SEVEN

Anti-circumvention Legislation and Competition Policy:

Defining a Canadian Way?

Michael Geist*

The Bureau may use its mandate to promote competition and the efficient allocation of resources to intervene in policy discussions and debates regarding the appropriate scope, definition, breadth and length of IP rights.[1]

— Intellectual Property Enforcement Guidelines,
Canadian Competition Bureau, 2000

I believe that the Internet is a transformative technology. While we may have overestimated its impact over the short term, I think that we may also be underestimating its long-term impact .... If we think about what the Internet has enabled so far, just think what could happen to e-business in the future.[2]

— Sheridan Scott, Commissioner of Competition, May 2004

---

* Canada Research Chair in Internet and E-commerce Law, University of Ottawa, Faculty of Law. Thanks to Alex Cameron, Jeremy deBeer, David Fewer, Ian Kerr, and several anonymous reviewers for their helpful comments on earlier versions of this essay; to Misha Feldmann, Alistair Forster, Jamie MacDonald, Michelle Gordon, and Kathi Simmons for excellent research assistance; and to Rene Geist for her exceptional editorial suggestions. Any errors or omissions remain the sole responsibility of the author.

1 **Canada, Competition Bureau,** *Intellectual Property Enforcement Guidelines* (Ottawa: Industry Canada, 2000), <http://cb-bc.gc.ca/epic/internet/incb-bc.nsf/en/ct01992e.html> at s. 6 [*IPEG*].

2 **Sheridan Scott, "Competition Law Compliance" (Speech to the Insight Conference,** May 2004), <http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct02858e.html>.

A. INTRODUCTION

In the early 1990s, Digital Equipment of Canada (DEC), one of the world's leading computer manufacturers,[3] established an "integrated service policy" which tied the servicing of its equipment to the purchase of operating system updates.[4] The Director of the Canadian Competition Bureau launched an action against DEC, arguing that its policy violated the *Competition Act*'s tied selling provisions.[5] The Director was particularly concerned that the policy would impede the entry of third party providers who might service DEC equipment, which would result in reduced competition and the inability for end-users of DEC equipment to access lower prices and enhanced services from the third party providers. In October 1992, the Director and DEC settled the matter as the company agreed to discontinue the policy.[6]

Storage Technology, better known as StorageTek, is a US-based company specializing in data storage and tape backup systems.[7] In July 2004, the company obtained an injunction from a federal court in Massachusetts that prohibited Custom Hardware Engineering and Consulting, a maintenance consulting company, from servicing StorageTek's products. Unlike the DEC case, where the computer maker sought to tie the sale of products and services, StorageTek did not need system upgrades or other enticements to keep third party providers at bay. Instead, it was able to rely on computer code and copyright law to effectively eliminate any third party competitors from servicing its products.

The DEC and StorageTek cases provide vivid illustrations of the shift over the past decade in the approach to intellectual property protection and its impact on marketplace competition. Intellectual property protections have always generated debate about their marketplace impact.[8] Patents and copyrights represent a state-sanctioned, limited monopoly on a

---

3 Richard Morochove, "IBM staff cuts highlight deeper problems" *The Toronto Star* (1 December 1991) H1.

4 George N. Addy, "Competition Policy and Intellectual Property Rights: Complementary Framework Policies for a Dynamic Market Economy" (Speech to the XXXVIth World Congress of the AIPPI, June 1995), <http://cb-bc.gc.ca/epic/internet/incb-bc.nsf/en/ct01407e.html>.

5 *Competition Act*, R.S.C. 1985, c. C-34, s. 77.

6 Above note 4.

7 Declan McCullagh "StorageTek Wins Copyright Injunction" *CNET News.com* (July 12, 2004), <http://ecoustics-cnet.com.com/StorageTek+wins+copyright+injunction/2100-1015_3-5266031.html>.

8 Above note 4.

particular work or invention, forcing policy makers and scholars to consider the optimum balance between protection and access. While competition policy in the 1980s and the early 1990s embraced intellectual property as pro-competitive, during the past ten years, the shift toward digital content, the ability to use technological protection measures to limit access and the use of that content, as well as the creation of legal protections for such technology (rather than the underlying content), requires a different framework for analysis.

The legal catalyst for these changes was the completion in 1996 of the World Intellectual Property Organization's *Copyright Treaty* (*WCT*)[9] and *Performances and Phonograms Treaty* (*WPPT*),[10] collectively referred to the WIPO Internet Treaties.[11] The twin treaties have had a transformative impact on the scope of copyright law, creating what some experts have referred to as "super-copyright"[12] or "para-copyright."[13] Both treaties feature a broad range of provisions targeting digital copyright issues; however, the most controversial provisions mandate the establishment within ratifying states' national law of anti-circumvention provisions that provide "adequate legal protection and effective legal measures" against the cir-

---

9 *WIPO Copyright Treaty*, 20 December 1996 36 I.L.M. 65, adopted by the Diplomatic Conference on 20 December 1996, <www.wipo.int/clea/docs_new/en/wo/wo033en.html> [*WCT*].

10 *WIPO Performances and Phonograms Treaty*, 20 December 1996 36 I.L.M. 76, adopted by the Diplomatic Conference on 20 December 1996, <www.wipo.int/clea/docs/en/wo/wo033en.htm> [*WPPT*].

11 The two WIPO Internet Treaties were formally adopted on December 20, 1996, though they only took effect in 2002 after each one reached the thirty-country ratification mark. As of January 2005, the *WCT* had fifty-one country ratifications, while the *WPPT* had forty-nine country ratifications. The United States and Japan are the two most notable countries on the ratification list. The European Union has yet to ratify, though some member states have incorporated the necessary provisions into their national copyright law. The remainder of the list is comprised of countries such as Indonesia and the Ukraine, often cited as leading sources of pirated music and software, as well as smaller developing countries from Africa, Latin America, and Asia, including Burkina Faso, Gabon, Saint Lucia, and Togo.

12 Industry Canada, *Memorandum Concerning the Implementation in Canada of Articles 11 and 18 of the WIPO Treaties Regarding the Unauthorized Circumvention of Technological Measures Used in Connection with the Exercise of a Copyright Right* by Mark S. Hayes (Ottawa: Ogilvy Renault, 2000), <http://strategis.ic.gc.ca/epic/internet/inippd-dppi.nsf/vwapj/ogilvyrenault_e.pdf/$FILE/ogilvyrenault_e.pdf> [*Hayes*].

13 Dan L. Burk, "Anticircumention Misuse" (2002-2003) 50 UCLA L. Rev. 1095 at 1096.

cumvention of effective technological protection measures (TPMs).[14] While that obligation may sound complex (and, as discussed below, it has been subject to a wide variety of interpretations), at its core it simply requires countries that ratify the WIPO Internet Treaties to establish legislation that protects against the circumvention of the digital locks (known as TPMs and frequently manifested as Digital Rights Management or DRM) used by content owners to restrict access or use of digital content.

This essay examines the competitive impact of anti-circumvention legislation in light of the introduction on 20 June 2005 of Bill C-60, which if enacted, would incorporate anti-circumvention provisions into Canadian law.[15] Should that happen, the Canadian Competition Bureau, which has previously indicated that it will consider intervening in the policy discussions surrounding intellectual property rights, will have an important role to play since the experience in other jurisdictions, most notably the United States, suggests that implementing legislation can have a damaging impact on innovation and marketplace competition.

Part one of this essay provides the necessary background for assessing TPM legislation and its competitive impact by examining the tensions between intellectual property and competition law. This part focuses on two provisions in the *Competition Act*, the Competition Bureau's Intellectual Property Enforcement Guidelines, and a handful of cases that have featured a noteworthy intellectual property component.

Part two of the essay surveys some of the alternative anti-circumvention provision implementations found in countries around the world. It notes that there is a fairly diverse array of implementing provisions, demonstrating that the US model found in the *Digital Millennium Copyright Act*, is but one approach open to Canada. In addition to discussing different statutory provisions, this part draws on some of the recent experience associated with TPMs and anti-circumvention legislation.

Part three examines the likely marketplace and competitive impact of Bill C-60's anti-circumvention provisions. The essay analyzes the core provisions, noting the link between circumvention and copyright infringement as well as the uncertainty surrounding a provision that targets circumvention service providers. It argues that the Canadian approach has several positive elements including the recognition of the flexibility

---

14 **Above note 9, at Arts. 11, 12; above note 10,** at Arts. 18, 19.

15 **Bill C-60,** *An Act to amend the Copyright Act,* 1st Sess., 38th Parl., 2005, Preamble, <www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF> [*Copyright Amendment*].

inherent in the WIPO Internet treaties, the linkage between copyright infringement and the anti-circumvention provisions, as well as the decision to focus on the act of circumvention, rather than on devices that can be used to circumvent.

