++++ DRAFT ++++

INTELLECTUAL PROPERTY AND INFORMATION WEALTH: COPYRIGHT AND RELATED RIGHTS

TO OBSERVE AND PROTECT? HOW DIGITAL RIGHTS MANAGEMENT SYSTEMS THREATEN PRIVACY AND WHAT POLICY MAKERS SHOULD DO ABOUT IT [+]

Ian Kerr[*]

A. INTRODUCTION

In the decade since the cold and wet December day when delegates from 150 countries finalized the universal mould for digital copyright reform[1], billions of keystrokes have been spent, tapping out arguments about whether and to what extent we need new laws to protect copyright's "technological protection measures" [TPMs].[2] The prevailing opinion in

---

[+] The following is the PENULTIMATE DRAFT of a chapter forthcoming in *Intellectual Property and Information Wealth: Copyright and Related Rights* (vol.1)*,* Edited by Peter Yu, Praeger Publishers, 2007.

[*] Dr. Ian Kerr holds the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa, Faculty of Law. He has published writings in academic books and journals on ethical and legal aspects of digital copyright, automated electronic commerce, artificial intelligence, cybercrime, nanotechnology, internet regulation, ISP and intermediary liability, online defamation, pre-natal injuries and unwanted pregnancies. His current program of research includes two large projects: (i) On the Identity Trail, focusing on the impact of information and authentication technologies on our identity and our right to be anonymous; and (ii) An Examination of Digital Copyright, focusing on various aspects of the current effort to reform Canadian copyright legislation, including the implications of such reform on fundamental Canadian values including privacy and freedom of expression.

This chapter is an adaptation of *If Left to Their Own Devices: How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy*, *in* THE PUBLIC INTEREST: CANADIAN COPYRIGHT IN A DIGITAL AGE 167 (Michael Geist, ed., 2005), *available at* http://209.171.61.222/PublicInterest/Two_03_Kerr.pdf. Researchers interested in a more extensive list of citations might wish to consult the original text. The author wishes to extend his gratitude to the Social Sciences and Humanities Research Council, the Canada Research Chairs program, Bell Canada and the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of this research. Special thanks also to Jeremy Hessing-Lewis, Dr. Hilary Young and Katie Black for their role in the adaptation of this chapter, and for their extraordinary efforts, their general brilliance, and for the high quality of research assistance that they so regularly and reliably provide.

[1] JESSICA LITMAN, *The Bargaining Table in* DIGITAL COPYRIGHT 122 (2001); Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369 (1997).

[2] See e.g., The Digital Millennium Copyright Act of 1998*,* Pub. L. No. 105-30, 112 Stat. 2860, *summary available at* http://www.copyright.gov/legislation/dmca.pdf [hereinafter *DMCA*]*;* Directive of the European Parliament and the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society (2001), L 167/10, *available at* http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/directive_copyright_en.pdf (EU) [hereinafter *EUCD*]; Copyright Amendment (Digital Agenda) Act, 2000, c. 110 (Austl.) [hereinafter *Copyright Amendment*]; Japanese Copyright Law No. 48, promulgated on 7 May

many countries with strong copyright industries is that we do. Their most powerful voices[3] tell us that such laws are necessary to protect the copyright industries from individuals who use devices to circumvent "copying-protecting" technologies. They say that existing laws do not adequately prevent the massive illegal dissemination of digital works taking place everyday off and online.[4] Consequently, jurisdictions including the United States, Australia, Hong Kong, and Japan have ratified the *WIPO Copyright Treaty*[5] and the *WIPO Performances and Phonograms Treaty*[6] by enacting new laws to protect TPMs.[7]

Living for nearly a decade in States-of-indecision, there remain a number of other signatories to the *WIPO treaties* that have not yet ratified them. Astonishingly, despite ten years of legislative inaction on the anti-circumvention front, many of these countries still intend to board the *Mothership*. For example, contemporaneous with the writing of this chapter, Canada has announced[8] that it will attempt, for a second time, to

---

1970 as amended by Law No. 77, of 15 June 1999 and the Japanese Anti-Unfair Competition Law (Jp.) [hereinafter JCL & JAUCL]; Copyright Act 1994 No. 143, as amended by Law No. 33, 2005 (N.Z.)[hereinafter *NZCA*]; and Copyright Ordinance (Cap. 528), entered into force June 1997 (H.K.) [hereinafter *HKCO*].

[3] As the Recording Industry Association of America (RIAA) points out on its website, "RIAA believes that the establishment of technological protection and management for all musical content, regardless of the media on which it resides or the method by which it is transmitted, is a central component for the expansion of both the music opportunities for the consumer and the business opportunities for the technology industry," http://www.riaa.com/issues/audio/newmedia.asp; the Canadian Recording Industry Association (CRIA) states in its submission to the Canadian Copyright Reform Process "Law and technology must be used together to maintain adequate incentives for creativity. Failure to offer adequate legal protection to technological protection measures (TPMs) will inevitably inhibit the development of electronic commerce in copyrighted products" (Sept. 14, 2001), http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp00249e.html; the Recording Industry Association of Europe's Mission statement includes "…[t]o ensure correct implementation of the European Copyright Directive, according to which fair compensation (e.g. levies) must be linked to the availability of technical protection measures," http://www.riae.org/mission.html (last visited May 7, 2006); and the Australian Recording Industry Association, in its submission to the Australian House of Representatives Standing Committee for Legal and Constitutional Affairs, supports "redrafting to anti-circumvention and effective technological protection provisions to render them commercially effective and in compliance with the WPPT." To this end it generally suggests broader definitions for TPMs that are to be protected by anti-circumvention laws, http://www.aph.gov.au/HOUSE/committee/laca/digitalagenda/Sub62.pdf.

[4] I and others remain unconvinced and have argued elsewhere against this position: Ian R. Kerr et al., *Technological Protection Measures* commissioned by the Department of Canadian Heritage (Canada) (pts. 1 & 2), *Trends in Technical Protection Measures and Circumvention Technologies* (2003), http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/tdm_e.cfm, *The Legal Protection of TPMs* (2003), http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/tdm_e.cfm; Ian R. Kerr et al., *Technical Protection Measures: Tilting at Copyright's Windmill* 34:7 OTTAWA L. REV. 82 (2003).

[5] *WIPO Copyright Treaty*, 20 December 1996, 36 I.L.M. 65 (entered into force 2 March 2002) *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

[6] *WIPO Performances and Phonograms Treaty,* 20 December 1996, 36 I.L.M. 76 (entered into force 20 May 2002), *available at* http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html.

[7] DMCA, Copyright Amendment, HKCO, JCL, *supra* note 2.

