2020

Unscrewing the Future: The Right to Repair and the Circumvention of Software TPMs in the EU

Anthony D. Rosborough

Technologies of Servitude
Understanding Firmware TPMs as Interests in Personal Property

Anthony D. Rosborough[*]

Keywords: technological protection measures, firmware, copyright, personal property, intellectual property, servitudes, digital locks

Abstract

Widespread computerization and embedded system design has facilitated the pervasive and latent implementation of technological protection measures ("TPMs") to restrict device firmware access. Often referred to as "digital locks," these restrictions impose a whole host of limitations on how owners use and manage the increasing number of products and devices in which they are incorporated. In many cases, TPM restrictions can prevent activities with social, environmental, and economical benefits, including repair, repurposing, and interoperability. In response, governments around the world are now revisiting and scrutinizing their TPM anti-circumvention laws within copyright and competition policy. Beyond these perspectives, this article looks at firmware TPMs' impact on personal property ownership. It examines whether the common law of property and its hostility toward personal property servitudes can assist in guiding future TPM policy. It reveals overlap between personal property servitudes and firmware TPMs on account of the lack of notice, durability, lack of standardization, and increased information costs on third parties. To ameliorate these impacts, it proposes that policymakers take guidance from tangible property law by requiring device manufacturers to provide notice of firmware TPMs, carry out research to prescribe technical standards and classification of TPMs, and impose temporal limitations on their legal enforceability.

I. INTRODUCTION

> *Freedom in the future will require us to have the capacity to monitor our devices and set meaningful policy on them, to examine and terminate the processes that run on them, to maintain them as honest servants to our*

---

[*] PhD Researcher in Law, European University Institute (Italy), anthony.rosborough@-eui.eu. This article is the product of participation in the conference, "Are We Owned? A Multidisciplinary and Comparative Perspective on Intellectual Property in the Algorithmic Society," hosted at the University of Stirling. The author would like to thank Professor Joshua Fairfield (Washington and Lee University School of Law) and Professor Guido Noto La Diega (University of Stirling) for the opportunity to participate in this conference and receive invaluable feedback.

> *will, and not as traitors and spies working for criminals, thugs, and control freaks.*
>
> *– Cory Doctorow, "The coming war on general computation"*[1]

Much scholarly ink has been spilled on technological protection measures ("TPMs") and digital rights management ("DRM") systems since their advent in the 1990s. These tools were originally envisioned as supplementary legal means for copyright owners to prevent unauthorized copying and distribution of their works via digital technologies. The introduction of anti-circumvention rules in the 1996 *World Copyright Treaty*[2] led to enormous scholarly concern over the preservation of exceptions and limitations and the public domain. These concerns envisioned a dark future. We were warned that TPMs would curtail user privacy,[3] undermine public interest exceptions to copyright, and push the entirety of copyright law into obscurity. Experts cautioned that copyright law itself may be supplanted by automated and technologically enforced rules predetermined by rightsholders.[4]

While this future has been realized in many respects, TPMs were only part of what has brought it about. The distribution of digital media has changed drastically over the past two decades. Physical embodiments of copyright works such as books and optical discs have been largely relegated to nostalgia.[5] Replaced by streaming media platforms, eBooks, and subscription-based access models, the threats of digital copying and online sharing are not quite the same as they once were. In many respects, today's digital media content distribution models have bypassed the problems of unauthorized reproduction through new business models and private ordering mechanisms. Many would be forgiven for believing that whatever doomsday "end of copyright" prophecies may persist in today's cloud and streaming world, the public interest harms posed by TPMs have largely faded into irrelevance.

But the old cries of concern regarding the consequences of TPMs have taken on a new life in recent years. The widespread proliferation of computerized devices and the conversion of previously analog objects into computerized appliances have broadened the scope, application, and impacts of TPMs. Rather

---

1 Cory Doctorow, "The Coming War on General Computation" (Speech before the 28th Chaos Communication Congress, Berlin, December 2011), online: < joshuawise.com/28c3-transcript >.

2 *World Intellectual Property Organization Copyright Treaty*, 20 December 1996, 2186 UNTS 38542 (entered into force 6 March 2002) at 11 [*WCT*].

3 Ian Kerr, "To Observe and Protect? How Digital Rights Management Systems Threaten Privacy and What Policy Makers Should Do About It" in Peter K Yu, ed, *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age* (Westport, CT: Praeger Publishers, 2007).

4 Julie E Cohen, "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them" (1997) 12:1 BTLJ 161 at 180 — 81.

5 Aaron Perzanowski & Jason Schultz, *The End of Ownership* (MIT Press, 2016) at 35.

than to serve as the guardian of digital media, today's device firmware TPMs prevent access to crucial device firmware. This issue is not limited to a narrow class of products or technologies. As evidenced by the current global microchip shortage, seemingly every product — refrigerators, hairbrushes, agricultural equipment, lightbulbs, cars, hot tubs, and coffee machines — now have computer chips embedded in their design.[6]

In effect, firmware TPMs can inhibit socially beneficial activities like repair, modification, interoperability, innovation, and diagnosis. In this way, device firmware TPMs reinvigorate the decades-old concerns about anti-circumvention laws and create negative externalities in new areas. In the United States, the constitutionality and free speech implications of anti-circumvention laws form the basis of ongoing litigation[7], and other countries have taken steps toward curtailing the negative effects of TPMs on innovation and repair.[8] Largely unforeseen at the turn of the millennium, governments, policy experts, and advocates are now awakening to the fact that device firmware TPMs are producing a number of negative externalities on markets, the environment, and the reasonable expectations of personal property ownership in tangible things.

This article examines the "access control" approach to TPMs, an approach that has taken hold in several jurisdictions around the world, beginning with the United States and since spreading to Canada, Australia, Japan, and many others. It analyzes this approach to TPMs where the underlying subject of protection is device firmware. In contrast to the expressive or creative works more conventionally regarded as copyrightable subject-matter, firmware is predominantly utilitarian in function. It regulates the basic and low-level functioning of myriad computerized devices and components. With the proliferation of Internet of Things ("IoT") devices and embedded system design, firmware is now ubiquitous. Yet, the expansive access control approach to TPMs permits manufacturers to legally cordon it off beyond the reach of users and device owners. As a result, firmware TPMs can become controls over the use and management of physical things. Through their ability to functionally "run" with objects, their durability, and the ubiquity of the restrictions they impose,

---

6 Leo Kelion, "Why Is There a Chip Shortage for Computers and Cars?," *BBC News* (5 February 2021), online: < www.bbc.com/news/technology-55936011 > .

7 Corynne McSherry & Kit Walsh, "EFF Asks Appeals Court to Rule DMCA Anti-Circumvention Provisions Violate First Amendment," *Electronic Frontier Foundation* (13 January 2022), online: < www.eff.org/press/releases/eff-asks-appeals-court-rule-dmca-anti-circumvention-provisions-violate-first > .

8 See Innovation, Science and Economic Development Canada, "A Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things" (2021) at 20, online (pdf): < www.ic.gc.ca/eic/site/693.nsf/vwapj/ConsultationPaper-AIEN.pdf/$file/ConsultationPaperAIEN.pdf > [Innovation]; and Australian Government Productivity Commission, "Right to Repair: Productivity Commission Inquiry Report No. 97" (29 October 2021) at 35, online (pdf): < www.pc.gov.au/inquiries/completed/repair/report/repair.pdf > .

firmware TPMs can resemble property interests in objects held or reserved by third parties.

The present analysis looks to precisely these sorts of instances, with smartphones, agricultural equipment, and video game consoles as examples. Looking to the common law of personal property, it then canvasses the doctrinal skepticism and distaste for chattel servitudes. Broadly, servitudes are durable interests held by third parties which run with property and bind successive owners. Within the law of real property, easements are perhaps the tritest example of servitude. Analogous property interests in the context of movables or chattel, however, are something that the common law has been loath to recognize. Analogous doctrinal skepticism also exists within the civil law tradition.[9] In analogizing device firmware TPMs as *de facto* servitudes on personal property, this analysis draws upon the common law's reluctance to recognize chattel servitudes for guidance on how to recalibrate access control TPMs within and outside of copyright law. In effect, it draws upon the policy reasons for rejecting chattel servitudes to better understand how to curtail the negative externalities on personal property ownership posed by firmware TPMs.

To date, the prevailing policy rationales for curtailing TPM overreach have been based in copyright doctrine and competition policy. Scholars and commentators have often pointed to three main costs of TPMs: their tendency to undermine the public domain and fair use; their effect of reducing access to creative works by eliminating secondary (used) markets; and their harms to competition and innovation.[10] The result has been a tendency to scrutinize the scope and content of TPM laws by measuring them in relation to copyright's balance of exclusive rights with the public interest or competition policy's distaste for restraints of trade. In either case, the focus in these approaches is centred on the content of TPM restrictions rather than their effects on personal property rights. The larger aim of this analysis, therefore, is to investigate whether the common law of property can provide a further analytical and normative perspective for guiding TPM policy reform.

This article is not the first to look to the law of tangible property (and personal property servitudes in particular) for normative guidance in the intellectual property and electronic commerce areas. Much of the existing scholarship in this area builds on the work of Zechariah Chafee Jr., who closely examined the judicial treatment of personal property servitudes under the common law.[11] He found that personal property servitudes have been generally

---

[9] See Athanassios Nicholas Yiannopoulos, "Predial Servitudes; Creation by Title: Louisiana and Comparative Law" (1968) 29:1 La L Rev 1; and Michele Graziadei, "The Structure of Property Ownership and the Common Law / Civil Law Divide" in Michele Graziadei & Lionel Smith, eds, *Comparative Property Law: Global Perspectives* (Cheltenham, UK: Edward Elgar, 2017), 71 — 99.

[10] John A Rothchild, "The Social Costs of Technological Protection Measures" (2006) 34:4 Fla St UL Rev 4 1181 at 1199.

[11] Zechariah Chafee Jr., "Equitable Servitudes on Chattels" (1928) 41:8 Harv L Rev 945;

rejected for sound public policy reasons but may nevertheless persist in certain cases and find utility in the future. Upon the advent of computer software licensing practices in the 1990s, Chafee's work was revisited by Thomas Hemnes, who examined whether the time had finally come to recognize personal property servitudes in the form of restrictive software licensing terms.[12] Molly Shaffer Van Houweling also traced the normative basis for IP exhaustion back to the social costs underlying the common law's skepticism of personal property servitudes.[13]

More recently, the proliferation of IoT devices gave reason for Christina Mulligan to investigate manufacturers' terms of service and licensing practices.[14] She reasoned that the "downstream control over software" present in these terms of service provides manufacturers with *de facto* servitudes over personal property. She cautioned that the resulting indefinite control by manufacturers has the potential to cause several social and economic harms.