The essay also outlines several recommendations for how the bill could be improved. First, it recommends parallel amendments to the *Competition Act* to ensure that the Competition Bureau is not restricted in its ability to bring actions against abusive behaviour stemming the application of the anti-circumvention provisions. Second, it calls for the creation of a positive, user right to circumvent for lawful purposes, arguing that such an approach is consistent with recent Supreme Court of Canada jurisprudence. Third, it calls for clarification of Bill C-60's anti-circumvention service provider provision, which has generated concern and uncertainty among software developers and researchers.

B. CANADIAN COPYRIGHT LAW AND COMPETITION POLICY

Intellectual property issues have commanded increasing attention from scholars and the Competition Bureau in recent years. [16] Howard Wetston, then the Competition Bureau's Director of Investigations, speaking of the pre-*WIPO Internet Treaty* copyright law, commented in 1990 that the Competition Bureau once viewed intellectual property as a "form of necessary evil that could easily impose excessive costs on consumers."[17] That view had changed by the 1990s, with intellectual property viewed as pro-competitive, fostering innovation and creativity.

The *Competition Act* includes two key provisions specific to intellectual property, including copyright. First, section 32(1) provides that:

> In any case where use has been made of the exclusive rights and privileges conferred by one or more patents for invention, by one or

16 See Herbert Hovenkamp, Mark D. Janis, & Mark A. Lemley, *IP and Antitrust: An Analysis of Antiturst Principles Applied to Intellectual Property Law* (New York: Aspen Publishers, 2004); W.T. Stanbury, *On the Relationship Between Competition Policy and the Copyright Act in Canada*, (2001) [unpublished].

17 Howard I. Wetston, "Competition Policy and Intellectual Property Rights: Complementary Framework Policies for a Market Economy" (Speech to the Conference on Global Rivalry and Intellectual Property: Developing Canadian Strategies, April 1990), <http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct01467e.html>.

> more trade-marks, by a copyright or by a registered integrated circuit topography, so as to
>
> *(a)* limit unduly the facilities for transporting, producing, manufacturing, supplying, storing or dealing in any article or commodity that may be a subject of trade or commerce,
> *(b)* restrain or injure, unduly, trade or commerce in relation to any such article or commodity,
> *(c)* prevent, limit or lessen, unduly, the manufacture or production of any such article or commodity or unreasonably enhance the price thereof, or
> *(d)* prevent or lessen, unduly, competition in the production, manufacture, purchase, barter, sale, transportation or supply of any such article or commodity,
>
> the Federal Court may make one or more of the orders referred to in subsection (2) in the circumstances described in that subsection.[18]

Section 32(2) grants the Federal Court a wide range of remedies including the right to declare a license void or order that licenses be granted to such persons and on such terms as the court believes is appropriate.[19] It is noteworthy that these powers are subject to section 32(3), which provides that "no order shall be made under this section that is at variance with any treaty, convention, arrangement or engagement with any other country respecting patents, trade-marks, copyrights or integrated circuit topographies to which Canada is a party."[20]

The Competition Bureau's Intellectual Property Enforcement Guidelines, finalized in 2000, provide further guidance on the Bureau's interpretation of these provisions.[21] The *IPEGs* note that "the Bureau will seek a remedy for the unilateral exercise of the IP right to exclude under section 32 only if the circumstances specified in that section are met and the alleged competitive harm stems directly from the refusal and nothing else."[22] Moreover, it advises that "[e]nforcement under section 32 requires proof of undue restraint of trade or lessened competition" that "[t]he Bu-

---

18 **Above note 5 at s. 32(1).**
19 *Ibid.*, at s. 32(2).
20 *Ibid.*, at s. 32(3).
21 **See above note 1.**
22 *Ibid.* at s. 4.2.2.

reau expects such enforcement action would be required only in certain narrowly defined circumstances."[23]

Section 32 therefore has limited application in a copyright context, since its requirements for use are very difficult to meet. In fact, the Bureau acknowledges as much in the *IPEGs*, concluding that only in very rare circumstances would all the factors needed for an action be met.[24]

The second noteworthy section related to copyright is section 79(5). In addressing the right of the Bureau to act in cases of abuse of dominance, the subsection provides that:

> For the purpose of this section, an act engaged in pursuant only to the exercise of any right or enjoyment of any interest derived under the *Copyright Act*, *Industrial Design Act*, *Integrated Circuit Topography Act*, *Patent Act*, *Trade-marks Act* or any other Act of Parliament pertaining to intellectual or industrial property is not an anti-competitive act.[25]

As the *IPEGs* note, this section confirms the Bureau's view that a mere exercise of an intellectual property right does not constitute a violation. Both former Directors of Investigations and Research Wetston and Addy have emphasized that they do not believe that section 79(5) provides a blanket exemption for abuse of intellectual property rights. Wetston argued that the exception "applies to acts that are engaged in 'pursuant only to the exercise of' rights or enjoyment of interests derived under intellectual property statutes … [t]he wording of the exception clearly suggests that the abuse of dominance provisions remain applicable to practices that are shown to constitute abuses of intellectual property rights."[26] Similarly, Addy concluded that "[t]his exception does *not* provide a blanket exemption for intellectual property holders from the application of the abuse provisions. The wording of the exception suggests that the provisions remain applicable to practices which are shown to constitute *abuses* of intellectual property rights (as opposed to the mere exercise of such rights)."[27]

Notwithstanding these comments, the Competition Tribunal has been very reluctant to tamper with intellectual property agreements. In *Canada (Director of Investigation and Research) v. Tele-Direct (Publications) Inc.*, a 1997 trademark case, the Director argued that section 79(5) "does not pre-

23 *Ibid.*
24 *Ibid.*
25 See above note 5, at s. 79(5).
26 Above note 17.
27 Above note 4.

clude a finding that 'abuses' of intellectual property are anti-competitive acts." The tribunal agreed that there may be instances where a trademark can be abused, but it made clear that such instances are rare, concluding that:

> While the evidence suggests that Tele-Direct is motivated, at least in part, by competition in its decision to refuse to license its trade-marks, the fact is that the Trade-marks Act allows trade-mark owners to decide to whom they will license their trade-marks. The respondents' motivation for their decision to refuse to license a competitor becomes irrelevant as the Trade-marks Act does not prescribe any limit to the exercise of that right.[28]

That same year, the Competition Tribunal affirmed that similar analysis was applicable to copyrights in *Canada (Director of Investigation and Research) v. Warner Music Canada Inc.*, a case involving Warner Music and its decision to refuse to license sound recordings to BMG, which maintained a competing music club.[29]

Consistent with these decisions, the plain language of the *Competition Act*, as well as the interpretation found in the *IPEGs*, there is an evident reluctance to interfere with the exercise of intellectual property rights.[30] While that may be an appropriate approach for the exercise of traditional copyrights, there is a danger that the legislation may leave the Bureau statutorily unable (as opposed to unwilling) to intervene in certain circumstances. These may include instances where competition is unduly harmed by the exercise of intellectual property rights yet is saved by an international treaty to which Canada is a party or where abuse of a dominant position is supported by rights provided under the *Copyright Act*.

The Competition Bureau's reluctance to intervene in intellectual property matters has coincided with a dramatic increase in the pace of Canadian copyright reform. In 1987, statutory reforms addressed the "grey market," making it unlawful to import works created outside the coun-

---

28 *Canada (Director of Investigation and Research) v. Tele-Direct (Publications) Inc.* (1997), 73 C.P.R. (3d) 1 at para. 33.

29 *Canada (Director of Investigation and Research) v. Warner Music Canada Inc.* (1997), 78 C.P.R. (3d) 321.

30 A notable exception is found in the *Copyright Act*, which provides at s. 70.5 that the Director of the Competition Bureau has the right to access any agreement of a collective society filed with the Copyright Board of Canada. If the Director considers that the agreement is contrary to the public interest, the Director may ask the Copyright Board to examine the agreement.

try that would infringe copyright.[31] The next year, the government completed "Phase One" of a new copyright reform process by adding explicit moral rights requirements, implementing specific offences for secondary infringement and rebroadcasting, adding industrial designs to the *Copyright Act*, and establishing the Copyright Board of Canada as the successor to the Copyright Appeal Board.[32]

In 1993, the government reduced registration requirements for copyright protection, granted courts the right to direct the responsible minister to prevent importation of any work that would infringe copyright, and expanded the definitions for music works, performances, and cinematographic works. It also added rental rights for computer programs and sound recordings, thereby eliminating the rental market for those works.[33]

After adding new performers rights in 1994,[34] the government completed "Phase Two" of the copyright reform process in 1997 by providing protection for exclusive book distribution arrangements, by adding neighbouring rights provisions to further compensate producers and performers, by establishing statutory damages, and by creating a new private copying compensation system that includes a levy on blank media.[35]

Not only have these changes vested new powers in rights holders, but they have also shaped the marketplace for such works. Restrictions on importation of certain works, the addition of rental rights for computer programs and sound recordings, as well was the addition of industrial designs and the private copying system have each had an important impact on the Canadian market. They have eliminated potential new consumer markets (rental rights), created significant new costs to existing markets (private copying), or injected new restrictions on innovation (industrial designs).