[8] *Conservative government to introduce copyright bill: Bev Oda*, THE HILL TIMES., April 10, 2006, http://www.thehilltimes.ca/html/index.php?display=story&full_path=/2006/april/10/politics/&c=1.

implement the *WIPO treaties*. Canada had made an earlier attempt to do so in a proposal known as *Bill C-60*.[9] Like legislation already enacted in other jurisdictions, a core provision of this now-defunct-but-soon-to-be-resurrected *Bill* would have afforded to copyright owners a number of remedies against anyone who, without consent, "circumvents, removes, or in any way renders ineffective a technological measure protecting any material form of the work..."[10] A second provision in the *Bill* would have generated similar consequences for anyone who "knowingly removes or alters any rights management information in electronic form…."[11] These proposed provisions are not, properly speaking, copyright provisions. They are *paracopyright* laws.

The purpose of *paracopyright* laws is to add a new legal layer that goes *beyond* existing copyright and contract laws. This layer seeks to deter people from tinkering with anti-copying technologies that automatically enforce copyright by restricting or monitoring the use of digital material. Central aims of all WIPO-inspired anti-circumvention legislation are "to provide rights holders with greater confidence to exploit the Internet as a medium for the dissemination of their material and provide consumers with a greater choice of legitimate material."[12] These are certainly laudable goals. However, it remains uncertain whether the newer, kinder, gentler anti-circumvention provisions[13], of the sort once proposed (though still not enacted) in Canada, would in fact do less harm to copyright's delicate balance[14] than laws proposed or enacted in the United States,[15] Europe,[16] and elsewhere.[17]

---

[9] Bill C-60, An Act to amend the Copyright Act, 1st Sess., 38th Parl., (2005) Preamble, *available at* http://www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF [hereinafter *C-60*]. However, this Bill died on the order paper with the fall of the Liberal government during the 38th Session of Parliament.

[10] Although Bill C-60 purported to operate against circumventions "for the purpose of an act that is an *infringement of the copyright* in it or the moral rights in respect of it …" (*id* at § 34.02).

[11] *Id*. at § 34.01.

[12] Statement, Canadian Heritage, Government Statement on Proposals for Copyright Reform (March 24, 2005), http://pch.gc.ca/progs/ac-ca/progs/pda-cpb/reform/statement_e.cfm.

[13] Unlike the United States' DMCA, which applies broadly to circumvention regardless of purpose, Canada's proposed law would have directly tied the act of circumvention to an infringing purpose.

[14] Press Release, Canadian Internet Policy and Public Interest Clinic (CIPPIC), CIPPIC Questions Unbalanced Copyright Bill (June 20, 2005), http://www.cippic.ca/en/news/documents/Media_Release_-_Copyright_Bill_-_20_June_05_Final.pdf.

[15] DMCA *supra* note 2 at § 1201(a)(1)(A).

[16] EUCD *supra* note 2 at 17 art. 6, §1-2, art. 7, §1.

[17] Copyright Act 1968 (Cth.), Act No. 63 of 1968 as amended, 2005, s. 116A *available at* http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/DBD28FED04130B18CA256FE7008378BB (Austl.); Japanese Copyright Law No. 48 promulgated on May 7, 1970, as amended by Law No. 92, of June 9, 2004, art. 30, § 1 *available at* http://www.cric.or.jp/cric_e/clj/clj.html (Jap.); Copyright Ordinance (Cap 528, 1997, H.K.), § 273-4

What is *less uncertain* is the effect that any of the proposed or existing anti-circumvention laws will have on privacy. When it comes to protecting *intellectual privacy*[18] – a core value underlying the doctrine of intellectual property – most of the anti-circumvention laws, proposed or enacted, whisper with the sounds of silence.[19] Although ample statutory language is offered to ensure that anti-circumvention, anti-tampering and anti-device laws will protect TPMs from people, such laws usually offer zero protection to people *from* TPMs.

In this chapter, I contend that statutory silence about the permissible scope of use for TPMs *risks too much* from a privacy perspective. In particular, I present the view that any law which protects surveillance technologies used to enforce copyright must also protect people's privacy. Such laws must contain express provisions and penalties that protect citizens from organizations using TPMs and Digital Rights Management systems [DRMs] to engage in excessive monitoring or the piracy of personal information. From a privacy perspective, the best solution is to not grant legal protection for TPMs at all. However, if the copyright industries and national governments insist that there is a legitimate need for new laws to prevent the circumvention of TPMs, then similar provisions are needed to protect citizens from organizations that use both TPMs and the law of contract as a kind of privacy circumvention device. Copyright owners should not be encouraged or allowed to use TPMs and contracts to circumvent fair information principles[20] or hack past data protection legislation. In this brief chapter, I offer a general description of the kind of counter-measures that are needed to ensure that anti-circumvention provisions adequately balance different stakeholder interests.

(H.K.); New Zealand: Copyright Act 1994, 1994/143, as amended by Law No.33 2005, § 226, *available at* http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes (N.Z.).

[18] i.e., the right to experience intellectual works in private, free from surveillance. See e.g., Julie Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace*, 28 CONN. L. REV. 981, 1003 (1996); Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 584 (2003); Graham Greenleaf, *IP, Phone Home: Privacy as Part of Copyright's Digital Commons in Hong Kong and Australian Law in* HOCHELAGA LECTURES 2002: THE INNOVATION COMMONS 17 (Lawrence Lessig, ed., 2003);

[19] The European Directive provides limited privacy protection: "Any such rights-management information systems referred to above may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data"(EUCD *supra* note 2 at 15, Preamble, §57).

[20] ORGANISATION OF ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html; CANADIAN STANDARDS ASSOCIATION, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (1996), *available at* http://www.csa.ca/standards/privacy/code/Default.asp?language=English; Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Schedule 1, *available at* http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp [hereinafter *PIPEDA*].

B. TPM/DRM

It is useful to distinguish between TPMs and DRMs. In its simplest form, a TPM is a technological measure intended to promote the authorized use of digital works. Of course, TPMs can also operate as a kind of "virtual fence" around digitized content and can lock it up regardless of whether it enjoys copyright protection. These protections are accomplished by controlling access to copyright works, or by controlling various uses of copyright works including: (i) copying, (ii) distribution, (iii) performance, and iv) display.

While TPMs are designed to *prevent* copying, DRMs are designed to *manage* copying by using various automation and surveillance technologies to identify content and technologically enforce certain licensing conditions. More and more, DRMs will be used to manage all rights reserved by content owners/providers usually on a take-it-or-leave-it basis.

Typically, a DRM consists of two components.

The *first component* is a set of technologies that might include: encryption, authentication, access control, digital watermarking, tamper-resistant hardware and software, and risk management architectures. Such technologies are used to *enforce* corporate copyright policies and pricing schemes through a registration process that requires purchasers to hand over certain bits of personal information. Usually, the ongoing exchange of personal information between users' devices and content owners'/providers' servers takes place in an *invisible handshake* occurring in the software layer. This allows for the transmission of personal usage information back to the content owner/provider, something Greenleaf once cleverly described as "*IP phone home.*"[21]

Other technologies are used to *express* copyright permissions in "rights expression languages" and other forms of metadata that make a DRM policy machine-readable. Rights expression languages are the bridge to the *second component* of DRM, which consists of a set of legal permissions. In the current context, these permissions are typically expressed as a licensing arrangement which, by way of contract, establish the terms of use for the underlying work.