Building on this line of scholarship, this article seeks to explore similar questions in the context of firmware TPMs as *hardware-based* restrictions on the use and management of tangible property. It begins with a survey of how TPM laws have been shaped to protect firmware protections, an overview of trusted system design, and a summary of the impact of the *Lexmark v. Static Controls*[15] decision in shaping future implementation of firmware TPMs. It then surveys some contemporary uses and implementations of firmware TPMs in various products and their impact on the personal property ownership expectations of consumers. In the second part, the shortcomings of dominant approaches to curtailing TPM overreach are canvassed, including enacting new or broadened exceptions permitting circumvention and curtailing anti-competitive uses of TPMs through competition policy. Third, a comparison is drawn between the negative impacts on personal property ownership facilitated through firmware TPMs and the common law's resistance to enforcing servitudes on chattels or movables. Points of convergence on this point are identified, including increased information costs, restrictions on future uses, and the effects of creating idiosyncratic property rights on third parties. Finally, implications are drawn from these points of convergence, including the need for future TPM policy to

---

and Zechariah Chafee Jr., "The Music Goes Round and Round: Equitable Servitudes and Chattels" (1956) 69:7 Harv L Rev 1250.

[12] See Thomas MS Hemnes, "Restraints on Alienation, Equitable Servitudes, and the Feudal Nature of Computer Software Licensing" (1994) 71:3 Denv UL Rev 577; and Glen O Robinson, "Personal Property Servitudes" (2004) 71:4 U Chicago L Rev 1449 at 1455.

[13] Molly Shaffer Van Houweling, "Exhaustion and Limits of Remote-Control Property" (2016) 93:4 Denv L Rev 951.

[14] Christina Mulligan, "Personal Property Servitudes on the Internet of Things" (2016) 50:4 Ga L Rev 1121.

[15] *Lexmark International v. Static Control Components*, 387 F.3d 522 (6th Cir., 2004) [*Lexmark*].

stress the importance of notice, technical standardization and classification, and temporal limitation on the protection of firmware TPMs.

II. DEVICE FIRMWARE TPMS AND PARACOPYRIGHT

TPMs are very loosely defined in both international legal treaties and national copyright statutes. The 1996 *World Copyright Treaty*'s ("WCT") Article 11 defines TPMs as "effective technological measures that are used by authors in connection with the exercise of their rights. . .and that restrict acts, in respect of their works, which are not authorized by the authors concerns or permitted by law."[16] Though this wording suggests a strong connection between the restricted acts and the exercise of exclusive rights, a more expansive approach has gradually taken shape internationally.[17] The impetus for this was the United States' *Digital Millennium Copyright Act* and the so-called "access right."[18] Through a series of bilateral trade agreements, many states around the world have since mirrored the DMCA's TPM approach by enacting broad definitions.[19] For example, Canada defines a TPM as "any effective technology, device, or component that, in the ordinary course of its operation, controls access to a work[. . .]"[20] Australia's *Copyright Act* adopts a very similar wording.[21] The effect is to treat TPM circumvention as *de facto* unlawful, regardless of the use made of works protected by them.

Shortly after the introduction of the access right, experts were quick to point out numerous pitfalls and drawbacks to this approach.[22] Concerns were raised over the absence of an exception permitting TPM circumvention for purposes unrelated to copyright, or which could otherwise preserve activities that fall within the ambit of fair use and fair dealing doctrines.[23] But in the end, the

---

16 *Supra* note 2.

17 See Ian Brown, "The Evolution of Anti-Circumvention Law" (2006) 20:3 Intl Rev L Comp & Tech 3 at 239 — 60.

18 *Digital Millennium Copyright Act,* 17 USC § 1002(c) (Supp V 1993) [*DMCA*].

19 Commission of the European Communities, "Green Paper on Copyright and the Challenge of Technology: Copyright Issues Requiring Immediate Action" COM(88) 172 final; Commission of the European Communities,"Green Paper: Copyright and Related Rights in the Information Society" COM(95) 382 final; see also Marlize Conroy, "A Comparative Study of Technological Protection Measures in Copyright Law" (LLD Thesis, University of South Africa, 2009), online: < uir.unisa.ac.za/handle/10500/2217?show = full > .

20 *Copyright Act,* RSC 1985, c C-42, s 41 (Canada). See also *DMCA*, supra note 18 at 1201a: ". . .a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."

21 *Copyright Act 1968* (Cth), 1968/63, s 10(1) (Australia).

22 Dan L Burk, "Anticircumvention Misuse" (2003) 50:5 UCLA L Rev 1095 at 1102.

23 See Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised" (1999) 14:2 BTLJ 519 at 543; and Carys

restrictive "access control" approach prevailed. Beyond its impacts on the public domain and lawful uses, the right of access granted original equipment manufacturers ("OEMs") of computerized devices a new platform for technological design. Sometimes referred to as "paracopyright"[24] or "pseudocopyright," this approach to TPMs enabled device manufacturers to envision a new paradigm of restrictions, one that could extend to the control and operation of devices and machines the primary purpose of which is not to embody copyright works.

Two factors accelerated the development of this paracopyright paradigm. The first is the lack of conceptual limitation regarding what exactly a TPM is or can be. This ambiguity can be traced back to early movements toward the protection of copyright works in the digital environment. In the 1995 *Intellectual Property and the National Information Infrastructure Report* (the "NII Report"), the US Information Infrastructure Task Force drew a very vague picture of technological protection, encompassing a "variety of technologies, based in software and hardware, to protect them against unauthorized uses of their information products and services."[25] A similarly vague picture was drawn by the European Commission in its successive Green Papers on copyright and technological protection.[26]

The ambiguity surrounding the scope of these technologies has persisted through to the present day. There remains no agreed-upon scope or limit to the types of technologies that can be used as a TPM.[27] Contemporary implementations have ranged from encryption to online authentication to physical dongles containing a piece of hardware that must be plugged into a device for its software to function.[28] Though arguably some limitations remain in that TPMs must be "effective," modern innovation has facilitated seemingly infinite means of controlling unauthorized uses of both software and hardware.

Craig, "Locking Out Lawful Users: Fair Dealing and Anti-Circumvention in Bill C-32" in Michael Geist, ed, *From Radical Extremism to Balanced Copyright: Canadian Copyright and the Digital Agenda* (Toronto: Irwin Law, 2010) at 188 — 91.

[24] Animesh Ballabh, "Paracopyright" (2008) 30:4 Eur IP Rev 138.

[25] US, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (US Government Printing Office, 1995) at 189 [*NII Report*].

[26] See e.g. Amendments to the *Japanese Copyright Act* and the *Unfair Competition Prevention Act* as part of Japan's Law No 33 [2011] and Law No 43 [2012] in Copyright Research and Information Center, "Copyright Law of Japan" (October 2014) at 15, online (pdf): <www.cric.or.jp/english/clj/doc/20150227_October,2014_Copyright_Law_of_Japan.pdf>.

[27] Zhaofeng Ma, "Digital Rights Management: Model, Technology and Application" (2017) 14:6 China Communications 156.

[28] Office of the Privacy Commissioner of Canada, "Digital Rights Management and Technical Protection Measures" (November 2006), online: <web.archive.org/web/20160414002554/http://www.priv.gc.ca/resource/fs-fi/02_05_d_32_e.asp>.

The second factor accelerating the paracopyright design paradigm is the ubiquity of embedded computer systems. The rise of "smart" products and IoT devices has seen the conversion of previously inert everyday objects into a litany of computerized machines. In some cases, this trend has produced products of questionable necessity, including the Hidrate Spark smart water bottle,[29] the Kérastase smart hairbrush,[30] and the Egg Minder.[31] Beyond such frivolous consumer products, however, embedded system design has also gradually taken root in key manufacturing sectors, including industrial machinery, medical equipment, and the automotive industry.[32]

In the world of embedded systems, code and hardware are codependent.[33] In contrast to software experienced at the user level, device firmware is what enables physical function in these systems. These are functions like blinking lights on an internet router, ABS brakes to actuate on a car, the colour profile of an electric display, and the cadence of pacemakers.[34] Most of today's embedded system devices feature general-purpose computing hardware that runs in accordance with manufacturer-stipulated firmware instructions. Though essential for hardware to function, firmware is technically a class of software — a protectable subject-matter under copyright law. This codependent relationship results in physical devices being indirectly safeguarded by firmware TPMs from unauthorized uses and manipulation.

The inextricability of firmware TPMs from the devices in which they are incorporated distinguishes them from TPMs that are used to protect digital media content. In the case of digital media stored on physical media or within devices, for example, value is derived from the copyrighted content.[35] But firmware has no real intrinsic value. Irrespective of its copyright originality, firmware functions as a series of utilitarian instructions. In this way, firmware

---

[29] Hidrate Spark Smart Water Bottle (Kickstarter), online: <www.kickstarter.com/projects/582920317/hidrateme-smart-water-bottle> (last visited 12 December 2021).

[30] Andrew Liszewski, "L'Oreal's Smart Hairbrush Knows More About Your Hair Than Your Salon Does" (4 January 2017), online: *Gizmodo* <www.gizmodo.com.au/2017/01/loreals-smart-hairbrush-knows-more-about-your-hair-than-your-salon-does/>.

[31] "Egg Minder Smart Tray Lets You Remotely Check the Freshness of Your Eggs" (5 July 2013), online: *Moving Global Services* <movingglobalservices.wordpress.com/2013/07/05/egg-minder-smart-tray-lets-you-remotely-check-the-freshness-of-your-eggs/>.

[32] Michael Accardi, "How the Auto Industry Let the Semiconductor Shortage Get So Bad" (31 December 2021), online: Muscle Cars & Trucks <www.musclecarsandtrucks.com/global-automotive-industry-microchip-shortage-how-it-happened/>.

[33] Jack Ganssle, *The Firmware Handbook: The Definitive Guide to Embedded Firmware Design and Applications* (Oxford: Elsevier, 2004) at vx.

[34] Justin Z Lee et al, "Pacemaker Firmware Update and Interrogation Malfunction" (2019) 5:4 HeartRhythm Case Reports 213, online: <www.ncbi.nlm.nih.gov/pmc/articles/PMC6453543/>.

[35] Daniel C Higgs, "Lexmark International, Inc. v. Static Control Components, Inc. & Chamberlain Group, Inc. v. Skylink Technologies, Inc.: The DMCA and Durable Goods Aftermarkets" (2004) 19:1 BTLJ 59 at 67.