---

31 *Customs Tariff*, R.S.C. 1987, c. C-49, ss. 118–19.

32 *An Act to Amend the Copyright Act and other acts in consequence thereof*, R.S.C. 1988, c. C-15.

33 *Intellectual Law Improvement Act*, R.S.C. 1993, c. 15; *An Act to amend the Copyright Act*, R.S.C. 1993, c. 23; *NAFTA Implementation Act*, R.S.C. 1993, c. 44.

34 *World Trade Organization Agreement Implementation Act*, R.S.C. 1994, c. 47, <http://laws.justice.gc.ca/en/W-11.8/110729.html>.

35 *An Act to Amend the Copyright Act*, R.S.C. 1997, c. 24.

C. TPMS AND ANTI-CIRCUMVENTION LEGISLATION

1) TPMs: An Introduction

Owners of online databases and other digital content deploy TPMs to establish a layer of technical protection that is designed to provide greater control over their content. Although TPMs are sometimes referred to as Digital Rights Management (DRM), the two are not the same as TPMs are component parts of an overall DRM system. The content industry has touted TPM's promise for more than decade, maintaining that technological locks could prove far more effective in curtailing unauthorized copying, distribution, performance, and display of content than traditional copyright laws.[36] While TPMs are frequently associated with encryption protection, TPMs encompass a broad range of technologies including more mundane approaches such as password protections.

While TPMs do not provide absolute protection — research suggests all TPMs can eventually be broken — companies continue to actively search for inventive new uses for these digital locks.[37] In certain instances their use is obvious to consumers. For example, DVDs contain a content scramble system that limits the ability to copy even a small portion of a lawfully purchased DVD.[38] Similarly, purchasers of electronic books often find that their e-books contain limitations restricting copying, playback, or use of the e-book on multiple platforms.[39] In fact, e-books are frequently saddled with far more restrictions than are found in their paper-based equivalents.

Sometimes the use of a TPM is far less obvious to consumers, manipulating markets to the detriment of consumers, rather than protecting content. For example, DVDs typically contain regional codes that limit the ability to play a DVD to a specific region.[40] The consumer is often unaware

---

36 Stefan Bechtold, "The Present and Future of Digital Rights Management"in Eberhard Becker, Willms Buhse, Dirk Günnewig, & Niels Rump,eds., *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (Berlin: Springer, 2003), <www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf> at 597–654.

37 Cory Doctorow, "Digital Rights Management" (September 21, 2004), <www.changethis.com/4.DRM>.

38 Rob Pegoraro, "DVD-Piracy Paranoia Proves Counterproductive," *The Washington Post* (22 June 2003) F7.

39 Mary Roach, "This Article Cannot Be Read Aloud" *Inc Magazine* (June 2001), <www.inc.com/magazine/20010615/22778.html>.

40 Patrick Marshall, "Wrong DVD code for region can derail your movie plans" *The Seattle Times* (3 July 2004) E6.

of the region code until they purchase a DVD while on vacation in one region only to find that they cannot play the disc on their DVD player when they return home. Online music services contain similar TPMs. For example, Apple iTunes sets limits on the number of copies that can be made from its music files,[41] while HMV in the United Kingdom has announced plans to launch an online music service that will feature songs that cannot even be played on the popular Apple iPod MP3 player.[42]

Of even greater concern is the increasing use of TPMs in completely unexpected environments. For example, Hewlett-Packard has begun to install TPMs into its printer cartridges.[43] The technology is used to block consumers from purchasing cartridges in one region and using them in another, thereby enabling the company to maintain different pricing structures for the same product in different global markets.

Despite the proliferation of TPMs, few consumers are aware of their existence and many manufacturers are loath to disclose their use. Some record labels have begun to post warnings on CDs,[44] yet few consumers would notice the disclaimer cautioning that their CD contains technological limitations that may inhibit them from being played in their car, on their personal computer, home stereo or other preferred electronic device. Beyond CDs, there is evidence that other TPM-enabled content delivery services similarly disrupt consumer expectations.[45]

In fact, consumers may soon find that these technological limitations force them to incur significant new costs as they face little alternative but to continually re-purchase content so that it functions on new equipment. The industry acknowledges as much, as according to Kevin Gage, a Vice-President with the Warner Music Group, this year [in 2005] we will begin

---

41 See "Apple – iTunes – Music Store," <www.apple.com/itunes/store/>. ("You can burn individual songs onto an unlimited number of CDs for your personal use, listen to songs on an unlimited number of iPods and play songs on up to five Macintosh computers or Windows PCs.")

42 Tony Smith, "HMV iPods not compatible with store's music downloads" *The Register* (17 June 2004), <www.theregister.co.uk/2004/06/17/hmv_ipod/>.

43 David Pringle & Steve Stecklow, "Electronics With Borders: Some Work Only in the U.S."*Wall Street Journal* (18 January 2005) B1.

44 Aaron Pressman, "Consumers in crossfire of labels' war on piracy" *The Christian Science Monitor* (4 March 2002) 18.

45 Deirdre K. Mulligan, John Han, & Aaron J. Burstein, "How DRM-based content delivery systems disrupt expectations of 'personal use'" in *Proceedings of the 2003 ACM workshop on Digital rights management* (New York: ACM Press, 2003), <www.sims.berkeley.edu/~john_han/docs/p029-mulligan.pdf>.

to see people with "large libraries of content that won't play with their devices."[46]

The impact of TPMs also extends far beyond consumer fairness. The same technologies can function much like spyware by invading the personal privacy of user. For example, TPMs can be used to track consumer activity and report the personal information back to the parent company.[47] There is also concern that TPMs can be used to induce security breaches. Recent reports indicate that hackers are using these technologies in the Microsoft Windows Media Player to trick users into downloading massive amounts of spyware, adware, and viruses.[48]

2) Legal Protection for TPMs

Given the flawed protection provided by TPMs, content owners have lobbied for additional legal protections to support them. Although characterized as copyright protection, this layer of legal protection does not address the copying or use of copyrighted work. Instead, it focuses on the protection of the TPM itself, which in turn attempts to ensure that the underlying content is only accessed and used as controlled by the copyright owner.

Both the *WCT* and *WPPT* contain an anti-circumvention provision requirement. Article 11 of the *WCT* provides that:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.[49]

Similarly, Article 18 of the *WPPT* provides that:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technologi-

---

46 Stefanie Olson, "Piracy fears threaten Hollywood innovation" *TechRepublic* (29 September 2004), <http://techrepublic.com.com/5102-22-5388602.html>.

47 Article 29 Data Protection Working Group, "Working Document on data protection issues related to intellectual property rights" (18 January 2005), <http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2005/wpdocs05_en.htm#wp104>.

48 Tom Spring, "Microsoft to Boost Media Player Security" *PCWorld.com* (20 January 2005), <www.pcworld.com/news/article/0,aid,119362,00.asp>.

49 Above note 9, at Art. 11.

> cal measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.[50]

The interpretation of several key words and phrases within these provisions play an important role in determining the scope and coverage of anti-circumvention legislation once implemented into national law. First, the treaties do not provide definitions for the words "adequate" and "effective" with respect to legal protections. Since all TPMs can be circumvented, the provision points to the fact that perfection is not required nor does a minimum global standard exist. Instead, any national legislation will be measured against an adequacy criterion such that the legal protections must provide some measure of protection that a reasonable person would perceive as evidencing effectiveness.

The meaning of "effective technological measures" has also generated some discussion among legal experts.[51] Given the imperfections of TPMs, it is clear that the provision does not afford protections merely for the most effective, technologically advanced TPMs. Conversely, a rights holder may not simply describe any technological control as a TPM and expect to benefit from legal protection. Protections that are plainly ineffective would be unlikely to merit legal protection.[52]

"Circumvention" is also subject to interpretation. Activities such as a brute force decryption of a TPM or hacking a closed system would obviously be covered by such a provision, though criminal provisions in many jurisdictions, including Canada, could similarly be applied to incidents that are otherwise described as computer crime.[53] Circumvention could be interpreted to extend to more mundane activities, however, including

---

50 Above note 10 at Art. 18.

51 See for example Heritage Canada, *Technical Protection Measures: Legal Protection of TPMs* by I. Kerr, A. Maurushat, & C. Tacit, (Ottawa: Nelligan O'Brien Payne, 2003) at 7–8, <www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/protection_e.pdf> [Heritage Canada]; see also Jacques de Werra, "The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)" (Paper presented to the ALAI Congress, June 2001) [unpublished],<www.law.columbia.edu/conferences/2001/program_en.htm> at 10.