The technological components of most full-blown DRMs are linked to a database which enables the automated collection and exchange of various kinds of information among rights owners and distributors about the

[21] Lee A. Bygrave, *Digital Rights Management and Privacy — Legal Aspects, in* THE EUROPEAN UNION IN DIGITAL RIGHTS MANAGEMENT— TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 418, 421 (Eberhard Beckar et al., eds. 2003).

particular people who use their products. This includes users' identities, their habits, and their particular uses of the digital material subject to copyright. The information collected can be employed in a number of ways. For example, it can be employed to promote the authorized use of an e-book by restricting access only to those who have paid to use the work, or by restricting one's ability to subsequently distribute it to others who have not.

The surveillance features associated with the database are crucial to the technological enforcement of the licensing component. It is through the collection and storage of usage information that DRMs are able to "authorize use" in accordance with the terms of the licensing agreement and thereby "manage" copyrights.

C. DIGITAL ROUTINE MONITORING?

While much of the above sounds extremely promising for copyright holders and consumers who want alternatives to traditional music album formats, etc., there is a dark side to DRM's monitoring and metering capabilities. DRM has the ability to monitor an individual's private activities while browsing, sampling, or shopping. It can also be used to collect information or monitor behaviour after a contract is entered into, with the aim of continuously scrutinizing a user's habits and activities, regardless of whether the user has complied with the contract.

It should therefore be evident that a full-blown DRM is much more than just a "virtual lock". Surprisingly, despite the fact that the capacity to monitor and meter customer habits is an essential feature of DRM, there is a dearth of sustained focus on the privacy aspects of DRM.[22]

The purpose of anti-circumvention provisions is to facilitate the implementation of DRM as a primary means of enforcing digital copyright. Consequently, it should be clear that privacy protection is an increasingly significant consideration of anti-circumvention provisions. After all, DRM and other technologies adopted by the private sector displace the adage that one's home is one's castle. The moats are long gone, and it is no longer sufficient to draw the blinds. DRM enables surveillance within the seclusion of one's home, providing "the ability to collect fine-grained information about uses of DRM-protected content and

[22] Though the existing research is excellent: See e.g. Greenleaf, *supra* note 18; Julie Cohen, *DRM and Privacy,* 18 BERKELEY TECH. L.J. 58 (2003); Bygrave, *id.*; Lee A. Bygrave, *Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place*, 9 PRIVACY LAW & POLICY REPORTER 135 (2002) [hereinafter Bygrave, *Privacy-Enhancing*]; Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems* 52 STAN. L. REV. 1251, 1255 (2000), *available at* http://cyber.law.harvard.edu/ilaw/Contract/Weinberg_Full.html. It is not difficult to imagine that the recent Sony "rootkit incident" (discussed below in Section D) will inspire increasing attention to this important set of issues.

the ability to reach into [citizens'] homes and restrict what they can do with copies of works for which they have paid."[23]

With an increased reliance on automation and wireless technologies, these monitoring systems are increasingly becoming a constant companion. The key difference is that *these* companions are seeking to monitor not what is going on *in one's home*, but rather, what is going on *in one's head*. This is a dangerous practice to allow, let alone protect. This is especially hazardous considering that many of the corporations who are building these mechanisms of social control into the content delivery system are also attempting to corner the production market, embedding corporate imperatives into the content itself. When this happens, public spaces for debate and thoughtful exchange disappear because the roadway *and* the scenery are artificially controlled.

D. SONY'S ROOTKIT PHONES HOME

The reality of DRM surveillance recently came to light in Canada and the U.S. with the exposé of the Sony-BMG rootkit. [24]

The story began on October 31, 2005, when a computer security specialist was testing diagnostics software that he had co-developed, known as a "rootkit detector."[25] Given his vigilant installation of software and cautious web-use, he was surprised to learn that the diagnostic tool revealed a rootkit on his system. His further investigation led him to a CD DRM application named XCP that had been installed via a Sony-BMG music CD: Van Zant's *Get Right with the Man*. Dismayed to find that Sony's music had surreptitiously installed the rootkit, he blogged about his experience with the copy protection software and the potential security threats that it posed.[26]

The "rootkit scandal" spread quickly across the web and into mainstream media. A series of clumsy moves by Sony-BMG, including a disastrous patch[27] and a public exchange with the Electronic Frontier Foundation,[28]

---

[23] Julie Cohen, *Overcoming Property: Does Copyright Trump Privacy?* 373 U.Ill. J.L. Tech & Pol'y 101 (2002), *available at* http://www.law.georgetown.edu/faculty/jec/overcomingproperty.pdf.

[24] Hull et al. v. Sony BMG Music Entm't., No. BC343385 (Cal. Super. Ct. filed Nov. 21, 2005) (class action complaint) *available at* http://www.eff.org/IP/DRM/Sony-BMG/sony_complaint.pdf. A rootkit is a software program used to cloak files from the user and is designed to be undetectable by consumer security and diagnostic software: Mark Russinovich, *Unearthing Root Kits*, WINDOWS IT PRO, June 2005.

[25] Mark Russinovich, *Unearthing Root Kits*, WINDOWS IT PRO, June 2005.

[26] Mark Russinovich, *Sony, Rootkits, and Digital Rights Management Gone Too Far*, http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html (Oct. 31, 2005).

[27] Mark Russinovich, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html (Nov. 4, 2005).

only made matters worse. The affair culminated with a complete recall of the affected CDs amid class action lawsuits,[29] Sony boycotts,[30] a consumer fallout, and growing artist discontent. It took months before the full threat of Sony-BMG's DRM software emerged. A study by Felten and Halderman concluded that "[t]he systems are surprisingly complex and suffer from a diverse array of flaws that weaken their content protection and expose users to serious security and privacy risks."[31]

To prevent copying, CD-based DRMs such as those used by Sony-BMG often employ both *passive* and *active* measures. *Passive* measures attempt to create "confusion" in order to limit one's ability to access the music. *Active* measures involve the installation of additional software to restrict use of the content. The design of the *active* measures can take the form of spyware.[32] For example,

Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.[33]

In addition to an ability to transmit user information without a user's knowledge and consent, spyware often lacks adequate uninstall utilities making it difficult to disable or remove.[34]

It turns out that Sony-BMG used spyware-like DRMs from two different companies to protect its music CDs. Relying on the Windows autorun feature to initiate installation of the DRMs' software once the CD is inserted into the drive, both presented significant privacy concerns. The

---

[28] Open letter from the Electronic Frontier Foundation, to Andrew Lack, CEO of Sony-BMG (Nov. 14, 2005) *available at* http://www.eff.org/IP/DRM/Sony-BMG/?f=open-letter-2005-11-14.html.