TPMs can control function of what economists refer to as *durable goods*[36] — particularly those that derive their value independently from the protected software. Though to a large extent computerization makes this dynamic possible, the lack of limitation on the techniques that can constitute TPMs offers manufacturers a platform to imagine a whole host of new, legally protected user restrictions.[37]

(a) Trusted System Design

Despite the lack of limitation on what may functionally constitute a TPM, TPMs require something more than merely coordinating software and hardware. Though some TPMs (such as digital watermarks) are self-executing, most firmware TPMs are built upon trusted computing technology.[38] In very general terms, trusted computing is a design model for software and hardware that can be "relied upon to follow certain rules."[39] This type of computer system relies upon built-in hardware that creates a foundation of trust for secondary software processes.[40] This design technique enables manufacturers to ensure that devices, products, and systems will behave in predetermined ways by enforcing preprogrammed policies and restricting program access.[41] The early trusted systems were developed primarily to ensure information security for government and military applications,[42] but the design approach has since become the dominant platform for the development of TPMs that can restrict device functionality and access to firmware.

The potential ills of trusted computing have been the subject of much controversy among software developers and activists. Of particular concern is the potential for trusted system design to limit the autonomy and choices of users in relation to the computers and devices that they lawfully own. Richard Stallman, a well-known programmer and free software activist, cautioned back in 2002 that trusted computing "will make sure your computer will systematically disobey

---

[36] Ronald H Coase, "Durability and Monopoly" (1972) 15:1 JL & Econ 143.

[37] John A Rothchild, "Economic Analysis of Technological Protection Measures" (2005) 84:2 Or L Rev 489 at 493 — 96.

[38] Spencer Cheng & Avni Rambhia, "DRM and Standardization — Can DRM Be Standardized?" in Eberhard Becker et al, eds, *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (New York: Springer, 2003) at 197.

[39] Mark Stefik, "Trusted Systems," *Scientific American* (March 1997) 78 at 79, online (pdf): < www.markstefik.com/wp-content/uploads/2011/03/1997-Trusted-Systems-Scientific-American1.pdf > .

[40] Chris J Mitchell, "What Is Trusted Computing?" in CJ Mitchell, ed, *Trusted Computing* (London: Institute of Engineering and Technology, 2005) at 3.

[41] Paul England & Marcus Peinado, "Authenticated Operation of Open Computing Devices" (Australasian Conference on Information Security and Privacy, 21 June 2002) 346.

[42] Cheng & Rambhia, *supra* note 38 at 188.

you. In fact, it is designed to stop your computer from functioning as a general-purpose computer. Every operation may require explicit permission."[43]

The foregoing reveals that manufacturers have several tools at their disposal to limit, control, and restrict user behaviour. The proliferation of products with embedded systems means that firmware is now an essential input for controlling how, when, and by whom various products and devices can be used. Accessing and manipulating that firmware can be protected by TPMs, the implementation of which may include a trusted system design model that has both a physical manifestation and hardware component. In these cases, users are bound to the use of products and devices on the terms set by its manufacturer. And where users attempt to circumvent these TPMs without authorization, the crucial role of firmware may render the entire device inoperable or limit its function until the original manufacturer configuration set by the manufacturer is restored. In this sense, firmware TPMs operate as self-contained compliance systems, which not only delineate rules, but also ensure that they are followed.[44]

(b) The *Lexmark* decision

Perhaps the most influential development for the future implementation of trusted system design in firmware TPMs was the 2004 *Lexmark v. Static Control Components* decision of the United States Court of Appeal for the Sixth Circuit. At issue was an authentication microchip used by Lexmark in its printer toner cartridges. The microchip enabled the printer and the toner cartridge to enter an authentication sequence to verify that the cartridge was "authentic." At a functional level, two computer programs were implicated in this process: the Toner Loading Program ("TLP") and the Printer Engine Program ("PEP"). The PEP (stored on the printer) controlled the operations and functions of the printer itself, while the TLP (stored within the toner cartridge's microchip) measured the toner level in the cartridge. Though neither program was encrypted, the printer would download the TLP stored on the toner cartridge's microchip at the start of each printing job to enable the printer and cartridge to interoperate.[45]

The defendant, Static Control Components ("SCC") manufactured microchips, and specifically a chip known as "SMARTEK," which included a copy of the TLP program. The SMARTEK chip enabled third parties to manufacture, refurbish, and refill useable toner cartridges sold at a lower cost than those sold by Lexmark. In response, Lexmark sued (in part) for unlawful circumvention of its TPMs protecting both the TLP and the PEP. In the end, the court rejected Lexmark's anti-circumvention claims. In reaching its decision, the

---

[43] Richard Stallman, "Can You Trust Your Computer?" (GNU Operating System, 2002), online: < www.gnu.org/philosophy/can-you-trust.html > .

[44] Tarleton Gillespie, "Designed to 'Effectively Frustrate': Copyright, Technology and the Agency of Users" (2006) 8:4 New Media & Society 651 at 653.

[45] For a more detailed and technical explanation of the interaction between the TLP and PEP, see Zohar Efroni, "A Momentary Lapse of Reason: Digital Copyright, the DMCA and a Dose of Common Sense" (2005) 28:3 Colum J L & Arts 249 at 258 — 64.

court found that the PEP stored on the printer was neither encrypted nor protected by any form of access control. Importantly, it could be readily accessed through the printer's memory without the TLP at all. In respect of the TLP, the court rejected the claim that the SMARTEK chip constituted unlawful "access" to the TLP. Rather, the SMARTEK chip physically and functionally replaced the TLP as configured by Lexmark, which itself was deemed purely functional and uncopyrightable. Overall, this decision highlighted that the mere facilitation of an authentication sequence between two otherwise unencrypted or uncopyrightable programs will not constitute circumvention of a TPM; something more is required.

While in some ways the *Lexmark* decision expresses judicial reluctance to accept firmware TPMs that do not principally protect copyright works, it also pointed to a technical workaround for manufacturers. Much of the court's reasoning in *Lexmark* hinged on the fact that the PEP was accessible by means other than using the toner cartridge's microchip. In being unencrypted, the PEP was readily accessible by printer owners. Had the PEP and TLP been designed within a trusted system design model, however, the story would likely have been different. In other words, TPMs will not be considered "effective" where the overall device design leaves access to a protected work possible by other means.[46] The result is that device manufacturers can easily meet this standard by ensuring that embedded device firmware is encrypted, or otherwise not accessible other than through circumvention. In effect, the court's decision in *Lexmark* pointed to an easy way out for manufacturers to avoid the same fate as the printer manufacturer by implementing encryption and trusted system design in their design.

(c) Examples of Contemporary User Restrictions

Over the past several decades, the range of devices and products restricted by firmware TPMs has grown substantially. Experts in the consumer and intellectual property realms have drawn attention and concern to some of the more notorious consumer-facing instances of firmware locking, including coffee makers and kids' toys.[47] Others have been discovered and reported by users on online forums.[48] The overall picture being painted is an increasingly wide range of products and devices that undermine personal property ownership through restrictions on use, modification, repair, and resale.

One example is Nintendo game consoles, which have long included firmware restrictions to ensure that only legitimate or authorized games can be used in them. In practice, these firmware restrictions prevent users from not only playing

---

[46] *Lexmark*, *supra* note 15 at 547.

[47] See e.g. Perzanowski & Schultz, *supra* note 5, for the Keurig 2.0 smart coffee maker example at 144 — 50.

[48] u/techyg, "PSA: Use caution when buying a used AirTV 2, it may be locked" (16 August 2021), posted on r/slingtv, online: <www.reddit.com/r/slingtv/comments/p5rysx/psa_use_caution_when_buying_a_used_airtv_2_it_may/>.

infringing copies of games in these systems, but also engaging in lawful activities like listening to music CDs games created by users (known as ''homebrew'' games). In other words, by default, the hardware will not run whatever code or program the user chooses — only those authorized by Nintendo. Users have developed several different hardware modification techniques to circumvent these firmware TPMs. Known as ''mod chips,'' implementation of these devices can involve soldering new microchip components into the console's circuitry or plugging in additional components that interrupt the Nintendo console's factory configurations.

Though similar device firmware TPMs exist in other game consoles, Nintendo has shown willingness to aggressively police the sale and use of mod chips through litigation. One such instance was part of the 2014 decision of the CJEU in *Nintendo v. PC Box*, where Nintendo sought to curtail the defendant's sale of mod chips on the basis that it constituted the distribution of unlawful circumvention devices.[49] In part, the CJEU was asked whether Directive 2001/29/EC's[50] (the ''InfoSoc Directive'') anti-circumvention provisions extended beyond those TPMs incorporated into digital media discs to include firmware TPMs in the console hardware. With the caveat that such TPMs must be ''proportionate'' to the protection of exclusive rights in order to be considered ''effective,'' the CJEU found that Nintendo's firmware TPMs were indeed protected.[51] It stopped short, however, of providing a framework for measuring proportionality or offering any limitation on the type of techniques that may constitute valid TPMs.

Just a few years later, Nintendo was back in court with a mod chip installer in Canada in *Nintendo of America Inc. v. King,* a 2017 decision of the Federal Court.[52] In comparison to *Nintendo v. PC Box*, the consequences of Canada's adoption of the explicit ''access control'' approach to TPMs resulted in a much harsher outcome for the respondent. At issue was the respondent's installation of mod chips in Nintendo's DS, 3DS, and Wii consoles. This required soldering and circumventing Nintendo's firmware TPMs. In contrast to the CJEU, Canada's Federal Court rejected the idea that firmware TPMs had to be proportionate to the protection of exclusive rights. It found that firmware TPMs were not required to present any barrier to copying or copyright's exclusive rights to be considered ''effective.'' In the end, Nintendo was awarded over $21-million CAD in statutory and punitive damages, as well as injunctive relief against the respondent mod chip installer for its circumvention of Nintendo's firmware

---

[49] *Nintendo Co. Ltd. and Others v. PC Box Srl* (C-355/12) EU:C:2014:25; [2014] EUECJ C-355/12 (CJEU) [*Nintendo v PC Box*].

[50] EC, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society,* [2001] OJ, L 167/10 [*InfoSoc Directive*].

[51] *Supra* note 49 at 27 — 31.

[52] *Nintendo of America Inc. v. King*, 2017 FC 246, 2017 CarswellNat 650, 2017 CarswellNat 7098 (F.C.).