52 See *Heritage Canada*, *ibid.* at 8.

53 *Criminal Code*, R.S.C. 1985, c. C-46, ss. 342.1, 430(1).

posting passwords or registration numbers on the Internet.[54] Moreover, although not obviously included within Article 11, some countries believe that incorporating protection against devices that can be used to circumvent a TPM, including software programs, is necessary to ensure that the national legislation meets the adequate legal protection standard.[55]

The most contentious interpretative issue lies with the latter half of the provision. As Professor Ian Kerr notes in his comprehensive study of TPMs:

> A literal interpretation of the requirements that TPMs must be "used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention" and "restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law" *suggests that TPMs must restrict acts that are protected by copyright law in order to qualify for legal protection* pursuant to article 11 of the *WCT*. According to this interpretation, article 11 of the *WCT* does not require states to prohibit the circumvention of a TPM in order to benefit from one of the exceptions to copyright (such as, for example, fair dealing in Canada). This suggests that only circumventions resulting in copyright infringement will be subject to article 11.[56] [emphasis added]

Kerr acknowledges, however, that others have interpreted the clause differently, focusing instead on the latter phrase "restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." The alternate interpretation posits that this provision seeks to protect rights holders against the circumvention of TPMs which limit access, effectively creating a *sui generis* right of access control.[57]

3) Implementing Article 11 (WCT) and Article 18 (WPPT)

In view of the broad range of interpretations open to Article 11 of the *WCT* (as well as Article 18 of the *WPPT*), it should come as little surprise to find that there is wide divergence among ratifying countries in the way they have

---

54 Ian R. Kerr, Alana Marushat, & Christian S. Tacit, "Technological Protection Measures: Tilting at Copyright's Windmills" (2002-2003) 34 Ottawa L. Rev. 7 at para. 54.

55 See for example U.S., Bill H.R. 2281, *Digital Millennium Copyright Act*, 105th Cong., 2d sess., 1998, <www.copyright.gov/title17/>, [*DMCA*] at s. 1201(a)(2).

56 Above note 54 at paras. 102–3.

57 *Ibid*. at para. 104.

implemented their anti-circumvention obligations into national law. Although a comprehensive review of the implementing legislation of the more than fifty countries that have ratified the WIPO Internet Treaties is beyond the scope of this essay, a spectrum of approaches is presented below.[58]

a) United States

The US ratification of the WIPO Internet Treaties was incorporated into the *Digital Millennium Copyright Act of 1998* [*DMCA*]. The US adopted a strongly protectionist approach, adopting provisions beyond what was strictly required under the WIPO Internet Treaties. The US anti-circumvention provision includes the following:

> **§s. 1201. Circumvention of copyright protection systems**
>
> **(a) Violations Regarding Circumvention of Technological Measures.—**
> (1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title…
> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.
> (3) As used in this subsection—
> (A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

58 For a compendium of national implementing legislation, see Standing Committee on Copyright and Related Rights, *Survey on Implementation Provisions of the WCT and WPPT,* UN WIPO, 9th Sess., (2003) <www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_9_6.pdf> [*WIPO Survey*].

> (B) 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.
>
> **(b) Additional Violations**
>
> (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.[59]

In addition to the above-noted provisions, the *DMCA* contains a series of exceptions designed to preserve certain copyright rights. These include a provision mandating a regular consultation on whether the *DMCA* provisions are likely to impair non-infringing uses of works.[60] The Librarian of Congress, together with the Registrar of Copyrights, are asked to consider a series of factors and to establish exceptions where needed.[61] Moreover, the statute contains several limited exceptions for non-profit libraries,[62] law enforcement,[63] reverse engineering,[64] encryption research,[65] security testing,[66] and privacy.[67] These exceptions have proven largely ineffective since the Librarian of Con-

---

59 **Above** note 55 at ss. 1201(a)(1)–(2), (b)(1).
60 *Ibid*. at s.1201(a)(1)(C).
61 *Ibid*. at s.1201(a)(1)(C)(i)–(v).
62 *Ibid*. at s.1201(d).
63 *Ibid*. at s.1201(e).
64 *Ibid*. at s.1201(f).
65 *Ibid*. at s.1201(g).
66 *Ibid*. at s.1201(j).
67 *Ibid*. at s.1201(i).

gress has established few exceptions and the exceptions apply solely to the act of circumvention. They do not extend to the provisions on devices, including new technologies, products, services, devices, and components that are used for purposes related to circumvention.

US implementation of the WIPO Internet Treaties in the *DMCA* is notable in several respects. First, the *DMCA* provisions include comprehensive restrictions on devices. These provisions shift the focus away from the actual alleged infringer and instead target manufacturers, service providers, and other innovators whose products are captured by the *DMCA* language. That language is quite broad as it even includes marketing products that can be used for the purposes of circumvention.

Second, the *DMCA* provisions contain only limited reference to the actual copyright underlying the TPM. The provisions do refer to TPMs that control access to "works under this title," yet it is clear that the provisions effectively extend beyond copyrightable work. For example, Professor Dan Burk of the University of Minnesota notes that a work might include copyrightable content mixed with uncopyrightable content (such as facts). If both are placed under the control of a TPM, an attempt to extract the unprotectable content from a copyrighted work by circumventing the TPM would result in an infringement under the Act.[68]

Third, although the section also includes a provision that states that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title,"[69] the statute does not provide a positive obligation on the copyright holder to ensure that the user retains their fair use rights. As Burk again notes,

> [b]ecause the right of access is defined in terms of the technological system, rather than the terms of the content, both copyrightable and uncopyrightable materials will be covered by the anticircumvention right. The controlled content may include uncopyrightable facts, public domain materials, or purely functional works, yet unauthorized access will constitute just as much a violation as it would if the content were copyrightable original expression.[70]

Burk's reference to public domain materials is particularly apt, since the *DMCA* also fails to include a limitation on the term of protection for a work under a TPM. Accordingly, unlike traditional copyright law, which

---

68 **Above note 13** at 1108.
69 **Above note 55 at s.1201(c).**
70 **Above note 13 at 1108.**

limits the term of protection, there is no limit to the term of protection accorded to a TPM, effectively extending the term of protection for works protected by a TPM indefinitely.[71]

Fourth, and most importantly, the litigation experience under the *DMCA* has raised significant concerns about the provisions negative effects on research, innovation, and competition. As former Cyber-security Czar Richard Clarke acknowledged in 2002 "a lot of people didn't realize that [the *DMCA*] would have this potential chilling effect on vulnerability research."[72] For example, in 2000, Edward Felten, a Princeton researcher, sought to release an important study on encryption that included information that could be used to circumvent a technological measure. When he publicly disclosed his plans, he was served with a warning that he faced potential legal liability if he went public with his findings, since the mere release of circumvention information might violate US law.[73]

One year later, Dmitry Sklyarov, a Russian software programmer, was arrested in Las Vegas when he presented a paper on the strengths and weaknesses of software used to protect electronic books.[74] Sklyarov, who was employed by a Moscow-based software company called Elcomsoft, was charged with violating criminal provisions found in the *DMCA*. He was initially held without bail and faced a maximum fine of US$500,000 and five years in prison. Although Sklyarov was eventually released, the case had an impact within the scientific community as researchers with ties to the United States reportedly removed information from websites for fear of facing potential lawsuits.[75]

Despite the negative publicity attached to these cases,[76] reports regularly surface of new incidents. In 2002, Hewlett-Packard threatened to launch a

---

71 *Ibid*. at 1107.

72 Hiawatha Bray, "Cyber Chief Speaks on Data Network Security," *The Boston Globe* (17 October 2002).

73 Lisa M. Bowman, "Researchers face legal threats over SDMI hack" *CNET News.com* (23 April 2001), <http://news.com.com/Researchers+face+legal+threats+over+SDMI+hack/2100-1023_3-256277.html>.

74 Michael Geist, "Russian's case shows severity of copyright law" *Globetechnology.com* (26 July 2001), <http://news.globetechnology.com/servlet/GAMArticleHTMLTemplate?tf=globetechnology/TGAM/NewsFullStory.html&cf=globetechnology/tech-config-neutral&slug=TWGEISY&date=20010726>.

75 Electronic Frontier Foundation, "Unintended Consequences: Five Years Under the *DMCA*" v.3 (24 September 2003), <www.eff.org/IP/*DMCA*/unintended_consequences.pdf> [EFF].

