about whether and to what extent future scientific research might be considered a violation of the DMCA.[67]

Consider also the case of *Davidson & Associates v. Jung*, in which the parent company of Blizzard Entertainment sued a group of open source developers for creating an interoperable game server (called the "BNETD" server) which allowed them to play Blizzard's Warcraft, Starcraft, and Diablo videogames.[68] In creating the BNETD server, the programmers deliberately avoided use of Blizzard's encryption protocols or authentication mechanisms that the client tried to send to the server in the hope that this would avert 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 their program 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 information, even in good faith, the courts found the developers were circumventing

64. *Id.* at 1203-04.

65. *See generally* Transcript of Motions, Felten v. RIAA., No. 01-CV-2669 (D.N.J. Nov. 28, 2001), *available at* http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20011128_hearing_transcript.pdf.

66. *See* Letter from Matthew J. Oppenheim, Esq., RIAA Counsel, to Professor Edward Felton (Apr. 9, 2001), *available at* http://cryptome.org/sdmi-attack.htm.

67. *See* Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 SCIENCE 2028, 2028-30 (2001) (discussing the chilling effects of this threatened lawsuit on security researchers).

68. Davidson & Assoc. v. Jung, 422 F.3d 630 (8th Cir. 2005).

Blizzard's TPM and were 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 this TPM existed or what limitations, either technologically or legally, it was meant to impose.

Yet another example of potential inadvertent anti-circumvention liability attributable to inadequate TPM notices arose as to Sony's Aibo robotic dog. Sony released this programmable pet into the marketplace in 1999. Soon thereafter, an enterprising group of Aibo dog enthusiasts reverse-engineered the Aibo code and discovered how to write new programs to run on the Aibo system so that the dog could be directed to do any number of creative (albeit unauthorized by Sony) maneuvers, e.g., jazz-inspired dance sequences.[69] In 2001, Sony sent a cease-and-desist letter to the developers of a website called "aibohack.com" demanding that it stop distributing code that was retrieved by bypassing the copy prevention mechanisms of the robot.[70] After its customers strongly protested against this, 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 attendant legal risks are notable.

Techmo v. Ninja Hacker is a sixth example of unintentional legal exposure resulting from inadequate TPM notice.[71] 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 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 to consumers from inadequate notice of TPMs occur when consumers discover to their dismay that TPM-protected

69. *See Sony Uses DMCA to Shut Down Aibo Hack Website*, SLASHDOT, Oct. 27, 2001, http://yro.slashdot.org/article.pl?sid=01/10/28/005233.

70. *Id*.

71. *See* Kevin Poulsen, *Hackers Sued for Tinkering with Xbox Games*, SECURITYFOCUS, Feb. 9, 2005, http://www.securityfocus.com/news/10466.

products or services they have purchased have been programmed to enable alteration of functionality without giving them notice of the changes or an opportunity to object or to obtain a remedy for the lessened 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.[72] 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.[73] 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 service in 2001. In 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.[74] Similar changes in service and features have occurred with personal video recorder manufacturers like TiVo as a result of deals these companies have made with TPM providers like Macrovision and content providers like HBO.[75]

Even more troublesome are situations in which companies that have tethered their content with TPMs discontinue service or go out of business. For example, when the DivX video disc system 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. However when the company that ran DivX went out of business, [76] it was unclear what would happen to those "lifetime" purchases. Would they be honored? Or would consumers lose access beyond the lifetime of the company?

72. *See* Cade Metz, *Intuit's TurboTax Activation Scheme Irks Users*, PCMAG, Jan. 10, 2003, http://www.pcmag.com/article2/0,1895,821308,00.asp.

73. *Id.*; *see also* The Gripe Line Weblog by Ed Foster, Steaming About DRM, http://www.infoworld.com/weblog/foster/2005/01/04.html (Jan. 4, 2005) (noting personal problems activating Christmas video game gift for his eight-year-old son).

74. *See* Apple Inc., iTunes Store – Terms of Service, http://www.apple.com/legal/itunes/us/service.html (last visited Oct. 20, 2007). Notably, at least one European Consumer Ombudsman has objected to this practice. *See iTunes Violates Norwegian Law*, FORBRUKEROMBUDET, June 7, 2006, http://www.forbrukerombudet.no/index.gan?id=11032467&subid=0.