TPMs. The decision has created a chilling effect on innovation and experimentation in several industries that require manipulation of OEM hardware.[53]

Device firmware TPMs implementation also extends far beyond consumer and entertainment devices. Similar techniques are well established in the agricultural equipment sector, led principally by John Deere's line of farming combines and machinery. The clearest example is John Deere's X9 combine, which is a is a $1-million USD piece of farming equipment featuring a proprietary hardware interface and an onboard computer (known as a "tECU") that can measure ambient temperature, soil hydration, GPS location, hydraulic pressure, and other variables. Like all mechanical things, however, these machines require maintenance and replacement parts.

To the dismay of farmers working on tight seasonal timelines, the physical interface coupled with the tECU does not let just anyone carry out repair and maintenance tasks. Connecting to the tECU requires special cables and software sold exclusively by John Deere to bypass firmware restrictions and receive diagnostic information.[54] These special tools are only made available to John Deere-authorized dealers and servicepeople.[55] And even where access to the onboard software is not strictly necessary for replacing parts, the tECU can prevent the use of those parts through co-verification and "activation" processes. In effect, the machine will not work unless the replacement part is activated by the central computer. Similar tactics are being deployed in the automotive industry, where manufacturers use a practice known as "VIN burning" to allow manufacturers to restrict the use of parts to a single car through firmware controls.[56]

No TPM system is infallible, however. Farmers have turned to circumventing[57] John Deere's TPMs using grey market firmware and cables to access diagnostic information and carry out repairs themselves.[58] Concerns over the future of agriculture and anti-competitive behaviour by John Deere has

---

[53] Innovation, *supra* note 8 at 24.

[54] Kevin O'Reilly, "Deere in the Headlights: How Software that Farmers Can't Access Has Become Necessary to Tractor Repair" (February 2021), online: *US PIRG* < uspirg.org/feature/usp/deere-headlights > .

[55] See Anthony D Rosborough, "Unscrewing the Future: The Right to Repair and the Circumvention of Software TPMs in the EU" (2020) 11 JIPITEC 26-48 [Rosborough, "Unscrewing the Future"].

[56] US, Federal Trade Commission, "Nixing the Fix: An FTC Report to Congress on Repair Restrictions" (May 2021) at 23, online: < www.ftc.gov/reports/nixing-fix-ftc-report-congress-repair-restrictions > .

[57] Jenny List, "The Icon of American Farming that You Now Have to Hack to Own" (24 March 2017), online (blog): *Hackaday* < hackaday.com/2017/03/24/the-icon-of-american-farming-that-you-now-have-to-hack-to-own/ > .

[58] Jason Koebler, "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware," *Vice* (21 March 2017), online: < www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware > .

resulted in the United States' Librarian of Congress issuing specific exemptions to US anti-circumvention law for repairing agricultural equipment. Initially issued in 2015, these exemptions have been continually renewed.[59]

In addition to game consoles and agricultural equipment, firmware TPMs are also found in our pockets. Preventing unauthorized modification and repair, Apple has deployed restrictive device firmware TPMs in some generations of iPhones and iPads. In 2016, iPhone 6 owners learned that their iPhone had been completely disabled (known as "bricking") during a software update after receiving an unauthorized repair.[60] Being the most fragile and exposed part of a smartphone, the screen is the part most likely in need of replacement. And when an iPhone 6's screen is replaced, the home button is often replaced as part of a single assembly. The iPhone 6's home button incorporates a fingerprint scanner, which cannot be reconfigured or replaced without authorization from Apple and verification through the device's firmware.[61] The result is that many iPhone owners (particularly in the developing world and remote places) were presented with "Error 53" during software updates weeks or months later. The error was presented only after having wiped all the data on the phone, including its operating system. In effect, the user's iPhone was reduced to a paperweight unless restored by Apple. The frustration resulting from the Error 53 debacle resulted in Apple being fined $9-million AUD under Australia's consumer laws in 2018.[62]

Though each of the above firmware TPM examples are distinct in their manner of implementation, they share a common theme. In relying on trusted system design and computerization, they restrict activities entirely unrelated to copyright. They take general computing devices and narrow their application to pre-determined tasks on solely the manufacturer's terms. Importantly, this can often run counter to the expectations of those who own the devices.

(d) Impacts on Ownership Expectations

Whether in relation to repair, modification, or diagnosis, the restrictions on user autonomy posed by firmware TPMs are often effective and wide ranging.

---

[59] US, Copyright Office, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," *Library of Congress* (28 October 2021), online: <www.federalregister.gov/documents/2021/10/28/2021-23311/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control>.

[60] Miles Brignall, "'Error 53' Fury Mounts as Apple Software Update Threatens to Kill Your iPhone 6," *The Guardian* (5 February 2016), online: <www.theguardian.com/money/2016/feb/05/error-53-apple-iphone-software-update-handset-worthless-third-party-repair>.

[61] Kyle Wiens, "What's Up With Error 53?" (5 February 2016), online: *iFixit* <www.ifixit.com/News/7889/whats-up-with-error-53 >.

[62] Mike Cherney, "Apple Fined as Customers Win a Right-to-Repair Right," *The Wall Street Journal* (19 June 2018), online: <www.wsj.com/articles/apple-fined-as-customers-win-a-right-to-repair-fight-1529399713>.

They run counter to the ingrained ownership expectations of users and their right to use devices beyond what the manufacturer permits.[63] The ways in which manufacturers can retain this control suggest that something less than ownership is being conveyed at the time of sale.[64] Scholars and experts in the consumer law realm have labelled some of these devices "tethered appliances" because they enable vendors to predetermine and ensure the scope of functionality indefinitely.[65] Exploring this dimension of firmware TPMs and their impacts on consumer perceptions is important for the discussion in relation to personal property servitudes that follows in subsequent parts of this paper.

At first blush, the notion of property "ownership" implies a type of *in rem* absolute dominium over things. However, this generally does not accord with how we enter property relationships in today's world, nor does it align with contemporary property theory. In recent times, common law property theory has coalesced around the "bundle of rights" theory,[66] where property ownership can be fractionalized among several individuals, each of whom can hold distinct entitlements in relation to a thing.[67] Each of these entitlements may be considered on its own as a type of property right or "interest" in the thing. An influential articulation of this understanding of property was put forward by A.M. Honoré in his 1961 essay, "Ownership." There, he laid out a generally accepted list of eleven property ownership "incidents":

> Ownership comprises the right to possess, the right to use, the right to manage, the right to the income of the thing, the right to the capital, the right to security, the rights or incidents of transmissibility and absence of term, the prohibition of harmful use, liability to execution, and the incident of residuary[. . .][68]

No single incident of ownership among the list of eleven is necessary to designate the owner of a particular thing.[69] In this sense, there is no primacy or hierarchy among the list of incidents. Rather than delineating a set of conditions or rules for property ownership, the list is best understood as a way of describing the entirety of ownership's constituent elements.

---

63 Kyle Wiens, "Self-Repair Manifesto" (9 November 2010), online: *iFixit* < www.ifixit.com/News/14266/self-repair-manifesto > .

64 Chris Jay Hoofnagle, Aniket Kesari & Aaron Perzanowski, "The Tethered Economy" (2019) 87:4 Geo Wash L Rev 783 at 809.

65 Jonathan L Zittrain, *The Future of the Internet — And How to Stop It* (London: Penguin, 2008) at 106.

66 Jane B Baron, "Rescuing the Bundle-of-Rights Metaphor in Property Law" (2013) 82:1 U Cin L Rev 57 at 62 — 67.

67 Abraham Bell & Gideon Parchomovsky, "A Theory of Property" (2005) 90:3 Cornell L Rev 531 at 546.

68 Tony Honoré, *Making Law Bind: Essays Legal and Philosophical* (Oxford: Clarendon Press, 1987) at 161.

69 *Ibid*. at 165.

There has been no shortage of critiques of the bundle of rights property theory over the years. Critics have pointed out that viewing property ownership as mere relationships between individuals reduces its social and normative significance, rendering it largely indistinguishable from contract.[70] Yet, few would argue against the notion that the bundle of rights theory comprises the consensus view of property in the common law world.[71]

Firmware TPMs can impact several of ownership's incidents in computerized devices depending on their implementation. Apple's Error 53 incident reveals that firmware TPMs can directly undermine the right to use, while the John Deere example reveals negative impacts on the right to manage. In other scenarios, firmware TPMs can also restrict resale, aligning quite closely to Honoré's right to capital or right to income.[72] The ownership impacts of firmware TPMs are not (in and of themselves) novel, however. One can think of many objects in our world that are subject to property interests held by multiple individuals. What makes firmware TPMs stand out in this regard is their tendency to conflict with the engrained ownership expectations of consumers.

We have come to expect varying degrees of "bundleness" in our ownership in different things. For example, we expect to take ownership of a car in a different way from a coffee maker. The ownership and use of a car is highly regulated. It involves title registration, insurance requirements, licensing, and often environmental and safety certifications as well. Cars are also commonly subject to purchase financing or leasing arrangements, leaving any number of ownership's incidents with third parties. Over time, we have developed expectations regarding this fractionalisation of ownership incidents and ownership asymmetries in relation to more bundled things like cars. We do not carry the same expectations for other things, however. Coffee makers do not require registration, insurance, or (in most cases) financing or leasing. Absent some clear agreement to the contrary, the coffee maker's owner expects to possess something closer to absolute dominium than does the owner of the car. In other words, our ownership expectations in relation to a given thing depends on the object or thing.

In a similar vein, whether an object is a physical embodiment of intellectual property also impacts our ownership expectations. The *in vacuo,* non-possessory nature of intellectual property rights means that merely having possession of a

---

[70] Thomas C Grey, "The Disintegration of Property" (1980) 22 NOMOS: Am Society for Political & Leg Philosophy 69 at 71.

[71] Bruce A Ackerman, *Private Property and the Constitution* (Yale University Press, 1977) at 26 — 27.

[72] See e.g. Jonathon Ramsey, "Tesla Reportedly Removing Paid-for Features After Used-Car Sales" (23 May 2020), online: *Autoblog* <www.autoblog.com/2020/03/23/tesla-removing-content-from-used-cars/> and "Device being locked in 24 hours due to trade in not complete" (14 October 2021), online: *Samsung* <eu.community.samsung.com/t5/tablets/device-being-locked-in-24-hours-due-to-trade-in-not-complete/td-p/4148435>.

thing does not entitle its possessor to do whatever he or she wishes with it.[73] Copyright and patent have long provided rightsholders with some degree of control over the use of tangible property possessed by others.[74] For example, upon purchase of a bicycle with a patented design, the buyer may change the bicycle's tires or handlebar configuration, and the buyer may sell or even destroy the bicycle. The purchaser may not, however, reproduce the patented design on another bicycle, sell those reproductions, or distribute them without licence or permission from the patent holder. The same is true of a physical book, where the book's owner is restricted from reproducing and distributing its contents despite lawfully "owning" it.