76 Adobe Software, which initiated the complaint against Dmitry Sklyarov, backed off soon after it was targeted with protests and other negative publicity. Geist, above note 74.

suit against researchers who planned to publish information on flaws in an HP UNIX operating system.[77] One year later, Blackboard Inc., an educational software company, used a *DMCA* threat to stop a presentation on research related to security vulnerabilities in its products at a conference in Atlanta.[78]

At a practical level, experts now issue warnings to researchers and the scientific community on potential copyright risks. For example, consider the advice of two US practitioners in a recent article on reverse engineering:

> … a company may find it beneficial to educate its technical personnel specifically about the practical implications of the *DMCA*. Engineers and scientists should be made aware that copyrightable material may be found in numerous contexts, some unexpected. An engineer who is routinely accustomed to deconstructing a semiconductor chip or analyzing software performance must know that while such activities are still generally permissible, certain related analyses such as decompiling or disassembling a software program resident on the chip (which may have become second nature for many technologists in the digital arts) may now be unlawful, if such analyses necessitate circumventing an access control measure.
>
> …
>
> Companies for whom reverse engineering and design around efforts are a principal competitive tool may find it desirable to lobby their congressmen to expand Subsection 1201(f) of the *DMCA* so as explicitly to permit reverse engineering for a wider variety of purposes. Until the *DMCA* is revised, however, companies must tread carefully, understand the limitations and increased scrutiny that Congress and marketplace realities have imposed upon reverse engineering, and design and implement their intellectual property policies and reverse engineering activities accordingly.[79]

The *DMCA*'s effects have extended beyond the scientific community into the marketplace with anti-circumvention cases covering copyright and non-copyright matters. On the copyright front, the prohibition against circumventing devices has been successfully invoked to limit competition in several instances. In one of the first *DMCA* cases, Real Networks, an Inter-

---

77 **EFF, above** note 75.

78 *Ibid*.

79 **Jeffrey Sullivan & Thomas Morrow, "Practicing Reverse Engineering in an Era** of Growing Constraints under the Digital Millennium Copyright Act and Other Provisions" (2003) 14 Alb. L.J. Sci. & Tech. 1 at 49–52.

net streaming company, sued a company called Streambox over the availability of a product that allowed for the recording of streamed content.[80]

Real Networks encoded its streamed content with "Copy Switch," a piece of data that contained the content owner's preference regarding whether or not the stream could be copied by end users. Streambox developed the equivalent of a VCR for streaming content, enabling end users to access and download copies of RealMedia files that were streamed over the Internet much like television programming. In order to do so, the Streambox product circumvented the Real Networks authentication procedure.

A federal court in Washington concluded that the Streambox product was a device that circumvented the Real Networks' TPM. In its defence, Streambox argued that its product could be used for lawful purposes, namely fair use copying of the programming. While the court did not challenge the notion that the device could be used for fair use purposes, it concluded that:

> Under the *DMCA*, product developers do not have the right to distribute products that circumvent technological measures that prevent consumers from gaining unauthorized access to or making unauthorized copies of works protected by the Copyright Act. Instead, Congress specifically prohibited the distribution of the tools by which such circumvention could be accomplished. The portion of the Streambox VCR that circumvents the technological measures that prevent unauthorized access to and duplication of audio and video content therefore runs afoul of the *DMCA*.[81]

Moreover, the court acknowledged that the *DMCA* was effectively divorced from traditional copyright analysis. It cited with approval the conclusion that

> a given piece of machinery might qualify as a stable item of commerce, with a substantial noninfringing use, and hence be immune from attack under *Sony's* construction of the Copyright Act but nonetheless still be subject to suppression under Section 1201. … As such, equipment manufacturers in the twenty-first century will need to vet their products for compliance with Section 1201 in order to avoid a circumvention claim, rather than under *Sony* to negate a copyright claim.[82]

---

80 *RealNetworks Inc. v. Streambox Inc.*, 2000 U.S. Dist. LEXIS 1889 [*Streambox*].
81 *Ibid.* at 2.
82 *Ibid.* at 22.

In recent years, several similar cases have been launched by the motion picture industry against software makers that allow users to make copies of their store-bought DVDs.[83] DVDs are encoded with several anti-copying technologies including Macrovision and the Content Scramble System (CSS). The Macrovision technology is designed to stop the copying of a DVD into analog format,[84] while CSS is an encryption tool that restricts the playback functionality of DVDs to those devices that contain the associated electronic keys.[85] In other words, the DVDs can only be played on devices that are authorized by the owner of copyright in the DVD. The Copyright Control Authority (CCA) controls access to the keys necessary to decrypt the CSS.[86]

321 Studios, a software company based in St. Louis, marketed a software program that allowed users to make backup copies of their store-bought DVDs. The company faced litigation from both Macrovision and MGM, a leading Hollywood motion picture studio. 321 Studios argued that its program merely enabled users to lawfully exercise their rights associated with copyrighted works that they had already purchased. Both Macrovision[87] and MGM[88] successfully argued that the 321 Studios product violated the provisions found in the *DMCA*, notwithstanding the potential lawful uses of its product. 321 Studios filed for bankruptcy protection in August 2004, as the company collapsed under the weight of the litigation.[89]

Perhaps the best-known *DMCA* case also involved a dispute over CSS. Since the CCA controls access to the keys necessary to decrypt CSS, it is effectively able to limit the playback of DVDs to specific devices or computer

---

83 See *Macrovision Corp. v. 321 Studios*, 2004 U.S. Dist. LEXIS 8345 [*Macrovision*]. See also *321 Studios v. MGM Studios, Inc*. 307 F. Supp. 2d. 1085 [*MGM*]. See also *Paramount v. Tritton Archive*, <www.eff.org/IP/DMCA/Paramount_v_Tritton/complaint.pdf>.

84 Electronic Frontier Foundation, "Analog Protection System" (Presentation to the Analog Discussion Group, March 2003) [unpublished], <www.eff.org/IP/DMCA/Macrovision_v_321Studios/20030320_Macrovision_APS.pdf>.

85 See *MGM*, above note 83; see also *Order Granting Defendant's Motion for Partial Summary Judgment and Resolving Related Motions* at 1, <www.eff.org/IP/DMCA/MGM_v_321Studios/20040219_Order.pdf>.

86 *Ibid*.

87 Above note 83. See also Electronic Frontier Foundation, "Macrovision c. 321 Studios Archive" <www.eff.org/IP/*DMCA*/Macrovision_v_321Studios/>.

88 Above note 83. See also Electronic Frontier Foundation, "Macrovision c. 321 Studios Archive" <www.eff.org/IP/*DMCA*/MGM_v_321Studios/>.

89 John Borland, "DVD-copying trailblazer shuts its doors" *CNET News.com* (3 August 2004), <http://news.com.com/DVD-copying+trailblazer+shuts+its+doors/2100-1025_3-5295913.html>.

operating systems. When DVDs were first introduced into the consumer marketplace, the CCA declined to make the keys available to those who used the open source Linux operating system. Accordingly, Linux users could purchase DVDs but were unable to play them on their computer systems, affecting both Linux users and Linux's credibility as a competitive mainstream computer operating system.[90]

Jon Johansen, a Norwegian teenager, developed a software program known as DeCSS, short for Decrypt CSS.[91] The program allowed users to decrypt the CSS incorporated into DVDs and thereby access the content. The DeCSS program was posted on the Internet and linked to by "2600," a quarterly hacker magazine. The Motion Picture Association of America (MPAA) filed suit against the magazine and its publisher for linking to the software program, arguing the mere Internet link violated the *DMCA*.[92] The MPAA proved successful in its claim as the 2nd Circuit Court of Appeals rejected arguments that the CSS was not an effective TPM and that DeCSS was merely being used to create a Linux-based DVD player.[93]

In addition to cases upholding restrictions on the lawful use of copyrighted materials, content companies have also used the *DMCA*'s anti-circumvention provisions to restrict competitive third party innovation. For example, Vivendi-Universal's Blizzard Entertainment successfully sued a group of volunteer game enthusiasts who created open source software that allowed owners of Blizzard games to play them over the Internet. The software, created through reverse engineering, used a server called "bnetd," which provided an alternative to Blizzard's own Battle.net servers. Blizzard sought to bar distribution of bnetd, claiming that the software was a circumvention device that violates the *DMCA* and that it was used to permit networked play of Blizzard games.[94]

In September 2004, a federal court in Missouri ruled in favour of Blizzard.[95] In addressing the *DMCA* issues, the court found that the software creators had violated the anti-circumvention provisions both on the

90 **Deborah Durham-Vichr,** "Focus on DeCSS Trial" *Linux World* (27 July 2000), <http://archives.cnn.com/2000/TECH/computing/07/27/decss.trial.p1.idg>.

91 *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d. 294 (SDNY 2000), aff'd 273 F. 3d 429 (2d Cir. 2001). See unofficial decision <www.2600.com/news/112801-files/universal.html>.

92 *Ibid*.

93 *Ibid*.

94 **See Electronic Frontier Foundation, "Blizzard v. BNETD"** <www.eff.org/IP/Emulation/Blizzard_v_bnetd> [*BNETD*].