[29] Mark Lyon, *Sony-BMG XCP Rootkit Lawsuits*: http://www.sonysuit.com/ (last modified April 7, 2006).

[30] Dan Goodin, *Boycott Sony*, WIRED NEWS, Nov. 14, 2005, http://www.wired.com/news/digiwood/0,1412,69559,00.html?tw=rss.TOP

[31] E. Felten & J.A. Halderman, *Lessons from the Sony CD DRM Episode* (Feb. 14, 2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf.

[32] *Id.* at 2.

[33] Anti-Spyware Coalition, Working Report, " Definitions and Supporting Documents" (October 27, 2005), *available at* http://www.antispywarecoalition.org/documents/definitions.htm.

[34] Felten & Halderman, *supra* note 31, at 2.

first, XCP, was distributed on an estimated 4.7 million CDs.[35] The second, MediaMax, was included on over 20 million CDs.[36]

Both XCP and MediaMax can "phone home" to servers operated by Sony-BMG. The stated purpose of such communications is to gather album artwork and lyrics in order to enhance the consumer's music experience. While the content of the connection seems to be limited to updates of album art and lyrics, these online transactions enable the server to log the IP address of the consumer, the date and time of access, and the ID of the copy-protected CD being played.[37] It is impossible to know whether Sony-BMG retains this information or whether it is even used. There was no mention of this data collection in the Sony-BMG end user license agreement.

Sony-BMG did not include an uninstaller with the XCP software. Consequently, the rootkit made it practically impossible for the average user to remove it. Sony-BMG eventually amended its DRM Frequently Asked Questions website to include a link to a form requesting uninstall information. This form required the consumer to provide country of purchase, artist name, artist title, store name, and the consumer's email address. This form also linked to a Sony-BMG privacy policy declaring that e-mail addresses may be shared with affiliates and used for marketing purposes.[38] Sony would then contact the consumer by e-mail with another form and offered a link to a de-cloaking patch whereby the XCP software could eventually be uninstalled. The process only completed with a final email and link to another URL. The patch unleashed additional security issues.[39] An attacker could use the uninstaller's ActiveX control combined with a webpage under their control to execute arbitrary code on the user's machine.[40]

After surveying the copy restrictions related to the rootkit scandal, Halderman and Felten noted that "the design of DRM systems is only weakly connected to the contours of copyright law."[41] At the same time, both XCP and MediaMax were able to dictate one-sided terms of use while concealing any possible collection of consumer information behind

---

[35] Hull et al. v. Sony BMG Music Entm't, *supra* note 24 at ¶ 16.

[36] Hull et al. v. Sony BMG Music Entm't *supra* note 24 at ¶ 18.

[37] Russinovich, *supra* note 26.

[38] Sony BMG Privacy Policy, http://www.sonybmg.com/privacypolicy.html (last visited May 8, 2006).

[39] Felten & Halderman, *supra* note 31, at 21.

[40] Felten & Halderman, *supra* note 31, at 21.

[41] Felten & Halderman *supra* note 31, at 25.

the veil of a DRM that is itself protected under U.S. anti-circumvention laws.

E. PRIVACY HANGS IN THE BALANCE

Given DRM's surveillance capability, it is extremely difficult to imagine why so many governments have failed to specifically and adequately address DRM's privacy implications within the scope of protection afforded to it. This section investigates three crucial policy considerations in achieving an appropriate balance between DRM and privacy: (i) the Anonymity Principle; (ii) Individual Access; and (iii) DRM Licenses. These considerations form the basis of three policy recommendations offered in the final section of the chapter.

1) The Anonymity Principle

The ability to disconnect one's identity from one's actions is of tremendous instrumental and social value. It can foster intellectual development by allowing people to assume roles, thereby testing the plasticity of their identities and the social norms to which they ascribe. In addition, anonymity facilitates the flow of information on public issues and lends a voice to speakers who might otherwise be silenced by fear of retribution.

Anonymity also plays an important role in privacy. It can enhance privacy by: (i) making it more difficult for others to control the collection, use, and disclosure of one's personal information; by protecting people from unwanted intrusions; and (ii) by focusing attention on "the content of a message or behavior rather than the nominal characteristics of the messenger."[42]

Nevertheless, the social utility of anonymity has limits. As Lawrence Lessig once noted, "[p]erfect anonymity makes perfect crime possible."[43] On the Internet, the prospect of true anonymity is largely illusory as the Internet presents an imperfect blend of anonymity and identifiability.[44] This blend is perhaps justified but, as the previous section illustrated, it could substantially change with DRM thrown into the mix.

---

[42] See generally, Gary T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity* 15(2) Info. Soc'y 99; *A. Michael Froomkin, Anonymity in the Balance in*, DIGITAL ANONYMITY AND THE LAW 5 (Chris Nicoll et al. eds., 2003).

[43] Lawrence Lessig, *The Path of Cyberlaw,* 104 YALE L.J. 1743 (1995). See also A. Michael Froomkin, *Anonymity and Its Enmities,* (June 1995) J. ONLINE L. ART. art. 4 ¶ 6, *available at* http://www.wm.edu/law/publications/jol/95_96/froomkin.html.

[44] Weinberg, *supra* note 21, at 1259.

Recall that various features of DRM can reduce or eliminate an individual's ability to consume intellectual goods anonymously. In analogous environments, cash can be used to buy books, CDs, movies, and the like. Paperbacks cannot report back to publishers about who is reading what.[45] By imposing a network of automated transactions between distributors, their products, users, and use, DRM threatens intellectual achievement by reducing the privacy in intellectual pursuits.

It is crucial to mention that DRM need not impose such threats. To say that DRM is inherently privacy-invasive is to confuse how something is with how it must necessarily be.[46] If, as Weinberg suggests, the purpose of DRM is to ensure that "a packet stream requesting access comes from a person who has paid or is otherwise entitled to access,"[47] then DRM *does not* require pervasive monitoring or the collection of personal information about identifiable individuals. The only design feature that the content provider really needs is a means of verifying that the person seeking access or use has the right credentials; that is, that the person has sufficient money or credit, and that they are old enough to view the content.

Not only is it technologically possible to implement DRM while maintaining the anonymity principle, but it is also required by many states' privacy laws. The basic concept was perhaps first articulated in the "Collection Limitation Principle" set out in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. This provision as part of a larger set of Fair Information Practice Principles [FIPPs], constructed in an international effort to harmonize national privacy legislation, recognizes that there should be limits to the collection of personal data. A number of countries which subsequently enacted privacy legislation have built upon this basic principle. In Canada, for example, the anonymity principle is rooted in its broader adjunct, referred to in Canada's federal private sector privacy legislation as the "appropriate purposes" principle. According to this principle, "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[48]

Since many of the current identification and surveillance features of DRM are generally unnecessary, there is good reason to think that the "appropriate purposes" principle is applicable. Its application would help protect the anonymity of those who obtain content through the distribution

---

[45] Greenleaf, *supra* note 18.