For objects that we ordinarily regard as embodiments of intellectual property, we have become accustomed to a more bundled understanding of property ownership. We implicitly recognize that our ownership of a patented bicycle or copyrighted book comes with certain caveats and limitations. We acknowledge that another (often remote) party holds certain entitlements to prevent certain acts as part of intellectual property's exclusive rights. We have developed these expectations with the engrained ownership expectations of consumers.

Automated restrictions imposed by TPMs upset our ownership expectations for two main reasons, however.[75] First, firmware TPMs generally implicate objects that we do not normally recognize as embodiments of intellectual property. Unlike a patented bicycle or book protected by copyright, the primary purpose of a printer, coffee maker, or farming combine is not to embody a protected work. It is to print, make coffee, or manage crops. Yet, firmware TPMs enable these core functions to be encapsulated within exclusive rights held by the manufacturer. Secondly, firmware TPMs differ from typical embodiments of intellectual property because they are embedded within the functioning of the device itself. As opposed to a shared rights relationship between the device owner and the manufacturer in a single object (e.g., a patented coffee maker design), firmware TPMs are direct and absolute functional controls. The consequence is an asymmetry between the *in vacuo* intellectual property-related interest in the object, and the degree of control afforded to the manufacturer by the firmware TPM. The device owner may use the coffee maker *to the extent and in the ways permitted* by the manufacturer. These limitations need not have any relationship

---

[73] Molly Shaffer Van Houweling, "Exhaustion and Personal Property Servitudes" in I Calboli & E Lee, eds, *Research Handbook on Intellectual Property Exhaustion and Parallel Imports* (Cheltenham: Edward Elgar, 2016) at 45 [Van Howling, "Exhaustion and Personal Property Servitudes"].

[74] Molly Shaffer Van Houweling, "Exhaustion and the Limits of Remote-Control Property" (2016) 93:4 Denv L Rev 951 at 952 [Van Howling, "Exhaustion and the Limits"].

[75] See e.g. Deirdre Mulligan, John Han & Aaron J Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of 'Personal Use'" (Proceedings of the 3rd ACM workshop on Digital Rights Management, October 2003) 77, online: < dl.acm.org/doi/10.1145/947380.947391 > .

to the manufacturer's underlying patent or copyright. In essence, this unhinged exercise of control runs contrary to our ownership expectations by extending the *in vacuo* nature of intellectual property rights to prohibit or permit uses that are unrelated to those rights.

III. SHORTCOMINGS OF THE PREVAILING REGULATORY APPROACHES

The negative impacts on device ownership caused by firmware TPMs can be viewed from several different legal perspectives. Though TPMs are a creature of copyright law, their use in firmware applications can transcend the protection of the exclusive rights provided by both copyright and patent laws. Naturally, this has resulted in calls for adjustments to anti-circumvention laws and has attracted the scrutiny of antitrust and competition policy. The following addresses these potential regulatory responses as well as their shortcomings in addressing the negative personal property ownership impacts of firmware TPMs.

(a) Permitting TPM Circumvention Through Copyright Exceptions

Perhaps the most intuitive route for addressing the negative externalities of TPMs is through enacting additional exceptions within copyright law to permit circumvention. Approaches to enacting exceptions vary between jurisdictions, but they generally take shape around permitting circumvention either for prescribed activities or for accessing specific types of works rendered inaccessible by TPMs.

The United States follows the latter approach. Its DMCA includes a rulemaking procedure led by the Librarian of Congress, which hears submissions from stakeholders and the public.[76] Every three years, exemptions permitting circumvention are assessed and renewed after measuring the actual or likely adverse affects in the ability "to make non-infringing uses [. . .] of a particular class of copyrighted works." The exemptions are then granted for specific classes of copyrighted works for a three-year period.[77] The exemptions granted to date have generally been quite narrow in scope. For example, an exception permitting circumvention of TPMs on game consoles is limited to the optical disc drive only.[78] Further limiting the utility of exemptions, the rulemakings do not permit the free circulation or "trafficking" of circumvention devices, but only the act of circumvention itself.[79] In effect, this restricts their application to mostly private acts of circumvention.

---

[76] *Supra* note 18 at 1201(a)(1)(C).

[77] *Ibid*. at 1201(a)(1)(D).

[78] *Nintendo v PC Box*, *supra* note 49 at 14: "For video game consoles, 'repair' is limited to repair or replacement of a console's optical drive and requires restoring any technological protection measures that were circumvented or disabled."

[79] *Supra* note 18 at 1201(a)(1)(E).

One shortcoming in this approach is that it requires that exempted circumvention activities have some connection to making "use" of copyright works protected by TPMs. In the case of firmware TPMs, however, the circumvention is not directed toward the use of software code but rather the hardware that it controls. In these instances, the adverse effects relate to the use and management of corporeal objects, which are not the actual subject of copyright protection. In some instances, it may even be that circumvention of firmware TPMs does not involve access or manipulation of software at all. Circumvention can be as simple as adding or removing a piece of hardware or circuitry to or from a device. In all, these types of scenarios do not resemble non-infringing uses of copyright works *per se* and may therefore not adequately be captured by this type of exemption process.

In other jurisdictions, however, the focus is not on specific classes of copyright works but rather on certain prescribed activities that necessitate circumvention. The United Kingdom[80] and Canada[81] permit circumvention for the purposes of aiding those with perceptual disabilities, law enforcement, encryption research, and other public-interest purposes. In contrast to the US, this approach is indifferent to the class of copyright work being protected by the TPM or to whether the work is "used." The European Union's anti-circumvention rules are bifurcated between distinct directives, but in general they follow the same approach of an exhaustive list of permitted acts.[82]

Though granting exceptions based on prescribed activities offers potentially greater opportunity to address the negative externalities of overprotection, both approaches show shortcomings in fully addressing the impacts of firmware TPMs on personal property ownership. There are two reasons for this. First, merely making it lawful to circumvent firmware TPMs does not mean that it will always be practically feasible to do so. Though some firmware TPMs can be circumvented through rudimentary techniques (such as removing a firmware "write protect" screw in a laptop[83]), many circumventions involve complete device disassembly, soldering, and technical skills beyond the reach of most people. Second, additional exceptions permitting circumvention do nothing to address the hidden and non-obvious nature of most firmware TPMs. In many instances, device owners may be unaware that the use restrictions on their device

---

[80] *Copyright, Designs and Patents Act 1988*, s 296ZA-E [CDPA].

[81] *Supra* note 20, ss 41.11 — 41.18. For a discussion of the application of these exceptions in relation to firmware TPMs, see Anthony D Rosborough, "If a Machine Could Talk, We Would Not Understand It: Canadian Innovation and the Copyright Act's TPM Interoperability Framework" (2021) 19 CJL & Tech 141 [Rosborough, "If a Machine Could Talk"].

[82] *InfoSoc Directive*, *supra* note 50 at art 6(4), and EC, *Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs*, [1991] OJ, L 122/42.

[83] See e.g. the 2013 Chromebook Pixel write protect screw: Kevin Fessler, "Remove the Write Protect Screw" (23 January 2018), online: *iFixit* < www.ifixit.com/Guide/Remove+the+Write+Protect+Screw/86362 > .

are the result of firmware TPMs, and even if they *do* know, they may not know whether circumvention is possible or feasible. In sum, merely adjusting anti-circumvention laws to provide additional lawful grounds for circumvention will not remedy the practical limitations posed by firmware TPMs on the use and management of devices by their owners.

(b) Antitrust and Market Competition Policy

An alternative or supplementary means of reducing the negative effects of firmware TPMs may be achieved through antitrust law or market competition policy.[84] As demonstrated by the Apple and John Deere examples, firmware TPMs can effectively restrain trade and restrict a whole host of market activity, including follow-on innovation and repair.[85] In this context, firmware TPM implementations may be deemed an anti-competitive industry practice where they result in tying or the abuse of dominant market positions through refusals to deal, or where they amount to the denial of an essential facility for secondary markets.[86]

Curtailing the anti-competitive effects of firmware TPMs through antitrust or competition law is not a purely hypothetical musing. Though decided on other grounds, *Lexmark v. Static Control Components*[87] and *Chamberlain v. Skylink Technologies*[88] (involving encrypted remote control garage door openers) both involved allegations of anti-competitive conducted facilitated through firmware TPMs. More recently, John Deere has been named in a class action antitrust suit filed in the United States District Court for the Northern District of Illinois for alleged violations of sections 1 and 2 of the US *Sherman Act*.[89] The violations, it

---

[84] Rothchild, *supra* note 37 at 507 — 13.

[85] Rosborough, "If a Machine Could Talk," *supra* note 81 at 151.

[86] There is terminological confusion between refusals to deal and the denial of essential facilities. In some instances, the concepts are used interchangeably. In general, however, the essential facilities doctrine is more explicitly endorsed in jurisdictions outside of the United States, and most notably the European Union. The essential facilities doctrine has never been formally applied under US antitrust law, but scholars have pointed out its conceptual overlap with refusals to deal. For an analysis of the overlap and conceptual distinctions between these terms and the doctrines they denote, see Csongor István Nagy, "Refusal to Deal and the Doctrine of Essential Facilities in US and EC Competition Law: A Comparative Perspective and a Proposal for a Workable Analytical Framework" (2007) 32:5 Eur L Rev 664.

[87] *Supra* note 18. See also Static Control Components' assertions that Lexmark's toner cartridge authentication systems were anticompetitive in *Static Control Components, Inc. v. Dallas Semiconductor Corporation and Lexmark International, Inc.*, 2003 Copr.L.Dec. P 28,656 (M.D. N.C., 2003), online (pdf): at <www.eff.org/files/filenode/Lexmark_v_Static_Control/antitrust_complaint.pdf>.

[88] *Chamberlain Group, Inc. v. Skylink Techs, Inc.*, 381 F.3d 1178 (Fed Cir., 2004).

[89] Dave Byrnes, "John Deere Accused of Monopolizing Tractor Repair Industry in Antitrust Suit," *Courthouse News Service* (12 January 2022), online: <www.courthousenews.com/john-deere-accused-of-monopolizing-tractor-repair-industry-in-antitrust-suit/>.

is alleged, are enabled by John Deere's reliance on firmware TPMs and its network of exclusive agreements with equipment dealers that keep a tight grip on diagnostic tools and software. In the class action complaint, the plaintiffs allege that John Deere's use of firmware TPMs to create this type of exclusion constitutes (among other things) conspiracy in restraint of trade, an unlawful tying arrangement, and monopolization of the repair services market.[90] The relief sought includes John Deere's permanent restraint from engaging in these anticompetitive practices and from adopting "any device having a similar purpose or effect" in the equipment it manufactures.[91] It remains to be seen whether the outcome of this litigation will impact or influence the TPM policy in the United States.