95 *Davidson & Associates, Inc. v. Internet Gateway*, 334 F.Supp.2d 1164 (E.D. Mo. 1 August 2003).

grounds that they had actually circumvented Blizzard's TPM and because the software program itself constituted trafficking in a circumvention device. The court dismissed the creators' arguments that their conduct was saved by the *DMCA*'s reverse engineering provision.[96] The case is currently under appeal.[97]

The string of cases, from Streambox to DeCSS to Blizzard, illustrates the potential for anti-circumvention provisions to be used as a sword to restrict competition and innovation. While a copyrighted work underlies each of the cases, by extending the scope of the *DMCA* to include the devices that can be used to circumvent a TPM, the United States has provided content holders with a powerful new tool to forestall competition and limit innovation. Moreover, the effect of the anti-circumvention provisions is to effectively replace copyright protection with access controls. This eviscerates fair use rights such as the right to copy portions of work for research or study purposes, since the blunt instrument of technology can be used to prevent all copying, even that which copyright law currently permits. Justice Binnie of the Supreme Court of Canada may have concluded in the *Théberge* case that "once an authorized copy of a work is sold to a member of the public, it is generally for the purchaser, not the author, to determine what happens to it,"[98] but that is plainly no longer the case in the United States under the *DMCA*.

Not only have there been a large number of anti-circumvention copyright-related cases, but in recent years there have also been several attempts to extend the applicability the *DMCA*'s anti-circumvention provisions outside the copyright arena in a direct assault on marketplace competition. The StorageTek case, in which the company obtained an injunction prohibiting Custom Hardware Engineering and Consulting, a maintenance consulting company, from servicing StorageTek's products, provides a perfect illustration.[99]

The StorageTek data storage system, which contains thousands of tapes, typically includes up to twenty-four control units that can hold hundreds of terabytes of data. Custom Hardware tricked the StorageTek security

---

96 *Ibid*. at para. 1185.

97 **Above note 94.**

98 *Théberge v. Galerie d'Art du Petit Champlain Inc*., 2002 SCC 34, <www.lexum.umontreal.ca/cscscc/en/pub/2002/vol2/html/2002scr2_0336.html>, [2002] 2 S.C.R. 336 [*Théberge*] at para. 31.

99 *Storage Tech. Corp. v. Custom Hardware Eng'g* & Consulting, 2004 U.S. Dist. LEXIS 12394 (D. Mass., 2 July 2004). See unofficial version <http://lawgeek.typepad.com/lawgeek/LegalDocs/storagetek*DMCA*.pdf>.

system into activating the proprietary "maintenance code" that activated functions like event logging and a special user interface. With the maintenance code in hand, Custom Hardware was then able to identify the repair functions that needed to be performed.

The court ruled that Custom Hardware's approach violated the *DMCA*'s anti-circumvention provisions, reasoning that the maintenance code was copyrightable material and that it was protected by an access control. Custom Hardware raised antitrust concerns, yet the court dismissed them, concluding that "the defendants cannot avoid an injunction against their illegal conduct by alleging violations of antitrust law on [the] plaintiff's part."[100]

Similar cases have been launched involving printer cartridges and garage door openers. In 2003, Lexmark, a leading computer printer manufacturer, launched a suit against Static Control Components, which provided low cost printer cartridge refills. Lexmark claimed that Static Control violated the *DMCA* by selling its Smartek chips to companies that refill toner cartridges and thereby undercut Lexmark's prices. The chips mimicked the authentication sequence used by Lexmark chips, thereby tricking the printer into accepting an aftermarket cartridge. Lexmark argued that that process "circumvents the technological measure that controls access to the Toner Loading Program and the Printer Engine Program," and asked the court to order the destruction of all Smartek chips.[101]

Lexmark succeeded in obtaining an injunction from a federal district court in Kentucky, which ruled that Lexmark's authentication sequence constituted a "technological measure" that "effectively controls access" to two copyrighted works — the Toner Loading Program and the Printer Engine Program.[102] The authentication sequence, it determined, controlled access because it controls the consumer's ability to make use of these programs. Since Static Control's chips circumvented the authentication sequence, the court reasoned that it violated the *DMCA*'s anti-circumvention provisions.

In an October 2004 decision, however, the 6th Circuit Court of Appeal overturned the injunction on appeal, ruling that the authentication system did not control access to a work and therefore the *DMCA* provision

---

100 *Ibid.* at para. 11.

101 **Declan McCullagh, "Lexmark invokes DMCA in toner suit"** *CNET News.com* (8 January 2003) <http://news.com.com/2100-1023-979791.html>.

102 *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943 at para. 969 (E.D. Ky., 2003).

was inapplicable.[103] The court added that "[n]owhere in its deliberations over the *DMCA* did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected."[104]

In a dissenting opinion, Judge Feikens indicated that had the facts been somewhat different, a *DMCA* violation would have occurred.[105] In particular, he noted that Static Control was unaware of the Toner Loading Program. He concluded that had the company been aware of the program and still sought to circumvent, the outcome of the case might have been different. He supported his conclusion by arguing that consumers did not have the right to refill a printer cartridge. If they used a Smartek chip to do so, he believed that it would constitute an unauthorized access.

In another much-publicized case, Chamberlain Group, a leading garage door opener manufacture, filed suit against Skylink, a small Canadian company that sold remote control devices that interoperated with Chamberlain's products.[106] Chamberlain argued Skylink's remote control device circumvented access controls to a computer program in its garage door opener. Both a district court[107] and the 7th Circuit Court of Appeals[108] dismissed Chamberlain's suit. The company later filed an unsuccessful appeal with the US Supreme Court.[109]

While the record on non-copyright *DMCA* anti-circumvention suits has been mixed, the impact of the cases surely has not. The threat and cost of litigation undoubtedly creates a significant drag on innovation by small and medium-sized businesses since for many companies, the risk, time, and cost of fending off a lawsuit may be too great to proceed with bringing a product to market. Not only does this impede the innovation process, but consumers also face the prospect of reduced competition, higher prices, and service provider lock-in.

---

103 *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 2004 U.S. App. LEXIS 22250 (6th Cir. Ky., 26 October 2004). See unofficial version <http://lawgeek.typepad.com/04a0364p-06.pdf>.

104 *Ibid*. at para. 549.

105 *Ibid*. at para. 553.

106 *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1023, 2003 U.S. Dist. LEXIS 15298 (N.D. Ill., 2003).

107 *Ibid*.

108 *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 2004 U.S. App. LEXIS 18513 (Fed. Cir., 2004).

109 **"Garage Door Maker Seeks Review of DMCA Case,"** *BNA Electronic Commerce and Law Review* (16 February 2005) at 151.

b) Australia

Australia's implementation of the WIPO Internet Treaties has occurred in two phases — first within the *Digital Agenda Act* in 2000, which amended the *Copyright Act* of 1968,[110] and second as part of the *US-Australia Free Trade Agreement* (*AUSFTA*) which was concluded in 2004.[111]

The first set of reforms focused on the distribution of circumventing devices rather than the act of circumvention or the individuals who use circumvention technologies. It prohibited supplying circumvention devices and services whose purpose is to circumvent effective technological protection measures.[112] It is noteworthy that the law did not prohibit use of a circumventing device, only its distribution. A circumventing device is defined as "a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure."[113]

The Act contained an exception that permits circumvention devices and services to be supplied in several circumstances. These include:

> (a) to a person authorised in writing by a body administering an educational institution to make reproductions and communications under the statutory licence in Part VB of the Act;
> (b) for the purpose of making reproductions and communications under that statutory licence;
> (c) of material which is not readily available in a form which is not protected by a technological protection measure.[114]

The *AUSFTA*, a comprehensive free trade agreement, specifically mandated that Australia incorporate additional anti-circumvention legislation into its national law.[115] Article 17.4.7(a) required Australia to change its law by providing for a ban on both the distribution and use of devices for circumventing TPMs.[116] In addition, Article 17.4.7(b) required Australia to adopt

---

110 *Copyright Act 1968* (Cth), <www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/>[*Copyright Act*].

111 *Copyright Amendment (Digital Agenda) Act 2000* No. 110, 2000 (Cth), <www.austlii.edu.au/au/legis/cth/num_act/caaa2000n1102000321/>[*Digital Agenda*].

112 *Australia-United States Free Trade Agreement*, Australia and United States, 1 January 2005, <www.dfat.gov.au/trade/negotiations/us_fta/final-text/>[*AUSTFA*].

113 **Above** note 111 at sch. 1, ss. 4–5.

114 *Ibid*.

115 **Above note 112**.

116 *Ibid*. at Art. 23.4(1).

a definition of a TPM that controls access to a protected work, or protects any copyright.[117] The change is believed to target Australia's practice of parallel importation.[118]

c) European Union

The European Union approach to WIPO Internet treaty implementation is found in *Directive 2001/29/EC*, better known as the *European Copyright Directive* (*EUCD*).[119] The directive entered into force in June 2001 and granted member states eighteen months to implement its provisions within their national law.[120] As of September 2004, eight countries — Belgium, Cyprus, Estonia, Finland, France, Portugal, Spain, and Sweden — had still failed to do so.[121]

Article 6 of the *EUCD* contains anti-circumvention provisions similar to those found in the *DMCA*. Article 6.1 requires that member states provide "adequate legal protection" against the deliberate circumvention of technological measures.[122] This applies regardless of whether such an act infringed any copyright, though a user must know or have reasonable grounds to know they are causing such circumvention. Article 6.2 focuses on circumvention devices, defining any device or service as one that is marketed or primarily designed to circumvent technical measures, or has only limited other commercial purpose.[123] The article bans the manufacture, importation, distribution, sale, rental, or advertisement of circumvention devices or services. Moreover, possession of such devices for commercial purposes is also prohibited, and recital 49 of the *EUCD* grants

---

117 *Ibid*. at Art. 17.4.7(a).