75. Lucas Graves, *Has TiVo Forsaken Us?*, WIRED, Nov. 2004, http://www.wired.com/wired/archive/12.11/view.html?pg=3.

76. *See, e.g.*, Stephanie Miles, *Behind the Death of DivX Were Angry Customers*, CNET NEWS.COM, June 17, 1999, 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, there was recently a news report suggesting that Sony would be shutting down the service, potentially leaving thousands of music fans and customers without access to the content they have legitimately downloaded.[77] Other subscription services such as Rhapsody and Napster raise the same issues about what will happen to consumers' access to TPM content if the company goes out of business or otherwise decides to shut the service down.

III. THE TPM NOTICE PROBLEM HAS BEEN NOTICED

Several European reports have emphasized the need for transparency when technical restrictions are embedded in mass-marketed digital content.[78] 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" ("INDICARE").[79] 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."[80] This report discusses several EU directives that have a bearing on disclosure of TPM restrictions,[81] as well

77. *See* Rafat Ali, *Sony Connect to Close Music/Video Services; Focus on Servicing Playstation Group; 20 People to Go*, PAIDCONTENT.ORG, June 16, 2007, http://www.paidcontent.org/entry/419-sony-connect-to-close-music-video-services-focus-on-servicing-playstati/; *see also* Virgin.com, Sorry - Virgin Digital Has Now Closed!, http://www.virgindigital.co.uk/Message.aspx (last visited Oct. 22, 2007) (announcing discontinuation of DRM-based music downloading service without clear guidance for how users who have purchased music can continue to listen to those songs).

78. *See, e.g.*, ALL PARTY PARLIAMENTARY INTERNET GROUP, DIGITAL RIGHTS MANAGEMENT (2006), *available at* http://www.apcomms.org.uk/apig/current-activities/apig-inquiry-into-digital-rights-management/DRMreport.pdf [hereinafter APIG REPORT]; EUROPEAN CONSUMER LAW GROUP, COPYRIGHT LAW AND CONSUMER PROTECTION (2005), *available at* http://www.europeanconsumerlawgroup.org/Content/Default.asp?PageID=488 (follow 'Copyright Law and Consumer Protection, ECLG/035/2005' hyperlink) [hereinafter ECLG REPORT]; HER MAJESTY'S STATIONARY OFFICE, GOWERS REVIEW OF INTELLECTUAL PROPERTY (2006), *available at* http://www.hm-treasury.gov.uk/media/6/E/pbr06_gowers_report_755.pdf [hereinafter GOWERS REPORT].

79. HELBERGER ET AL., *supra* note 9.

80. *Id*. at vi.

81. *See id*. at 51-55.

as German legislation and French case law that require content owners to give consumers adequate notice about TPM restrictions.[82]

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."[83] More specifically, there was agreement that "all [copy-protected] 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.'"[84] Full disclosure should also be given, says APIG, if technically protected CDs will not play on all devices, will not be playable if the users' device breaks or is stolen, and will record identity information about users.[85] 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."[86] A second British report, Gowers 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.[87]

The first American policy initiative aimed at addressing consumer concerns about inadequacy of notice as to TPM-protected copyrighted works was Congressman 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.[88] 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."[89] 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.'"[90] The bill proposed to authorize the FTC to develop standards for appropriate labeling of such

82. *See id*. at 53 (discussing German labeling requirement for TPM'd content).

83. APIG REPORT, *supra* note 78, at 15.

84. *Id.* at 16.

85. *Id*.

86. *Id.* at 17.

87. *See* GOWERS REPORT, *supra* note 78, at 7 (noting in Recommendation 16 the need for a DRM systems labelling convention).

88. Digital Media Consumers' Rights Act of 2003, H.R. 107, 108th Cong. § 3 [hereinafter Boucher Bill].

89. *Id.* § 2(1).

90. *Id.* § 2(2).

CDs.[91] After promulgation of these standards, recording companies would be required to comply with those standards.[92] Thereafter, it would be an unfair trade practice for firms to introduce into the market unlabeled or mislabeled copy-protected CDs or to advertise such CDs unless the copy-protection feature was disclosed.[93] The bill would have also required the FTC to submit a report to Congress about the effects of the legislation.[94]

Senators Brownback and Wyden introduced similar legislation, although their bills were more general in addressing disclosure issues as to technically protected digital media products.[95] 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 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.[96]

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 the "legal, expected, and customary uses" of these products.[97] 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 [a]s intended or reasonably could be foreseen to have on the consumers', educational institutions', or libraries' use of the product."[98] 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 allow customers to engage in lawful uses, and the extent to which notices of technical restrictions are effective.[99]

The Wyden bill had the same goal as the Brownback bill—to give

91. *See id.* § 3(d)(2)(A) (proposing to amend § 24 of the FTC Act to include "appropriate labeling requirements applicable to [certain] new audio discs").