The European Union has had comparatively less occasion to address anti-competitive market behaviour enabled by firmware TPMs over the years. Nevertheless, in the widely cited *Magill* decision,[92] the CJEU found that in "exceptional circumstances" the exercise of intellectual property rights can amount to abusive conduct. This will more likely be the case where an intellectual property right acts as an indispensable product or service in a downstream or aftermarket and is withheld to exclude competition.[93] In the *Microsoft Corp* decision, for example, the European Commission found against Microsoft for its refusal to licence interoperability information necessary for competing products to work within its server products.[94] It is possible that the implementation and reliance on firmware TPMs could result in a similar finding under EU competition law, particularly in secondary markets that require circumvention for follow-on innovation, remanufacturing, repair, and servicing.[95] The feasibility of such a claim and finding may depend on the extent to which firmware TPMs are considered intellectual property rights in and of themselves. Their recognition as intellectual property rights may be necessary for the use of firmware TPMs to be captured by the precedent set in *Magill*.

As fruitful as antitrust and competition laws may be for curtailing the negative externalities caused by firmware TPMs on *markets*, however, this approach does little to ameliorate the impacts on personal property ownership.

---

[90] *Forest River Farms v. Deere & Co*., Doc. 1:22-CV-00188, 2022 WL 111030 (N.D. Ill., 2022) at 44, online (pdf): <www.courthousenews.com/wp-content/uploads/2022/01/forest-river-deere-complaint.pdf>.

[91] *Ibid* at 218.

[92] *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v. Commission of the European Communities* (Magill) (C-241 and 242/91P), [1995] ECR I-743; [1995] 4 CMLR 718 (CJEU).

[93] *Istituto Chemioterapico Italiano SpA and Commercial Solvents Corporation v. Commission of the European Communities* (C-6 and 7/73), [1974] ECR 223; [1974] 1 CMLR 309 (CJEU).

[94] *Microsoft Corp. v. Commission of the European Communities* (Microsoft) (C-T-201/04), [2007] ECR II-3601 (Ct First Instance).

[95] Rosborough, "Unscrewing the Future," *supra* note 55.

Whether viewed within the lens of US antitrust law or EC law, competition analyses are focused within a defined "relevant market."[96] Identifying the relevant market generally involves a hypothetical analytical exercise that looks to the effects of a price increase for a given product or service and whether hypothetical consumers can reasonably look elsewhere.[97] In other words, the rationale for competition or antitrust laws in providing remedies is based largely in economic theory and oriented around measuring aggregate demand and pricing. The impacts of firmware TPMs on personal property ownership, however, are not always measurable through such market or economic analyses. In fact, some of these impacts may address use and management of personal property that has no market basis at all.[98] It is not clear that in every case the personal property-related "injury" suffered by a device owner with embedded firmware TPMs is the kind of harm that antitrust or competition law intends to prohibit.[99] Competition and antitrust policy revisions can therefore only partially ameliorate the negative ownership impacts enabled by firmware TPMs.

Recalibrating TPM exceptions under copyright law and curtailing the anticompetitive uses of firmware TPMs are undoubtedly important aims. But in both cases, scrutiny is directed toward the content and market impact of trade restraints and uses of copyright works. Though important, this does not necessarily address the impact of firmware TPMs on the use and management of tangible property.[100] For these reasons, recalibrating anti-circumvention laws and responding to TPM overreach by manufacturers requires more than merely looking to copyright and competition policy. Policymaking in this area should also be normatively and analytically guided by the law of property and its rejection of personal property servitudes.

IV. FIRMWARE TPMS AS PERSONAL PROPERTY SERVITUDES

The common law of real property has long recognized special types of interests in property held by someone other than its owner. The basis for this recognition is the view that agreements that are inextricably connected to the use of land ought to be embedded within the framework of property rights as opposed to mere contractual entitlements. Borrowing from Roman law, early English law treated these types of agreements as remaining with or "running

---

96 Adriaan ten Kate & Gunnar Niels, "The Relevant Market: A Concept Still in Search of Definition" (2008) 5:2 J Competition L & Economics 297 at 302.

97 Øystein Daljord, Lars Sørgard & Øyvind Thomassen, "The SSNIP Test and Market Definition with the Aggregate Diversion Ratio: A Reply to Katz and Shapiro" (2007) 4:2 J Competition L & Economics 263 at 263.

98 Pamela Samuelson, "Freedom to Tinker" (2016) 17:2 Theor Inq L 563 at 569.

99 Thomas V Vakerics, *Antitrust Basics* (New York: Law Journal Seminars-Press, 1985) at §3.03[2].

100 Christina Mulligan, "Personal Property Servitudes on the Internet of Things" (2016) 50:4 Ga L Rev 1121 at 1130.

with" the land. This allowed the agreement in respect of land to benefit and bind third parties and subsequent purchasers.[101] Likely the most familiar example of this type of right in the common law is an easement, where the owner of a dominant tenement has the right to require the owner of the servient tenement to allow some type of use or bear restrictions in the use of the land.[102] This can also include (for example) a right of way over servient lands for accessing a dominant one, or wayleave for utilities to enter onto land to install or maintain infrastructure that passes through it.[103]

Though the law of easements finds its basis in English law, analogous principles are found throughout the US law of real covenants, easements, and equitable servitudes.[104] Similar principles also exist in the civil law tradition.[105] And though legal systems may categorize, name, and calibrate these non-possessory property interests differently,[106] we may consider them to all fall under the general category of "servitudes" for the sake of this analysis.

While the common law has come to recognize numerous land servitudes in furtherance of social planning objectives and the impacts of industrialization,[107] personal property has generally been left out of this development. One practical explanation for this is that, in contrast to land registration systems for real property, there is no reliable means to verify interests in movable personal property.[108] This makes it very difficult to confirm the ownership, scope, and duration of such servitudes. Beyond these practical limitations, however, courts have also resisted the enforcement of personal property servitudes on account of their tendency to produce several undesirable outcomes, including limiting unforeseen future uses of things, often without notice.[109]

---

[101] Robert Megarry, HWR Wade & Charles Harpum, *The Law of Real Property*, 5th ed (London, UK: Sweet and Maxwell, 1984) at 743 — 46.

[102] *Ellenborough Park, Re*, [1956] Ch. 131 (Eng. Ch. Div.), affirmed [1955] 3 All E.R. 667 (C.A.).

[103] Roger J Smith, *Property Law*, 7th ed (London: Pearson, 2011) at 495.

[104] Lawrence Berger, "Integration of the Law of Easements, Real Covenants And Equitable Servitudes" (1986) 43:2 Wash & Lee L Rev 337 at 349 — 51.

[105] For an analysis of the similarities and differences between the English law of easements and servitudes as emanating from Roman law, see K Kahana Kagan, "Servitudes in Comparison with Easements of English Law" (1950) 25 Tul L Rev 336.

[106] For example, under United States property law, non-possessory interests such as easements, real covenants and equitable servitudes are all generally considered "servitudes," while English law generally considers these rights as types of "incorporeal hereditaments." For an analysis of the doctrinal differences and shared history of these systems, see Uriel Reichman, "Toward a Unified Concept of Servitudes" (1982) 55:6 S Cal L Rev 1177.

[107] Ariel Katz, "The First Sale Doctrine and the Economics of Post-Sale Restraints" (2014) 2014:1 BYUL Rev 55 at 57 — 58.

[108] Henry Hansmann and Reiner Kraakman, "Property, Contract, and Verification: The *Numerus Clausus* Problem and the Divisibility of Rights" (2002) 31:2 J Leg Stud S373 at S407.

Corresponding to these undesirable outcomes, Van Houweling has identified three recurring themes to the common law's reluctance to accept personal property servitudes: the notice and information costs that arise when purchasers acquire things without knowing of an encumbrance or a restriction in its use; the undesirable limits on the free use and management of things by future generations; and the impacts or externalities on third parties.[110] While similar concerns also arise in the context of land servitudes, doctrinal limitations and registration systems have generally reduced their impacts.[111]

Each of these rationales for resisting personal property servitudes also speaks to the operation and effects of firmware TPMs. The following portion of the paper surveys the points of convergence between the law's reluctance in allowing personal property servitudes and the operation and effects of firmware TPMs. It then addresses some of the implications of these points of convergence for the development of future TPM policy.

(a) Notice and Information Costs

Notice and information costs relate to the inconvenience and difficulty for a purchaser of property burdened by servitudes to understand exactly which rights in the bundle he or she is acquiring. Most servitudes allow for ownership and conveyance of property subject to specific caveats and limitations on its use or management. Where there is clear and easily decipherable notice given of such restrictions, the information costs are low. Where deciphering and determining the content and extent of such restrictions is more difficult, the information costs are increased. Whether the reason is to avoid future liability or to ensure that certain rights are acquired, the purchaser will only engage in an investigation of this sort to the extent that its benefits outweigh the costs.[112] Nevertheless, a failure to take notice of a restrictive servitude could result in a significant limitation on the use and management of property down the road.

In comparison to land, personal property is transferred and sold fairly frequently. This is owed to the fact that items of personal property are generally low value goods, but also due to their movability.[113] This increases both the importance and costs involved in determining the scope and content of personal property servitudes.[114] Part of the common law's reluctance to adopt personal property servitudes stems from the much higher likelihood that purchasers will be unable to determine the scope and nature of these restrictions easily and

---

[109] Perzanowski & Schultz, *supra* note 5 at 198.

[110] "Exhaustion and the Limits," *supra* note 74.

[111] Katz, *supra* note 107 at 97.

[112] Thomas W Merrill and Henry E Smith, "Optimal Standardization in the Law of Property: The Numerus Clausus Principle" (2000) 110:1 Yale LJ 1 at 26.

[113] Glen O Robinson, "Personal Property Servitudes" (2004) 71:4 U Chicago L Rev 1449 at 1489.