[46] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 2 –29 (1999).

[47] Weinberg, *supra* note 22, at 1279.

[48] PIPEDA, *supra* note 20, at § 5(3).

channels of DRM.[49] The cryptographic work of David Chaum[50] is a good example of an "appropriate purpose" technology that enforces contractual restrictions and holds users accountable without needing to collect personal information, monitor, or meter behavior.

The anonymity principle is firmly in place in many jurisdictions with strong privacy and data protection laws. For example, Australia's national privacy law states:

Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization.[51]

Germany has similar provisions in its Federal Data Protection Act and its Teleservices Data Protection Act:

s. 3(a) [Federal Data Protection Act] The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected.

s. (6) [Teleservices Data Protection Act] The provider shall make it possible for the user to utilize and pay for teleservices anonymously or under a pseudonym if this is technically possible and can be accomplished at reasonable effort. The user shall be informed of this possibility.[52]

Finally, anonymity is protected by the U.S. Constitution's First Amendment which relates to freedom of expression. American courts have frequently interpreted the right to freedom of expression to include the right to anonymous speech.[53]

---

[49] Bygrave cites the EC Directive on data protection (Directive 95/46/EC of the European Parliament) arts. 6(1)(e) and (c), together with arts. 7-8: Bygrave, *supra* note 21, at 429.

[50] David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete* 28 COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY 1030, 1030 (1985); David Chaum, *Achieving Electronic Privacy* (August 1992) SCIENTIFIC AMERICAN 96, *available at* http://ganges.cs.tcd.ie/mepeirce/Project/Chaum?sciam.html. Why Chaum's techniques (and the innovations he has subsequently inspired) have failed in the marketplace, despite achieving Weinberg's specification of the original aim of DRM, is an interesting question worthy of pursuit.

[51] Privacy Act 1988 (Cth), as amended by the Privacy Amendment (Private Sector) Act 2000 (Cth), Schedule 3, Principle 8, *available at* http://scaleplus.law.gov.au/html/comact/10/6269/top.htm (Austl.).

[52] Federal Data Protection Act of 1990, as amended May 24, 2001 (Bundesdatenschutzgesetz) (Germany), *available at* http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm#sec3 ; Information and Communication Services Act of 1997 (Informations- undKommunikationsdienste-Gesetz – IuKDG) (Germany), art. 2, Teleservices Data Protection Act (Teledienstedatenschutzgesetz TDDSG) as amended in 2001, *available at* http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf.

[53] "[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." McIntyre v. Ohio Elections Commisison, 514 U.S. 334 (1995).

Infusing the anonymity principle into the design of DRM should be promoted as a matter of public policy; however, it is crucial to recognize that such infusion is by no means sufficient privacy protection. Given the market failures of privacy-enhancing technologies to date,[54] law must also be used to ensure the appropriate balance between the interests of copyright industries and citizens. Just as the copyright industries claim that law is needed to protect DRM, law is also needed to protect citizens against DRMs designed to unjustifiably circumvent the anonymity principle.

2) Individual Access

In the copyright context, one of the chief concerns about DRM is its ability to lock up a work. The ability to control access has the effect of skewing copyright's delicate balance because the exercise of many of the balancing provisions in many countries' copyright laws are premised on the ability to gain access to the work in the first place. Consequently, the only way to restore balance is to create a positive obligation on the copyright holder to ensure that alternative means of obtaining access to a work remain available. Under this sort of approach, copyright owners would have a positive obligation to provide access to a work when persons or institutions fall within an exception or limitation set out in the relevant copyright legislation. This might entail a positive obligation to allow access-to-works in the public domain, or to provide unfettered access-to-works to institutions such as universities who are currently exempted from a number of the provisions in copyright law.

Returning to DRM in the privacy context, corollary access and control issues stem from the FIPPs set out in the *OECD Guidelines* and codified in a number of national privacy schemes.[55] Informational privacy is

---

[54] See e.g., Tim Clark, *Digicash files Chapter 11,* CNETNEWS.COM, Nov. 4, 1998, http://news.com.com/2100-1001-217527.html?legacy=cnet; Robert Lemos, *Net users lose a secret-alias tool*, CNET NEWS.COM, Oct. 4, 2001, http://news.com.com/2100-1023-273956.html; Tom Mainelli, *SafeWeb Dumps Free Online Privacy Service*, PC WORLD.COM, Nov. 21, 2001, http://www.pcworld.com/news/article/0,aid,72466,00.asp. See generally, Bygrave, Privacy-Enhancing, *supra* note 22; Ian Goldberg, *Privacy-enhancing technologies for the Internet, II: Five years later*, http://www.freehaven.net/anonbib/papers/petfive.pdf.

[55] The EU has implemented its OECD obligations regarding FIPPs in its Data Protection Directive (No L. 28 OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES 31 (Nov. 23, 1995)) and the following states have either fully or partially implemented their obligations under this Directive: Belgium, the Czech Republic, Denmark, Germany, Estonia, Greece, Spain, France, Ireland, Italy, Luxembourg, Hungary, Malta, The Netherlands, Austria, Poland, Cyprus, Latvia, Lithuania, Portugal, Slovenia, Slovakia, Finland, Sweden and the United Kingdom. For links to each of these countries' privacy legislation, see: http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm. In Canada, FIPPs are incorporated into PIPEDA (*supra* note 20). In contrast, "the U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level. Instead, the Principles have formed the basis of many individual laws at the both federal and state levels -- called the 'sectoral approach.' Examples are the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act." See Privacy Rights

premised on the idea that individuals ought to be able to determine for themselves when, how, and to what extent information about them is communicated.[56] As is the case with access to digital content, an individual's ability to control personal information in some instances depends on that individual's ability to gain access to it in the first place. FIPPs-based privacy legislation in a number of countries contemplates this possibility. Such legislation posits a general duty upon organizations to ensure that the individual has knowledge of, and consents to, the collection of personal information. Moreover, such organization must subsequently provide the individual with access to personal information which has been collected about him or her.

Like digital content, personal information is sometimes locked-up in a technological measure or a DRM database. The individual can have no way of knowing what personal information has been collected, nor any means to access it without hacking past the technology. Obviously, this is problematic from the perspective of informational privacy. An anti-circumvention law that is silent with respect to exceptions permitting circumvention in order to obtain control over or access to one's personal information would therefore facilitate the circumvention privacy laws through DRM.

Without adequate legal measures that re-enable one's ability to access or control personal information that is under digital lock and key, informational privacy (i.e., one's ability to determine when, how, and to what extent information about oneself is communicated) will be seriously undermined.