118 Kimberlee Weatherall, "Submission to the Senate Select Committee on the Australia-United States Free Trade Agreement" Intellectual Property Research Institute of Australia (30 April 2004), <www.ipria.org/research/Submission_KWeatherall_SenateSelectCommittee2.pdf>.

119 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] O.J. L. 167/10, <www.ivir.nl/legislation/eu/copyright-directive.doc>, [*EUCD*]. For a critical analysis of the EUCD, see B. Hugenholtz, "Why the Copyright Directive is Unimportant and Possibly Invalid," 11 E.I.P.R. 501.

120 *Ibid*., Art. 13.1.

121 Urs Grasman & Michael Girsberger, "Transposing the Copyright Directive: Legal Protection of Technological Protection Measures in EU-Member States, A Genie Stuck in a Bottle?" in Berkman Publication Series No. 2004-10 (November 2004) at 8, <http://cyber.law.harvard.edu/media/eucd> [*Berkman*].

122 Above note 119 at Art. 6.1.

123 *Ibid*. at Art. 6.2.

member states the right to further ban private possession of circumvention devices.[124]

The *EUCD* does contain one crucial article that seeks to address the issue of copyright balance. Article 6.4 provides that:

> Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law…the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.[125]

The *EUCD* lists several exceptions that are mandatory. These include exceptions in relation to photocopying, copy and archiving activities by educational facilities, broadcaster ephemeral recordings, non-commercial broadcasts, teaching and research, use by disabled individuals, and public safety.[126] Moreover, member states are also permitted to take measures to preserve private copying rights.[127]

Implementation of the *EUCD* varies considerably between member states. For example, in Germany paragraph 95a(2) of the *Copyright Act* limits the coverage of anti-circumvention protection solely to works that are subject to copyright protection. Accordingly, where TPMs are applied to non-copyrightable works, including the non-copyright cases described above and works in the public domain, the anti-circumvention protection does not apply.[128]

Denmark's implementation includes an explanatory text that indicates that only TPMs used to prevent copying are protected. Accordingly, if a TPM seeks to expand protection beyond mere copyright protection it does not enjoy legal protection. For example, encoding DVDs with regional coding would presumably not enjoy protection, an interpretation confirmed by the Danish Ministry of Culture which has opined that it would not be unlawful to circumvent DVD regional encoding for lawfully acquired

---

124 *Ibid*. at Art. 49.
125 *Ibid*. at Art. 6.4.
126 **Above note 121 at 10.**
127 *Ibid*. at 11.
128 *Ibid*. at 13.

DVDs, nor to circumvent a TPM if the sole purpose is to use a lawfully acquired work.[129]

Among implementing member states, Italy has moved the furthest toward applying the *EUCD*'s Article 6.4 to private copying. Its legislation includes the right to make one copy for personal use notwithstanding a TPM, provided that the work is lawfully acquired and the single copy does not prejudice the interests of the rights holder.[130] Other member states have sought to provide users with a positive right of access. For example, Greece provides such a right with the condition that failure to obtain the right leads first to mediation, followed by a legal right of action.[131] Both Austria and the Netherlands have legislation that assumes access for non-infringing material — Austria has said it is "monitoring" the situation, while the Netherlands has included the ability for the Justice Minister to issue decrees on the matter.[132]

The EU experience to date illustrates the significant flexibility in implementing the WIPO Internet treaties. Although on the surface the *EUCD* appears similar to the *DMCA*, at the member state level it is clear that many countries have sought to closely link anti-circumvention legislation with traditional copyright infringement. Moreover, the *EUCD*'s openness to the establishment of TPM exceptions to protect user exceptions represents an important potential compromise designed to preserve the copyright balance.

d) Developing Countries

The majority of countries that have ratified the WIPO Internet Treaties are not developed countries such as the US, Australia, and EU, but rather developing countries from South America, Africa, Eastern Europe, and Asia.[133] Although the many smaller developing countries are not presently significant copyright importing or exporting countries, their ratifications were needed to obtain the minimum number of country ratifications in order for the treaties to take effect.

In 2003, WIPO released a comprehensive review of national implementing legislation. Contrary to some expectations, WIPO's review dem-

---

129 *Ibid*. at 14.
130 *Ibid*. at 23.
131 *Ibid*. at 21.
132 *Ibid*. at 22–3.
133 For a complete list of ratifying countries, see <www.wipo.int/treaties/en/documents/pdf/s-wct.pdf> and <www.wipo.int/treaties/en/documents/pdf/s-wppt.pdf>.

onstrated that many countries had ratified the WIPO Internet Treaties without even including anti-circumvention provisions. Countries that have ratified at least one of the WIPO Internet Treaties but do not have anti-circumvention legislation within their national law include Albania, Argentina, Chile, Croatia, El Salvador, Gabon, Kyrgystan, Latvia, Mali, Mongolia, Panama, the Philippines, Romania, Saint Lucia, and Senegal.[134] It may be possible that some of these countries have allowed for the WIPO Internet treaties to take direct effect within their countries and that they have therefore effectively incorporated the *WCT* and *WPPT*'s anti-circumvention provisions. In such instances, it would be difficult to discern the precise legal rules since the *WCT* and *WPPT* do not contain the specificity typically found in implementing legislation.

Even among those developing countries that have implemented anti-circumvention legislation within their national law, a variety of approaches have been taken, further confirming the flexibility inherent in implementation afforded by the treaties. For example, Peru's law provides that circumvention of a TPM is only unlawful if it occurs for a commercial purpose or results in copyright infringement.[135]

D. TOWARD A CANADIAN WAY ON ANTI-CIRCUMVENTION LEGISLATION

As Canadians consider the anti-circumvention provisions contained in Bill C-60, several lessons learned elsewhere bear repeating. First, anti-circumvention represents an entirely new approach to copyright law. While copyright law seeks to balance creator and user rights by identifying the rights and limitations on rights holders, TPMs, supported by anti-circumvention legislation, creates new layers of protection that do not correlate with traditional copyright law.

As noted above, Justice Binnie stated in *Théberge* that "once an authorized copy of a work is sold to a member of the public, it is generally for the purchaser, not the author, to determine what happens to it."[136] Cases such as *Streambox* serve as an important reminder that this is not always the case, since activity that is lawful under traditional copyright law, may be unlawful under certain anti-circumvention legislation. This change in the law should resonate with the Competition Bureau since it challenges its

134 *WIPO Survey*, above note 58.
135 *Ibid*. at 618.
136 *Théberge*, above note 98 at para. 31.

longstanding position that a hands-off approach to intellectual property is warranted given its characterization of IP as pro-competitive.

Second, there is considerable flexibility in how a country implements its anti-circumvention obligations into national law. While the US *DMCA* is the best-known implementation, the approaches in several European countries, as well as those in the developing world, indicate that a country can seek to maintain the copyright balance, avoid regulating technologies, and foster a pro-competitive marketplace within the WIPO framework.

Third, the US *DMCA* experience illustrates that the fears raised by critics of the US approach have come to fruition. In only seven years, the *DMCA* has become a heavily litigated statute used by rights holders and non-rights holders to restrict innovation, stifle competition, and curtail fair use. This has occurred in large measure due to the US decision to strictly regulate anti-circumvention devices and to downplay the connection between TPM protection and copyright.

1) Bill C-60: A Competition Perspective

Bill C-60 leaves few areas of Canadian copyright law untouched, with new provisions addressing the rights of performers and photographers, the role of Internet service providers, as well as the digital delivery of books and lessons by educators and librarians. As Canadians debate the bill, the provisions that incorporate anti-circumvention legislation into Canadian copyright law are likely to prove to be the most contentious. As addressed elsewhere in this book, those provisions will have a significant impact on freedom of expression and privacy as well as raise concerns about the constitutionality of para-copyrights.

This section focuses more narrowly on the marketplace competition concerns raised by the provisions. The bill begins by defining technological measures as "any technology, device or component that, in the ordinary course of its operation, restricts the doing … of any act that is mentioned in section 3, 15 or 18 or that could constitute an infringement of any applicable moral rights."[137] The Canadian approach interestingly avoids inclusion of the word "effective," choosing instead to focus on technologies that restrict the use of works subject to copyright "in the ordinary course" of their operation. This may prove to be a distinction without a difference, however, since courts may use a similar analysis to determine the con-

137 Above note 15 at s. 1(2).

tours of "ordinary course" as they would use to establish an effectiveness standard.