[114] Molly Shaffer Van Houweling, "The New Servitudes" (2008) 96:3 Geo LJ 885 at 931.

efficiently.[115] Just as land registration systems operate through title documents denoting a variety of interests in real property, commentators have argued that restrictions on the use of personal property require some standardization of terms and methods of providing notice.[116]

Manufacturers utilizing firmware TPMs, however, have largely achieved what the common law has been loathe to adopt. Manufacturers incorporating these restrictions do not need to provide notice of their existence nor articulate the types of uses or management that they restrict.[117] In fact, they have a disincentive to provide such notice on account of it deterring consumers or resulting in negative perceptions in the marketplace. Some of the specific harms that are produced by the lack of TPM notice requirements include the lack of expected interoperability, anti-competitive lockouts, risks of unforeseen anti-circumvention liability, unanticipated changes made without consent, or discontinuation of device functionality.[118] Each of these unforeseen restrictions can impose significant limitations on the use and management of devices without the ability for purchasers to identify them in advance. In this way, these firmware TPM restrictions enable *de facto* personal property servitudes without notice, resulting in high information costs.

(b) Costs Imposed on the Future

The common law has also been reluctant to recognize personal property servitudes on account of their permanence, durability, and difficulty to undo down the road. Put simply, they are *sticky*. This tends to place undesirable control over the use and management of property and resources by future generations. Borrowing from the body of real property servitude scholarship, Van Houweling refers to this justification for limiting personal property servitudes as the "problem of the future."[119] A utilitarian basis for this concern is that property use allocations through servitudes may in the future turn out to be undesirable or inefficient.[120]

One factor that exacerbates these problems in the case of personal property is the remoteness between the benefit and burden holders, and particularly during periods of social and technological change. This remoteness exacerbates the difficulty involved in altering the terms of the servitude or renegotiating it. This remoteness is likely to be more extreme in the case of products produced by large

---

[115] Zechariah Chafee Jr., "The Music Goes Round and Round: Equitable Servitudes and Chattels" (1956) 69:7 Harv L Rev 1250 at 1261.

[116] Though not all agree with this position. See Robinson, *supra* note 113 at 1484 — 88.

[117] Pamela Samuelson and Jason Schultz, "Should Copyright Owners Have to Give Notice About Their Use of Technical Protection Measures?" (2007) 6:1 J on Telecommunications & High Technology L 41 at 47.

[118] *Ibid.*

[119] "Exhaustion and Personal Property Servitudes," *supra* note 73 at 50.

[120] Gerald Korngold, "Privately Held Conservation Servitudes: A Policy Analysis in the Context of in Gross Real Covenants and Easements" (1984) 63:3 Tex L Rev 433 at 457.

institutional manufacturers and purchased by end consumers. Overall, this justification for limiting personal property servitudes recognizes that, even more so than land, the allocation and use of personal property requires a high degree of malleability into the future.

Firmware TPMs, however, can impose significant costs on future uses of personal property. As noted in the above examples, they can functionally restrict the use and management of personal property on absolute terms. As opposed to *in vacuo* contractual or legislative restrictions mandating restricted personal property use or management – such as intellectual property rights – firmware TPMs are direct functional limitations on physical use. This makes them extraordinarily durable, permanent, and difficult (if not impossible) to undo in many cases. Being embedded within the function of these devices also makes firmware TPMs effective in binding future owners into perpetuity.

Consistent with the common law's concerns, firmware TPMs impose direct and substantial negative impacts on the future. Where repairs or maintenance of devices with embedded firmware TPMs require authentication to complete, the unlawfulness of circumvention can result in premature abandonment of many products and devices. Often these are devices that could have otherwise been repurposed or repaired.[121] Abandonment of computerized devices due to firmware TPM restraints has also accelerated the production of electronic waste, which is now the fastest-growing solid waste stream globally.[122] And beyond the shortened lifespan of these devices through planned obsolescence, their disassembly, recycling, and disposal results in disproportionate impacts on health and social inequality in the global south.[123]

A further negative impact of firmware TPMs on the future is on learning and innovation. Locking down devices can restrict future experimentation, innovation, and new discoveries. Take for example the Linksys WRT54G wireless internet router. Released in 2002, the WRT54G was a common relic in workplaces and households for years, distinctive for its blue and black plastic design. Its low cost resulted in millions of sales worldwide before Linksys was acquired by Cisco Systems in 2003. The WRT54G routers manufactured and sold by Linksys incorporated chipset firmware that had been developed by a third party. That firmware was built upon a GPL licence, requiring the source

---

[121] See e.g. the Sonos smart speaker "recycling mode," which resulted in many devices being needlessly and prematurely discarded: Chris Welch, "Sonos Is Getting Rid of the Controversial Recycle Mode that Needlessly Bricked Its Older Devices," *The Verge* (5 March 2020), online: < www.theverge.com/2020/3/5/21166777/sonos-ending-recycle-mode-trade-up-program-sustainability > .

[122] Sabab M Abdelbasir et al, "Status of Electronic Waste Recycling Techniques: A Review" (2018) 25:17 Environmental Science & Pollution Intl 16533, online: < pubmed.ncbi.nlm.nih.gov/29737485/ > .

[123] Michelle Heacock et al, "E-Waste and Harm to Vulnerable Populations: A Growing Global Problem" (2016) 124:5 Environmental Health Perspectives 550 at 550.

code to be always freely available to end users. This fact was unbeknownst to Cisco when it acquired Linksys in 2003.[124]

Eventually, hardware engineers at Cisco discovered that the WRT54G's firmware was built upon a GPL licence. After threats of legal action by the Free Software Foundation, Cisco had no option but to release the firmware's source code. This resulted in the firmware (and router hardware itself) being used for endless hardware hacking projects, adding new capabilities that had not been anticipated. In one modification, the router was converted into a controller for a DIY camera-equipped home robot.[125] Before the development of the Raspberry Pi, the WRT54G served as an unexpected learning and experimentation device for hardware engineers around the world. Its status as an innovation and hacking platform also led to the development of OpenWRT, an open-source software project for embedded operating systems on home internet routers, smartphones, and personal computers.

Had the WRT54G's firmware not been built upon a GPL licence and instead safeguarded by TPMs, it is highly unlikely that the router would have led to such productive future use and discovery. In effect, open firmware permits experimentation and unforeseen uses of hardware. This can have numerous social and economic benefits, including the prolonged use and repurposing of tangible property. By restricting access and manipulation of firmware, TPMs undermine socially beneficial uses of hardware and impose costs on the future.

(c) Third Party Externalities

The third justification for the common law's reluctance to extend servitudes to personal property is the impact on third parties. Though the impacts on the future and the notice and information costs may be considered pointed examples of third-party externalities, this additional layer of concern focuses primarily on certainty and standardization. The primary concern here is that the creation of these kinds of personal property rights will cause confusion and uncertainty among potential successors in interest and third parties who hold similar rights.[126]

To illustrate this point, Merrill and Smith use the example of a wristwatch timeshare where the purchaser is entitled to use the watch only on Mondays, while the seller would retain the right to use the wristwatch during every other day of the week.[127] Though the law of contract permits such an agreement, there are important reasons why the law of property does not. Merrill and Smith reason that property law rejects the creation of idiosyncratic property rights like

---

[124] David Cassel, "The Open Source Lesson of the Linksys WRT54G Router" (24 January 2016), online: *The New Stack* <thenewstack.io/the-open-source-lesson-of-the-linksys-wrt54g-router/>.

[125] Caleb Kraft, "WiFi Robot: A Hacked WRT54G Router" (28 August 2008), online: *Hackaday* <hackaday.com/2008/08/28/wifi-robot-a-hacked-wrt54gl-rover/>.

[126] Merrill & Henry, *supra* note 112 at 27.

[127] *Ibid.*

this because of the confusion and increased transaction costs it would impose on others:

> Given the awareness that someone has created a Monday-only right, anyone else buying a watch must now also investigate whether any particular watch does not include Monday rights. Thus, by allowing even one person to create an idiosyncratic property right, the information processing costs of all persons who have existing or potential interests in this type of property go up.[128]

Glen Robinson, on the other hand, dismisses this rationale for prohibiting the creation of idiosyncratic property rights.[129] His view is that numerous variations in products and services already exist within the market, including the number of features, quality, and durability. For Robinson, the costs involved in deciphering idiosyncratic property rights through servitudes should not be regarded any differently from other market variations in terms of the information costs that they create.

Firmware TPMs, however, lack the type of salience assumed by Robinson. They are often not discoverable until the owner of a device attempts to carry out some use, procedure, or modification. It is only *then* that the device owner learns that the manufacturer has restricted a certain use or activity. In this sense, the confusion and uncertainty that they create can come long after the point of purchase. This renders the issue beyond a simple analysis of variation in the market. Although consumers may have reason to suspect that certain devices are more likely to incorporate firmware TPMs than others, determining their precise impacts is hardly as straightforward as analyzing product features and durability.

In many ways, firmware TPMs have caused the very undesirable third-party effects pointed to by Merrill and Smith. Supporting this contention, a growing body of scholarship and commentary points to increasingly destandardized personal property rights in relation to many different computerized devices and their related services.[130] In effect, new consumer norms are being established in relation to the use and management of computerized devices on account of embedded restrictions. Though software licensing and terms of service can trace this trend back quite far, rights destandardization through firmware is a more recent phenomenon, beginning roughly around the time of cellphone unlocking and the exclusive control of mobile carriers over the use of these devices.[131]

---

[128] *Ibid.*

[129] *Supra* note 113 at 1488.

[130] See Perzanowski & Schultz, *supra* note 5 at 35. See also Aaron Perzanowski & Chris Jay Hoofnagle, "What We Buy When We Buy Now" (2017) 165:2 U Pa L Rev 315; and Hoofnagle, Kesari & Perzanowski, *supra* note 64 at 815.

[131] Kyle Wiens, "Forget the Cellphone Fight — We Should Be Allowed to Unlock *Everything* We Own," *Wired* (18 March 2013), online: < www.wired.com/2013/03/you-dont-own-your-cellphones-or-your-cars/ > .

Rights destandardization is also explicitly acknowledged by manufacturers of these products. For example, John Deere provides us with yet another example. In 2015, Deere made submissions before the US Copyright Office in response to a proposed TPM anti-circumvention exemption for the repair of agricultural equipment, contending the following:

> In the absence of an express written license in conjunction with the purchase of the vehicle, the vehicle owner receives an implied license for the life of the vehicle to operate the vehicle, subject to any warranty limitations, disclaimers or other contractual limitations in the sales contract or documentation.[132]

The notion that equipment owners receive merely an "implied licence to operate" has caused understandable uproar and consternation among equipment owners and commentators.[133] But it also produces impacts on third parties by upsetting and destandardizing the norms of ownership. Much like Merrill and Smith's "Monday-only right" of property in a wristwatch, the implied licence to operate computerized equipment increases the information costs and uncertainty. Both purchasers of used computerized equipment and other market participants looking to buy related products may now reasonably question the nature of their property rights.[134] Overall, rights destandardization through firmware TPMs imposes significant cost externalities on third parties.