3) DRM Licenses

Like other contractual devices, an Intellectual Property (IP) license allows copyright holders to set the terms of use for their products. In the DRM context, intelligent agent technologies facilitate the automatic "negotiation" of contractual licenses between content providers and users.

In an automated environment, most informational transactions take place invisibly through software exchanges between machines, about which few humans are aware and fewer still have the technical expertise to alter. Bits and bytes of data, not to mention various forms of personal information, are collected and inconspicuously interchanged without human intervention and often without knowledge or consent. Automation therefore exacerbates an already problematic inequality in the bargaining power between the licensors and licensees resulting from standard form

---

Clearinghouse, *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy* (February 2004), http://www.privacyrights.org/ar/fairinfo.htm.

[56] See e.g., ALAN F. WESTIN, PRIVACY AND FREEDOM 322 1970.

agreements and mass market licenses. The combination of TPMs and contracts in this manner could therefore lead to unfair transactions.

With increasing frequency, the terms of these licenses are used to override existing copyright limitations. And, as Guibault aptly articulates:

The copyright bargain reached between granting authors protection for their works and encouraging the free flow of information would be put in serious jeopardy if, irrespective of the copyright rules, rights owners were able to impose their terms and conditions of use through standard form contracts with complete impunity.[57]

The above analysis similarly applies in the privacy context. An unbridled use of TPM with anti-circumvention legislation and contractual practices would permit content owners to extend their surveillance and personal information collection practices far beyond the bounds of what might otherwise be permitted by privacy law, to the detriment of everyone who uses DRM. Like copyright, privacy law's compromise between the needs of organizations and the right of privacy of individuals will also be put in serious jeopardy if, irrespective of privacy rules, content owners are able to impose their terms and conditions through standard form contracts with complete impunity.

There is value in contemplating basic common law principles and their applicability for setting appropriate limits on DRM's ability to exploit the law of contract. Contract law commences with the idea of freedom to contract and then systematically proceeds to undermine the idea through various doctrines. Waddams states that, "[p]erhaps the most open opposition to the principle of the free enforceability of contractual agreements has been the striking down of agreements on the ground that they are contrary to public policy."[58] While the courts generally avoid interfering with individual bargains, they will sometimes render void a contract that contravenes a statute.

To date, there has not yet been a formal finding within the international Data Commissioners' Community of a DRM that contravenes FIPPs-based legislation. Given that there is no single technological standard for DRM and that different providers offer different terms of use, the more appropriate question is whether DRM surveillance *could* contravene the legislation. Although the answer to this question involves some speculation, there are good grounds for answering in the affirmative. At least, that is what one Federal Privacy Commissioner thinks. Interested in

[57] Lucie Guibault, *Contracts and Copyright Exemptions in* COPYRIGHT AND ELECTRONIC COMMERCE: LEGAL ASPECTS OF ELECTRONIC COPYRIGHT MANAGEMENT 160 (Bernt Hugenholtz ed., 2000).

[58] Stephen Waddams, The Law of Contracts 399 (4th ed. 1999).

the privacy implications of DRM for some time, the Privacy Commissioner of Canada has recently expressed her concerns as follows:

> We would certainly have concerns about any commercial enterprise in Canada that deployed privacy-invasive DRM technologies in contravention of the provisions of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and the fair information practices underlying it.[59]

This passage, though not intended as dispositive, lends credence to the possibility that a DRM device engaging in excessive monitoring or collection would contravene FIPPS-based legislation. The Canadian Commissioner went on in that same correspondence to suggest that DRM fits within a class of "similar surveillance issues, including RFID tags, computer spyware, and 'lawful access' proposals."[60]

If this is so, then there is good reason to believe that courts might set aside a DRM license aiming to circumvent FIPPS-based legislation on the grounds of the contract law doctrine of "statutory illegality." After all, as one Canadian Supreme Court Justice ruled long ago, "[i]t would be a curious state of the law if, after the Legislature had prohibited a transaction, parties could enter into it, and, in defiance of the law, compel the courts to enforce and give effect to their illegal transaction."[61]

The principle of statutory illegality is maintained in a number of countries whose legal systems stem from the common law. These include the UK,[62] U.S.,[63] Australia, New Zealand[64], and Singapore.[65] It is also maintained in a number of civil law jurisdictions as well.[66]

---

[59] Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Phillipa Lawson, Executive Director, Canadian Internet Policy and Public Interest Clinic (CIPPIC) and Alex Cameron, Associate, CIPPIC (Nov. 24, 2004), available at http://www.cippic.ca/en/projects-cases/copyright-law-reform/LF_Privacy_Commissioner_re_copyright_and_DRM_&_TPM_-_Nove_24_04.pdf.

[60] *Id*. It should be noted that Commissioner Stoddart was careful to disclose her intention to "maintain the neutrality and impartiality expected of a national ombudsman, in order to be able to address complaints fairly and with credibility. This can sometimes mean neither endorsing nor condemning specific technologies and standards — particularly when not all the facts are known."

[61] Bank of Toronto v. Perkins (1884), [1884] 8 S.C.R. 603 at 610, Ritchie C.J.

[62] THE UK LAW COMMISSION, ILLEGAL TRANSACTIONS: THE EFFECT OF ILLEGALITY ON CONTRACTS AND TRUSTS, *available at* http://www.lawcom.gov.uk/docs/cp154.pdf

[63] See Cramer v. Consol. Freightways, Inc., 255 F.3d 683 (9th Cir.2001) (en banc), amended by, 2001 U.S. App. Lexis 19157, cert. denied, 122 S.Ct. 806 (2002).

[64] Colin Fitzgerald v F J Leonhardt pty ltd., No. AP 15 of 1995.

[65] Singapore Law, *Contract Law* §12, http://www.singaporelaw.sg/content/ContractLaw.html (last visited May 11, 2006).

F. FREEDOM *FROM* CONTRACT

My thesis should be clear by now. If anti-circumvention laws are to "ensure that … privacy rights are not reduced or undermined,"[67] amendments to the *Copyright Act* must include a different set of anti-circumvention provisions. We need counter-measures that expressly prohibit the use of DRM to circumvent the protection of privacy law. Achieving an "appropriate balance" requires a legal lock aimed at organizations that would use TPMs, the proposed anti-circumvention law, and the law of contract as a means of hacking away at *PIPEDA*. In order to understand why this is so, it is necessary to describe the chief tool in the DRM hack-back-pack: contractual consent.