92. *See id.* § 3(b)(1)–(2).

93. *See id.*

94. Boucher Bill, *supra* note 88, at § 4.

95. Digital Consumer Right to Know Act, S. 692, 108th Cong. (2003) [hereinafter Wyden Bill]; Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, S. 1621, 108th Cong. [hereinafter Brownback Bill].

96. Brownback Bill , *supra* note 95, at § 4(a).

97. *Id.* § 4(d).

98. *Id.* § 4(c).

99. *Id.* § 7.

consumers effective notice about technical restrictions built into digital media products—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."[100] However, it also recognized the legitimacy of consumer expectations about their ability to use and manipulate digital content "for reasonable, personal, and noncommercial purposes."[101]

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 the lawful secondhand sale or distribution of such content."[102]

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.[103]

The bill proposed to authorize the FTC to "prescribe different manners of disclosure for different types of content and different distribution channels,"[104] and also to make exceptions to the notice requirement as to uses of TPMs "that are sufficiently unusual or uncommon that the burdens of prior disclosure would outweigh the

100. Wyden Bill, *supra* note 95, at § 2(a)(2)-(3).
101. *Id.* § 2(a)(1).
102. *Id.* § 2(a)(4)-(6).
103. *Id.* § 3(b)(1).
104. *Id.* § 3(b)(2).

utility to consumers" or "that have no significant application for lawful purposes."[105]

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 to protect against loss, or to use excerpts for such purposes as criticism or commentary, and to transfer one's copy to others.[106] 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."[107]

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."[108]

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 its copy-protected CDs covert installed software on purchasers' computers.[109] Sony BMG's failure to give proper notice of the installation of this software was one of the key problems requiring a regulatory response.[110] The FTC's settlement agreement requires Sony BMG to "clearly and prominently disclose" any software that will be installed on user hard-drives or any TPM-based limitations on the usability of the digital content on users' computers. [111]

In a recent address discussing the role of consumer protection in regulating TPMs, FTC Commissioner Thomas Rosch observed that the

105. *Id.* § 3(d).

106. Wyden Bill, *supra* note 95, at § 3(c).

107. *Id.* § 3(e).

108. *Id.* § 2(b).

109. Complaint, *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (Jan. 30, 2007), http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf.

110. *See* J. Thomas Rosch, *A Different Perspective on DRM*, 22 BERKELEY TECH. L.J. (forthcoming 2007).

111. Decision and Order of the F.T.C., *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (June 28, 2007), http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf.

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."[112] 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.[113] "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."[114] 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.[115] "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."[116] Among the questions the CDT report 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?"[117] "Disclosure is particularly important where DRM-equipped products will not work with certain devices or in certain configurations,"[118] and is "certainly warranted when DRM will

112. Rosch, *supra* note 110, at 3.

113. *Id.* at 3-4 (citing three consent orders in such cases).

114. *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.

115. *See* CDT REPORT, *supra* note 12, at 2. This report offers four metrics for evaluating DRM products and services: transparency, effect on use, collateral impact, and purpose and consumer benefit. *Id.* at 3.

116. *Id.* at 1.

117. *Id.* at 11. 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.* at 12. 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 13.

118. CDT REPORT, *supra* note 12, at 12. Region-coding restrictions in DVDs, for example, should be disclosed to consumers before they purchase copies that may not work on

cause a product's function to deviate significantly from mainstream consumer expectations. . . ."[119]

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.[120] 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,[121] and harms to competition insofar as TPMs are used to lock users into a particular family of products.[122] 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.[123]

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. The 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 to encourage the industry 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.[124]

---

their machines.

119. *Id.*
120. *Id.*
121. *Id.* at 19.
122. *Id.* at 22.
123. *Id.* at 20.
124. Mulligan & Perzanowski, *supra* note 4.

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 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 not only legislatively mandate that effective notice be given about TPM restrictions or other relevant technical features, but would also substantively regulate certain features in TPM systems, such as privacy-invasive monitoring of consumer usage. In order to give content developers meaningful incentives to comply with notice requirements, Congress might also 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 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.[125] 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.[126] Content owners are also understandably reluctant to disclose TPM restrictions, such as the copy-protection software embedded in some CDs, because consumers do not particularly like TPMs.[127] 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.[128] 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.[129]

The reluctance of vendors to disclose TPM restrictions and features means that members of the public, consumer product reporting services, news reporters, and policymakers are largely ignorant about TPMs. 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,[130] these have yet to take hold as a meaningful market

125. 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. CDT REPORT, *supra* note 12, at 4-5. Consumers are likely to find out about the TPM restrictions only when they try to use the DVD movie in a different way than merely playing it to watch the movie.