V. IMPLICATIONS FOR FUTURE TPM POLICY

The foregoing demonstrates the close parallels between the common law's apprehension around enforcing personal property servitudes and the ownership impacts of firmware TPMs. In seeking to curtail the negative environmental and economic impacts of TPMs, many jurisdictions around the world are currently scrutinizing anti-circumvention laws and their indirect social and environmental impacts. Beyond adjusting competition policy or recalibrating the balance of exclusive rights within copyright, policymakers can also draw influence from the law of servitudes and its doctrinal limitations. The inherent difficulty in providing notice, the undue restrictions on future uses, and the impacts on third parties point to the importance of TPM notice, technical standardization, and

---

[132] Darin Bartholomew, "Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201" (2 December 2014) at 6, online (pdf): *US Copyright Office* <copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_-Class21_1201_2014.pdf>.

[133] Kyle Wiens, "We Can't Let John Deere Destroy the Very Idea of Ownership," *Wired* (21 April 2015), online: <www.wired.com/2015/04/dmca-ownership-john-deere/>.

[134] See e.g. BMW's decision to transform the heated seats in certain car models into a subscription access service controlled through onboard firmware. Alistair Charlton, "BMW Wants to Charge You A Subscription For Your Heated Seats," *Forbes* (2 July 2020), online: <www.forbes.com/sites/alistaircharlton/2020/07/02/bmw-wants-to-charge-you-a-subscription-for-your-heated-seats/?sh=20103c863c64>.

temporal limitations. The following outlines how adjusting TPM policy to incorporate these attributes can ameliorate some of these negative externalities.

(a) Notice

One way to ameliorate the problems raised by the lack of notice and associated information costs would be to require manufacturers to disclose the use of firmware TPMs in products and devices. This requirement would operate in tandem with a system of TPM categorization and standardization. In 2007, Pamela Samuelson and Jason Schultz approached the question of TPM notice.[135] Drawing on prior research conducted by the Center for Democracy & Technology,[136] they examined a variety of potential approaches for a TPM notice system in the United States, ranging from self-regulatory systems to rigid prescriptive rules. Their analysis was conducted largely in the context of DRM systems protecting digital media. After surveying several potential approaches to notice, they recommended that the Federal Trade Commission ("FTC") investigate and develop standards for notice of TPMs.[137]

Though the FTC never took up that task,[138] the call for such an inquiry remains as relevant today as it was in 2007. Requiring manufacturers of products with embedded firmware TPMs to provide notice of the restrictions they impose would lower the information costs borne by consumers, especially as an increasing number of products on the market have come to adopt these restrictions. Beyond self-regulation, the requirement to provide notice could be implemented by governments in a few different ways, one of which would be to make legal protection for firmware TPMs through copyright law conditional on device owners having reasonable notice of their existence.[139] This would require amendments to anti-circumvention laws to offer greater specificity over which measures constitute TPMs capable of protection. Alternatively, governments could look to consumer protection laws to prohibit the sale of devices incorporating firmware TPMs where they are not adequately disclosed at the time of sale.[140] As outlined in previous sections, firmware TPMs can often be extraordinarily effective in restricting conduct even in the absence of legal protection. For this reason, empowering consumers with guarantees may be particularly effective in the case of computerized devices that incorporate them.

---

[135] *Supra* note 117.

[136] Center for Democracy and Technology, "Evaluating DRM: Building a Marketplace for the Convergent World" (September 2006), online (pdf): < cdt.org/wp-content/uploads/copyright/20060907drm.pdf > .

[137] *Supra* note 117 at 66.

[138] The FTC did, however, address the negative impacts of TPMs on consumers in their 2021 report to the US Congress. *See supra* note 56 at 23 — 24.

[139] Samuelson & Schultz, *supra* note 117 at 70.

[140] *Ibid*. at 73.

Disclosure of firmware TPMs may also be made more feasible through related consumer information campaigns. Though not focused on TPMs *per se*, there are currently efforts afoot in several jurisdictions around the world to score products according to their repairability. These scores are based upon the availability of replacement parts, tools, and information. France was the first to implement such a system,[141] which has since been voluntarily adopted by technology firms around the world.[142] Due to the global distribution of many computerized devices, it is likely that countries around the world will soon begin to implement similar systems.

Criterion 5.3 of France's repairability index measures the extent to which it is possible to "reset software" in products. One way for governments and regulators to provide better notice of firmware TPMs is to sharpen the specificity of this criterion. Ensuring that the presence of firmware TPMs is clearly identified as part of these scoring systems would reduce the information costs borne by consumers. And though firmware TPMs can act to restrict a broader range of use and management than just repair activities, including explicit notice of their existence in computerized products in this context would be a step in the right direction.

(b) Standardization

Closely related to the need to provide effective notice of firmware TPMs is the means to standardize and categorize their technical design and function. This is because providing notice of firmware TPMs first requires a clear conceptualization of what they *are* at the technical level. Beyond the categorization of harms suffered by consumers through the implementation of firmware TPMs, there is currently a paucity of legal and policy research categorizing the variety of techniques and industry practices involved in incorporating TPMs into physical devices. Ambiguous statutory definitions and the broad applicability of trusted system design has only exacerbated this uncertainty. The effect is that pinpointing exactly what constitutes a firmware TPM (as opposed to latent restrictions or inconvenient design) is quite difficult. Though research along these lines has been conducted in relation to TPMs protecting digital media content,[143] the impacts of TPMs in the hardware and device functionality realm requires better understanding at the technical level.

There are, however, ways in which doctrinal adjustments to consumer protection and anti-circumvention laws can indirectly produce some manner of firmware TPM standardization. One such approach is to impose limitations on

---

[141] "Indice de réparabilité" (France), online: *L'Indice de Réparabilité* < www.indicereparabilite.fr > .

[142] Kevin Purdy, "Apple is Using France's New Repairability Scoring — Here's How It Works" (1 March 2021), online: *iFixit* < www.ifixit.com/News/49158/france-gave-apple-some-repairability-homework-lets-grade-it > .

[143] John S Erickson, "Fair Use, DRM, and Trusted Computing" (2003) 46:4 Communications of the ACM 4 at 34.

the types of activities that firmware TPMs can prohibit. On this point, TPM policy could borrow from tangible property law's "touch and concern" doctrine, which requires that servitudes have some connection to the property that they burden.[144] Looking to Merrill and Smith's Monday-watch analogy, the effect would be to mandate that watches must tell the time for every day of the week. In the context of firmware TPMs, this could mean amending consumer protection laws to restrict the use of firmware TPMs in ways that impair activities unrelated to the exercise of copyright.[145] Overall, in the absence of clear policy guidance specifying the range of techniques that may be incorporated in device design, limiting the scope of the permissible use restrictions enabled by firmware TPMs could provide owners with much greater certainty.

(c) Temporal Limitation

Finally, to mitigate the potential negative impacts on future uses of devices with embedded TPMs, policymakers could confine firmware TPM protection to specified periods according to product categories. For products that are no longer being manufactured or for which successive generations have been released, the law could permit circumvention for the purposes of accessing and modifying device firmware. This approach would also require the development of policy categorizing and specifying firmware TPMs according to their technical makeup. This is no small task, but if achieved the benefits could be significant and numerous. As the Linksys WRT54G router story demonstrates, the ability to manipulate firmware can result in several social, educational, and innovative benefits. It can also extend the lifespan of devices by finding new purposes and applications for hardware, thereby reducing the environmental impacts of premature device obsolescence.

Measuring the temporal limitation on firmware TPM protection could be accomplished by reference to existing regulations stipulating product standards. In the European Union, for example, TPM policy could draw reference to Directive 2009/125/EC (the EcoDesign Directive).[146] This Directive mandates a series of product standards in relation to the environmental performance of various products. In 2019, the EU enacted implementing regulations issued pursuant to the Directive that require manufacturers of certain products to provide access to replacement parts, tools, and repair information after products have existed on the market for prescribed periods.[147] In reforming TPM policy,

---

[144] Van Howling, "Exhaustion and Personal Property Servitudes," *supra* note 73 at 48.

[145] Samuelson & Schultz, *supra* note 117 at 73.

[146] EC, *Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products*, [2009] OJ, L 285/10 (EcoDesign Directive).

[147] EC, *Commission Regulation (EU) 2019/2021 of 1 October 2019 laying down ecodesign requirements* for electronic displays pursuant to Directive 2009/125/EC of the European Parliament and of the Council, amending Commission Regulation (EC) No 1275/2008 and repealing Commission Regulation (EC) No 642/2009, [2019] OJ, L 315/241.

these product categories and mandated timelines could be referenced to set durational limits on legal protection for firmware TPMs.

In sum, the common law's hesitation to enforce servitudes on personal property provides useful insight for the development of future TPM policy. As they produce many of the same negative impacts in terms of increasing information costs, hindering future uses of property, and upsetting established norms and expectations, firmware TPMs should be subject to greater scrutiny by policymakers. The negative externalities on personal property ownership could be at least partly ameliorated by mandating a notice requirement, technical standards, and a temporal limitation on their legal enforceability.

VI. CONCLUSION

Access to device firmware has become increasingly important in today's world of ubiquitous computerized devices. Restricting access through TPMs has numerous detrimental social, environmental, and economic impacts. The crucial nature of firmware for many devices can also mean that restricting access has very real impacts on the exercise of personal property rights and ownership expectations.

The primary contribution of this article is its contention that firmware TPMs produce the precise negative impacts on personal property ownership that the common law of property cautions against. In canvassing several examples of firmware TPM implementations across a number of products and devices, it reveals that firmware TPMs are particularly damaging to personal property ownership on account of their lack of salience, their permanence, their absolute rulemaking function, and their tendency to impact third parties through destandarization and increased information costs. In the absence of a wholesale repeal of anti-circumvention laws, the foregoing contends that some of these negative effects can be ameliorated by requiring notice of firmware TPMs, establishing technical standards, and imposing temporal limits on legal protection.

Policymakers around the world are currently scrutinizing the efficacy and scope of anti-circumvention laws on account of the ability for TPMs to undermine repair activities and interoperability between products and devices. These efforts should not only consider these impacts in the context of market competition and copyright's balance of interests, but also within the context of personal property ownership. In moving this effort forward, policymakers have much wisdom to gain from consulting tangible property law and its reluctance to enforce personal property servitudes. In better appreciating the personal property impacts of firmware TPMs, policy reforms have a better chance of safeguarding user autonomy and empowering consumers to exercise ownership through modification, manipulation, repair, experimentation, and innovation.