When it comes to DRM and privacy, there are two kinds of consent. The first is the consent required to give rise to the DRM contractual license. The second is the consent required to satisfy FIPPs. FIPPs consent is usually a much more robust form of statutory consent. It is crucial to note the distinction. As Daniel Solove notes:

> The law currently does not provide meaningful ability to refuse to consent to relinquish information.…
>
> Giving people property rights or default contract rules is not sufficient to remedy the problem because it does not address the underlying power inequalities that govern information transactions. Unless these are addressed, any privacy protections will merely be "contracted" around, in ways not meaningful either to the problem or to the contract notions supposedly justifying such a solution. People will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought.[68]

Thus, the legal threshold for contractual consent is not well-suited to protecting privacy. Such privacy protections would barely exist if they were within the exclusive domain of contract law. In too many instances, "freedom of contract" means "take-it-or-leave-it." If left to their own devices, DRM licenses will offer all or nothing contracts: "either consumers agree to forgo privacy, or else they forgo access."[69] In some

---

[66] Many civil jurisdictions have codified provisions for statutory illegality. See e.g. CIVIL CODE OF QUÉBEC arts. 8, 9, 989, 990, 1411, 1413, 1417 C.C.Q. (Qué.); CODE CIVIL [C. CIV.] arts. 1131-1133 (Fr.); §309 Nr. 2 BGB (Ger.).

[67] This is an explicit promise made by the Government of Canada. See Copyright Reform Process — Frequently Asked Questions (Mar. 23, 2005), http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp01143e.html.

[68] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 82–85 (2004).

[69] I borrow this way of characterizing things from Ann Bartow.

instances people need freedom *from* contract; privacy is certainly such an instance.

Some FIPPs-based legislative regimes specifically recognize the dangers of leaving private law to its own devices. Such regimes have included counter-measures to the low threshold of contractual consent and the one-sided nature of standard form agreements. For example, Canada's *PIPEDA* contains at least three such elements: (i) an appropriate purpose requirement; (ii) a higher statutory threshold for consent; and (iii) a "refusal to deal" clause. The Canadian approach is discussed briefly below.

1) Appropriate Purpose

Section 5(3) of *PIPEDA* uses the common law construct of the "reasonable person" to limit what the private law might otherwise deem to be a consensual collection of personal information:

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.[70]

Even if a person carefully considers and then expressly consents to the collection of personal information, her consent will be vitiated if the purpose for collection is said to be unreasonable. When parties enter into a contract, so long as there is fairness during the bargaining process, the courts are loath to determine whether the bargain between the parties is reasonable. Section 5(3) therefore offers protections not provided by the common law because it requires the courts to consider the reasonableness of the purpose for collection, use, or disclosure determinative.

2) Higher Statutory Threshold for Consent

In addition to the constraints placed on contractual consent, Principle 4.3 of Schedule 1 in *PIPEDA* provides for a higher threshold of consent than that usually required by the law of contract.[71] Unlike the weaker party to a

---

[70] PIPEDA, *supra* note 20, at § 5(3).

[71] PIPEDA, *supra* note 20, Schedule 1, at § 4.3.2:
The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
§ 4.3.4 states that:
The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

contract, who clicks through a standard commercial agreement, the data subject must be said to consent *knowingly*.

A further provision[72] ensures that the consent has been obtained in a meaningful way. It generally requires that organizations communicate the purposes for collection so that the person will reasonably know and understand how the information will be collected, used, or disclosed.

PIPEDA also ensures a high threshold for consent by contemplating different forms of consent depending on the nature of the information and its sensitivity. "Sensitive" information will generally require more detailed and in some instances express consent. The rationale for this is that "in obtaining consent, the reasonable expectations of the individual are also relevant."[73] Note that this is a different "reasonableness" requirement than the one discussed in the preceding section. There, the reasonableness related to an organization's purposes for collection, use, or disclosure. Here, reasonableness relates to the information subject's actions and whether consent can truly be inferred from them.

One further difference between contractual consent and the consent requirement in *PIPEDA* is that only in the latter can consent be withdrawn with impunity. This signals that, in the privacy context, consent is an ongoing obligation. To some extent, it empowers the weaker party in the transaction to change her or his mind. It is not all-or-nothing and is therefore quite distinct from contractual consent which occurs in an instant.

Canada provides one example of how the concept and application of consent in FIPPs-based legislative regimes is nuanced and difficult. Among other things, the consent requirement will vary based on the purpose of the collection, use, or disclosure of the information; the sensitivity of the information; the reasonable expectation of the parties; and the reasonableness of the information subject's actions in and around the collection process. Generally, the consent threshold is significantly higher in the privacy context than in contract law. The lower threshold of contractual consent is too blunt a tool for privacy law. It therefore ought not to be used to undermine FIPPs, nor to data-mine or conduct surveillance against those who use DRM-delivered intellectual content.

Finally, § 4.3.8 provides that:
An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

[72] PIPEDA, *supra* note 20. Schedule 1, § 4.3.2.

[73] PIPEDA, *supra* note 20. Schedule 1, § 4.3.5.

This point was not overlooked by those who enacted Canada's privacy legislation. *PIPEDA* contains a "refusal to deal" clause, which highlights the need to distinguish between DRM's contractual consent and a significantly higher consent threshold in FIPPs. Principle 3.3 prohibits an organization from requiring an individual to consent to the collection, use, or disclosure of information as a condition of the supply of a product or service. This provision is a clear limit to the take-it-or-leave-it approach of DRM's contractual consent.

The combination of the reasonable purpose requirement, *PIPEDA*'s higher consent threshold, and the "refusal to deal" clause provides protections to individuals which could not be achieved by "self-regulation" through the device of contract. Should DRM licenses be permitted to circumvent these protections? Should consumers, who often have no idea what is at stake, be allowed to "contract-away" these protections unknowingly? Should anti-circumvention laws be drafted in a manner that permits and protects privacy-invasive DRMs possibly operating in breach of privacy or other operative statutes? Perhaps the dictum of the Supreme Court of Canada bears repeating: "[i]t would be a curious state of the law if, after the Legislature had prohibited a transaction, parties could enter into it, and, in defiance of the law, compel the courts to enforce and give effect to their illegal transaction."[74] Privacy law is meant, in some instances, to provide *freedom from contract*.

G. THE SOUNDS OF SILENCE

Having examined the prospect of DRM and its potential impact on privacy, it is alarming to see that most anti-circumvention laws do not adequately deal with privacy protection against excessive uses of DRM.[75]

Most paracopyright laws simply expand the ambit of copyrights by treating acts of circumvention as though they are acts of infringement.[76] The effect of such provisions will be to further expand the law of copyright so that it includes certain *acts* that have nothing to do with copying, such as: "circumvent[ing] a technological measure that effectively controls access to a work…"[77]

---

[74] Ritchie C.J, *supra* note 61, at 610.

[75] The DMCA does contain an circumvention exception for the protection against the collection of personally identifying information (see DMCA, *supra* note 2, § 1201(i)). However, this limitation fails to prevent the monitoring of personal information and assumes that users are capable of circumventing the TPM. The preamble of the European Union's Directive [CITE DIRECTIVE] requires that the collection of information is consistent with the privacy requirements of Directive 95/46/EC of the European parliament (EUCD, *supra* note 2, Preamble, §57). Australia, Hong Kong, New Zealand, and Japan have not adopted any provisions protecting privacy.