126. *See, e.g.*, Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 792-95 (2007) (discussing the complex licensing regime that the DVD Copy Control Association has used to maintain secrecy for encryption keys used to protect DVD movies).

127. 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 competitive 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.

128. 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, 523-24 (1998).

129. *See, e.g.*, Jon Healey, *Bit Player: Sony dis-Connects*, L.A. TIMES, June 18, 2007, http://opinion.latimes.com/bitplayer/2007/06/sony_disconnect.html (discussing the demise of Sony Connect as attributable in part to restrictive TPMs, contrasting this service with Apple's); Yuri Kageyama, *Sony Admits Losing Out on Gadgets; Company Was Hung Up on Content Rights, Executive Says*, WASH. POST, Jan. 21, 2005, at E5 (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).

130. CDT REPORT, *supra* note 12, at 2-3.

constraint on the deployment of TPMs.

While market mechanisms induced some recording industry firms to recalibrate their copy-protection systems to be more consumer-friendly,[131] disclosure of TPM restrictions and capabilities among digital media products remains woefully thin. As Part II has shown, the lack of disclosure has harmed consumers in numerous ways. Given the extent of these harms, we are skeptical that market mechanisms alone will bring about sufficient disclosures about TPMs.[132]

B. Trust Self-Regulation

We are tempted to limit our discussion of the policy option of industry self-regulation to simply stating our belief that 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, 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. 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.[133] 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

131. *Id.* at 7.

132. Our skepticism about the "trust the market" approach was recently reinforced when Sony released another TPM'd product that has reportedly made consumers' computers vulnerable to security attacks. *See* Liam Tung, *Sony Pleads Innocent in Latest Rootkit Fiasco*, ZDNET UK, Aug. 31, 2007, http://news.zdnet.co.uk/security/0,1000000189,39288988,00.htm.

133. *See, e.g.*, Joseph J. Oliver, President & CEO, Inv. Dealers Ass'n of Can., Address at the 85th Investment Dealers Association of Canada Annual Meeting and Conference: The Public Interest in Self-Regulation (June 18, 2001), *available at* http://www.ida.ca/Files/Media/AnnualConf/2001/Speeches/2001OpenAddress_en.pdf.

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 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.[134] 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.[135] 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.

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.[136]

The broader implications of the *Sony BMG* case, however, are

134. *See, e.g.*, Mulligan & Perzanowski, *supra* note 4.

135. *See, e.g.*, Preston Padden, Executive Vice President, Walt Disney Co., Remarks at the Silicon Flatirons Conference: Digital Rights Management (Feb. 11, 2007) (endorsing a trust-the-market approach). The videogame industry widely uses TPMs, without giving notice about TPM restrictions; they have yet to feel any public pressure to provide meaningful notice of TPMs.

136. Decision and Order of the F.T.C. at 3-5, *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (June 28, 2007), http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf (setting forth consent decree disclosure requirements).

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.[137] As we have shown, Sony BMG is far from the only deployer of TPMs that has 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 into the extent of transparency about TPMs in mass-marketed software and digital media products (or lack thereof) 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.[138] Part II cites many examples of transparency problems with TPM deployments, which suggests that a broad empirical investigation is warranted of industry practices as well as the mismatch between consumer expectations and TPM restrictions and features. 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

Designing 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 experienced 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 on market incentives tied to legal

137. Rosch, *supra* note 110, at 4.

138. *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; FED. TRADE COMM'N, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

entitlements.

Section 1201 of the Digital Millenium Copyright Act[139] provides a strong legal incentive for firms to incorporate TPMs into their products and provides strong intellectual property right-like protection against the circumvention of TPM systems. However, unlike most other intellectual property grants,[140] it does not provide sufficient incentives to give notice of the scope of the associated rights and restrictions it protects. 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 those in the entertainment industry, who rely heavily 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. Other systems of intellectual property rights have mechanisms for giving adequate and effective notice of the metes and bounds of one's property right, which are often important triggers to "intentional" or "willful" liability for infringement of the right.[141] As noted above in Part II, adequate and effective notice was and should be one of the key concerns raised in cases such as *Lexmark* and *Skylink*. Recall that the defendants in those cases did not have adequate notice that copyrighted works were even allegedly protected by a 1201-relevant 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 it was circumventing or intended to circumvent the known restrictions on access or copying, potential plaintiffs would have

139. 17 U.S.C. § 1201.