[76] Copyright Amendment, *supra* note 2, § 34.01 & 34.02.

[77] DMCA, *supra* note 2, at § 1201(a)(1)(A).

Such provisions place new restrictions on people's ability to examine, investigate, or interact with the technologies destined to become a global distribution channel for delivering digital content. Some academics are concerned that such restrictions could interfere with the security community's "freedom-to-tinker."[78] They believe this will have a chilling effect on important research in cryptography and other areas.

Of course, there are other legitimate reasons to tinker. Unless these are articulated and expressly distinguished from illegitimate circumventions in anti-circumvention legislation, it may be practically impossible to distinguish legitimate from infringing purposes. A relevant example is circumvention or alteration for personal information protection purposes. Data protection legislation is premised on the idea that individuals should be able to gain access to personal information collected about them. Organizations need to be open about the policies and practices relating to their management of others' personal information. In the case of DRM, that information is often not generated or stored at some organization's facilities but is in fact housed on the data subject's own computer by software.

So, one might wish to tinker with a DRM in the interest of knowing whether excessive collection or monitoring is taking place. Perhaps one even suspects this, in which case the purpose of circumvention is to achieve transparency. Just as organizations might not always be in a position to obtain consent in advance when collecting personal information (say, for security purposes), so too might it be necessary for individuals to circumvent or remove personal information without permission in order to secure their personal information against illegitimate collection, use, and disclosure.

Are people permitted to unlock the devices wrapped around legally purchased products in order to investigate what is happening with their personal information? Under what circumstances should be allowed to? What if doing so undermines or defeats an access control mechanism? What remedies are available if the DRM *is* being used in a manner contrary to privacy law? The list of questions is endless and yet none of them have been addressed in most enacted paracopyright regimes. If balanced legislation is the goal then silence simply won't do. Anti-circumvention provisions must specifically stipulate the elements of an illegal circumvention. This must be done in a manner that expressly distinguishes "infringing activities" from other activities such as security research, obtaining access to personal information collected by a DRM, or

---

[78] See e.g., Edward W. Felten, Freedom to Tinker, at http://www.freedom-to-tinker.com (last visited May 4, 2006); Scott A. Craver et al., *Reading Between the Lines: Lessons from the SDMI Challenge,* 10 USENIX SECURITY SYMPOSIUM (2001), http://www.usenix.org/events/sec01/craver.pdf .

exercising control over personal information consistent with the rights guaranteed by FIPPs and privacy law. Moreover, the privacy protections must not be so narrow as to be practically illusory.[79]

In the next section, I "break the silence" by articulating three recommendations that would provide the sort of counter-measures necessary to offset the new powers and protections afforded to TPM and DRM.

H. SUMMARY OF RECOMMENDATIONS

1) Include an Express Provision Prohibiting the Circumvention of Privacy by TPM/DRM, Notwithstanding License Provisions to the Contrary

An appropriate counter-measure could be achieved by transposing the proposed anti-circumvention law into the privacy context. This would generate a new kind of "anti-circumvention" provision which prohibits the use of TPM/DRM to collect, use, or disclose personal information (or otherwise monitor identifiable individuals) in contravention of existing privacy law. In order for this counter-measure to be effective, the law must expressly provide that privacy-waivers or other similar contractual provisions built into the standard forms of DRM licenses shall not be enforceable where the collection, use, or disclosure by the DRM would otherwise contravene privacy law. Likewise, the counter-measure will only be effective if appropriate penalties or remedies for the circumvention of privacy laws are provided.

2) Include an Express Provision Stipulating that a DRM Licence is Voidable when it Violates Privacy Law

In addition to the first recommendation, a broader contractual remedy is needed for individuals whose privacy has been breached. Individuals should have the option to avoid such contracts, treating any obligations set out in the license as at an end.

3) Include an Express Provision Permitting the Circumvention of TPM/DRM for Personal Information Protection Purposes

A third counter-measure would draw a laser-bright line between "infringing" and other purposes for circumventing a TPM/DRM. In particular, the provision must expressly permit the circumvention of

[79] Chillingeffects.org criticizes the privacy exception to the DMCA's anti-circumvention law on two grounds. First, the exemption is limited to a few specific circumstances and second, because the distribution of privacy protection tools is still banned, individuals must have expertise in computer source code in order to protect their privacy on the Internet, http://www.chillingeffects.org/anticircumvention/faq.cgi#QID107 (last visited May 8, 2006).

technological measures where necessary for personal information protection purposes, stating its scope and limits. This would certainly include circumstances in which the DRM is operating in breach of privacy laws, but should also include circumstances where an individual needs to circumvent a technological protection measure in order to confirm the possibility of such a breach. While some might not perceive "mere suspicion" to be a sufficient reason to circumvent a DRM, FIPPS-based privacy law in some countries currently affords similar powers to DRM to collect, use, or disclose personal information without knowledge and consent in order to ensure an organization's security and for other related purposes. To achieve balanced legislation, it is suggested that the scope of permission afforded to individuals to circumvent TPM/DRM should be proportional to the scope of permission afforded to organizations to circumvent the knowledge and consent requirements of privacy law under analogous circumstances.

I. CONCLUSION

Despite the obvious privacy threats that automation, cryptographic techniques, and other DRM surveillance technologies impose, anti-circumvention laws proposed or enacted in various jurisdictions protect these technologies without protecting people from excessive or illegitimate uses of them. In this chapter, I have argued that statutory silence about the permissible scope of use for DRMs *risks too much* from a privacy perspective and that counter-measures are needed.

If laws are to prohibit people from circumventing the technologies that protect copyright, then they ought also to prohibit those same technologies from circumventing the laws that protect privacy. If governments wish to extend its copyright laws to regulate copyright enforcement technologies, then they must include rules that place restrictions upon the private powers that those technologies are now able to exert. If digital and network technologies increase the prospect of digital piracy, then our proposed solutions ought not to diminish the prospect of digital privacy. The legitimate goal of online anti-piracy protection must not succumb to the excessive and dangerous business of online anti-privacy protection.[80]

[80] One begins to believe Freud when re-reading the headnote at ¶17 of the official Federal Court of Canada decision in BMG Canada Inc. v. John Doe, [2004] 3 F.C.R. 241, 2004 FC 488, *available at* http://reports.fja.gc.ca/fc/2004/pub/v3/2004fc34396.htm, which (in)advertently characterizes MediaSentry (a business "enabling the successful growth of online distribution for companies in the entertainment and software industries," http://www.mediasentry.com/corp/overview/index.html) as an "online anti-privacy protection business." I owe the enjoyment of reporting this delicious irony to my brilliant, witty colleague, Jane Bailey, who first spotted this and shared it with me.