140. *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(a) (2000) (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 (2000) (denying profits and damages for trademark infringement without proper notice of registration); CAL. CIV. CODE § 3426.1(b) (West 2007) (requiring actual or constructive knowledge of trade secrecy or improper acquisition in order to find liability for misappropriation).

141. *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) (West 2007) (authorizing exemplary damages up to twice actual damages for willful or malicious trade secret misappropriation); 35 U.S.C. § 284 (authorizing treble damages for patent infringement).

incentives to give clear, adequate, and effective notice of TPM restrictions in order to make their case as easy as possible to win. Without proper notice, defendants should be able to legitimately defend against Section 1201 charges if they had no knowledge of the TPM or intent to circumvent it.

A change of this sort could be implemented in at least two ways. First, courts could decide that defendants who could not have anticipated potential 1201 liability for developing technologies or reverse engineering TPMs should not be deemed to violate 1201 on fundamental fairness grounds. Second, Congress could 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, it must know of the existence of the access or copy control and know that either it is circumventing that TPM or that the primary purpose of the device it is trafficking in is to do so. This would negate liability for those innocently caught in the web of undisclosed TPMs like the defendants in the *Lexmark* and *Skylink* cases, while still holding liable those who intentionally circumvent TPMs or assist other in circumventing TPMs to facilitate infringing acts. These are the bad actors that Section 1201 was truly intended to reach.

Conditioning the ability to bring 1201 claims on giving consumers adequate and effective notice practices of TPM restrictions is consistent with the WIPO Copyright Treaty, the international agreement which first called for regulation of circumvention of TPMs.[142] Under that treaty, nations are required to adopt anti-circumvention regulations to punish those who defeat TPMs in order to facilitate copyright infringements. However, the treaty was also 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.[143] Adding notice of TPM requirements and/or knowledge and intent requirements to Section 1201 supports this goal, as it would encourage TPM vendors and copyright owners to make sure their technological restrictions are in line with the limits of their rights; failure

142. *See* World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65, *available at* http://www.wipo.int/clea/docs_new/pdf/en/wo/wo033en.pdf.

143. *See, e.g.*, *id.* at Art. 11 (requiring the parties to legally protect and enforce TPMs, but only to the extent that the TPM operates against unauthorized or illegal uses). For a discussion of the balance embedded 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. 981 (2007).

to do so would not only risk critical public scrutiny but also forfeiture of Section 1201 enforceability. [144]

E. Substantive Consumer Protection Laws

A final policy response to consumer protection concerns posed by TPMs would be to consider enacting new laws that would substantively address specific harms identified in Part II above, perhaps even a "digital consumer bill of rights." For example, Congress could outlaw the use of TPMs that substantially impair the use of computers and digital content in ways unrelated to the lawful exercise of copyright owner control over access to or copying of copyrighted works protected by TPMs or use of TPMs that increased the risk of unauthorized access by third parties.[145] Congress could also outlaw any TPM that collects non-public data on consumer uses of technically protected content 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.[146] Finally, Congress could pass laws enabling users to circumvent TPMs for public interest uses.[147]

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 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

144. A conditional requirement is already present in 17 U.S.C. § 1201(k)(2), which requires those who copy-control technologies for videocassette recorders to maintain consumer capabilities to engage in time-shifting of broadcast and some cable television content. Other scholars have similarly suggested conditioning section 1201 enforcement on copyright owner willingness to respect legitimate consumer concerns, such as the right to gain access to TPM content for fair use purposes. *See generally*, Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41, 55-58 (2001).

145. This would be consistent with the European Union's implementation of the WIPO Copyright Treaty which imposes an obligation on EU member states to ensure that consumers will be able to exercise exceptions and limitations even when works are technically protected. *See* Reichman, Dinwoodie & Samuelson, *supra* note 143, at Pt. III.

146. *See, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) (discussing the value of intellectual privacy, and legal bases for protecting it from infringing TPMs).

147. *See* Boucher Bill, *supra* note 88; Reichman, Dinwoodie & Samuelson, *supra* note 143.

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.[148] 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.[149]

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.[150] 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 and the capabilities of TPM systems. Fortunately, the FTC has demonstrated considerable 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 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.

148. *See* Digital Media Consumers' Rights Act of 2005, H.R. 1201, 109th Cong. § 2(1).

149. *See generally* CDT REPORT, *supra* note 12.

150. 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 Group Ltd., EMI Music Launches DRM-Free Superior Sound Quality Downloads Across Its Entire Digital Repertoire (Apr. 2, 2007), *available at* 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.*, Posting of Steve Jobs on Apple Inc., Thoughts on Music, http://www.apple.com/hotnews/thoughtsonmusic/ (Feb. 6, 2007).

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.