Bill C-60 includes three anti-circumvention provisions. The first provision establishes the general prohibition on circumventing a technological measure:

> 34.02 (1) An owner of copyright in a work, a performer's performance fixed in a sound recording or a sound recording and a holder of moral rights in respect of a work or such a performer's performance are, subject to this Act, entitled to all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right against a person who, without the consent of the copyright owner or moral rights holder, circumvents, removes or in any way renders ineffective a technological measure protecting any material form of the work, the performer's performance or the sound recording for the purpose of an act that is an infringement of the copyright in it or the moral rights in respect of it or for the purpose of making a copy referred to in subsection 80(1).[138]

This provision accomplishes several things. First, it establishes who is entitled to exercise the new right against anti-circumvention, namely all copyright holders including owners and performers. Second, it grants those copyright holders the full scope of potential remedies, including injunctions and damages, in the event of infringement. Third, and most important, it renders it an infringement to break a technological measure for the purpose of an act that constitutes copyright infringement. It is important to note that this provision does not make circumvention of a technological measure an infringement *per se*; an infringement will only occur where the purpose of the circumvention is to infringe copyright.[139] This limitation suggests that circumvention for the purposes of fair dealing would be lawful under Canadian law. Moreover, this provision only targets the act of circumvention; Bill C-60 does not establish legal limitations on devices that can be used to circumvent technological measures.

The second provision is somewhat more cryptic and difficult to interpret:

---

138 *Ibid*. at s. 34.02(1).

139 A notable exception is that circumvention for the purposes of making a private copy (*i.e.*, breaking anti-copying technology on a music CD to make a private copy).

> (2) An owner of copyright or a holder of moral rights referred to in subsection (1) has the same remedies against a person who offers or provides a service to circumvent, remove or render ineffective a technological measure protecting a material form of the work, the performer's performance or the sound recording and knows or ought to know that providing the service will result in an infringement of the copyright or moral rights.[140]

On one reading, this provision merely establishes similar limitations on persons who provide a specific service to circumvent a technological measure. The crucial wording is that the service provider "knows or ought to know that providing the service will result in an infringement." Since mere circumvention is not an infringement under Bill C-60 (infringement requires circumvention with an infringing purpose), it may be that a service provider will only be caught under this provision where they directly know the party for whom they are circumventing the technological measure and they know (or ought to know) that the circumvention is for an infringing purpose. Under this interpretation, merely providing a circumvention service (or distributing software or other devices capable of circumvention) would not be caught since the service provider would not know with certainty that the service will be used for an infringing purpose.

While this may have been the drafters' intent, the provision could be interpreted in a broader manner, capturing not only the actions described above, but also those service providers who "ought to know" that their services will be used for an infringing purpose. Under this interpretation, distributing software that is frequently used for infringing purposes might be caught within the provision.

The third provision is fairly straightforward, as it merely establishes legal limitations on what can be done with work subject to copyright that has had a technological measure removed. This covers activities that arise after the copyright work has been circumvented, and restricts the sale, rental, trade, or distribution of the work. The specific provision states that:

> (3) If a technological measure protecting a material form of a work, a performer's performance or a sound recording referred to in subsection (1) is removed or rendered ineffective in a manner that does not give rise to the remedies under that subsection, the owner of copyright or holder of moral rights nevertheless has those remedies

140 Above note 15 at s. 34.02(2).

against a person who knows or ought to know that the measure has been removed or rendered ineffective and, without the owner's or holder's consent, does any of the following acts with respect to the material form in question:

(*a*) sells it or rents it out;
(*b*) distributes it to such an extent as to prejudicially affect the owner of the copyright;
(*c*) by way of trade, distributes it, exposes or offers it for sale or rental or exhibits it in public; or
(*d*) imports it into Canada for the purpose of doing anything referred to in any of paragraphs (*a*) to (*c*).[141]

2) Bill C-60's Anti-circumvention Provisions: The Positives

a) Flexible Implementation of the WIPO Internet Treaties

The Canadian approach to anti-circumvention as contained in Bill C-60 has several positive elements. First, the government has clearly recognized the flexibility inherent in the WIPO Internet Treaties. Although it may face criticism from some US-linked rights holder groups for deviating from the *DMCA* model, the review of *WIPO Internet Treaty* implementations in other jurisdictions illustrated that there is more than one model that can be used to become "WIPO compliant."

b) Direct Connection between Anti-Circumvention and Copyright Infringement

The federal government has appropriately ensured that the anti-circumvention provisions feature a direct connection to traditional copyright infringement by limiting the scope of a circumvention offence to users who circumvent for the purpose of committing copyright infringement. Copyright, competition, and constitutional law analysis all support this approach.

From a copyright perspective, failure to link circumvention with copyright would alter the balance between creators and users as it would invariably lead to an expansion of the rights attached to copyright. The US experience provides ample evidence in this regard as courts have openly acknowledged that copyright compliant activity or devices are no longer sufficient, since anti-circumvention renders illegal activity that is legal

141 *Ibid*. at s. 34.02(3).

under traditional copyright norms. Such an approach would run directly counter to recent Supreme Court of Canada pronouncements on Canadian copyright law that have emphasized the need for an appropriate balance to encourage creativity and innovation in the long-term interests of society as a whole.

The impact of non-linkage would extend the provisions well-beyond works typically associated with copyright. As the *StorageTek*, *Lexmark*, and *Chamberlain* cases illustrate, provisions that open the door to using anti-circumvention provisions beyond traditional copyright norms risk generating uncertainty in the marketplace and the potential for lawsuits that restrain competition and limit consumer choice. This issue has not escaped the attention of many other countries, including Germany and Denmark, which have implemented laws that link anti-circumvention legislation to copyright infringement.

Beyond the copyright and competition policy reasons for a direct connection between anti-circumvention and copyright, as Jeremy deBeer persuasively argues in Chapter 4, there is a strong constitutional law reason for doing so. The federal government's jurisdiction over copyright is derived from section 91(23) of the *Constitution Act, 1867*.[142] Anti-circumvention legislation that is closely connected to copyright principles would be less susceptible to constitutional challenge.

c) No Legislation Against Devices

Canada has rightly decided to not legislate against anti-circumvention devices. Regulating technology is always a slippery slope — the experience in the US illustrates that banning the distribution or possession of devices leads to significant innovation disincentives since small and medium-sized businesses, scientists, venture capitalists, and other parties that facilitate innovation are likely to abandon cutting edge research and projects for fear of potential legal liability. Those fears have been made manifest in security research in the United States, where the impact of lawsuit threats against scientists several years ago is still being felt today.

The challenge of discerning between "appropriate" and "inappropriate" devices is very difficult and likely to result in overbroad coverage that criminalizes devices with multiple legitimate uses. That is certainly the case in the United States, where the DeCSS case demonstrates how a

142 *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, s. 91(23), reprinted in R.S.C. 1985, App. II, No. 5.

software program with a legitimate use (playing a store-bought DVD on a computer with the Linux operating system) can be rendered illegal.

Bill C-60 is on safe ground here since there is no legal requirement within the WIPO Internet Treaties to incorporate provisions on devices that can be used for circumvention purposes. Rather, a framework that covers the act of circumvention as it relates to copyright infringement provides rights holders with the adequate protection mandated by the treaties.

3) Bill C-60's Anti-circumvention Provisions: Room for Improvement

a) *Competition Act* Amendments

Notwithstanding Bill C-60's positives, from a competition law perspective there remains some room for improvement. First, alongside the amendments to the *Copyright Act* prescribed by the Bill, the *Competition Act* should be amended to ensure that the Competition Bureau is not restricted in its ability to bring actions against abusive behaviour stemming from the application of an anti-circumvention right. Although Wetston and Addy have argued that section 79(5) of the *Competition Act* does not grant blanket immunity to intellectual property rights holders, both the Competition Tribunal and the Bureau's own *IPEGs* evidence a strong reluctance to interfere with the application of an intellectual property right. Accordingly, a statutory exception would be needed to ensure that section 79(5), which precludes the Bureau from taking action against abusive behaviour that arises directly from the exercise of a right under the *Copyright Act*, would not apply to anti-circumvention provisions.

The experience with TPMs in other jurisdictions provides a compelling case for a fully engaged, active Competition Bureau as the technology is inserted into ever-more products and services. In fact, while the WIPO Internet treaties provide protection for TPMs, it is increasingly evident that the marketplace may require protection from TPMs. As noted at the beginning of this essay, in 1992 the Bureau acted against computer maker DEC over tied selling activities that bear a striking resemblance to conduct that is now protected in the United States by anti-circumvention legislation. If the Bureau is to maintain a vital role in fostering innovation and a competitive marketplace, it cannot face statutory restrictions to act against anticompetitive, harmful market conduct.

An active and unrestricted Competition Bureau is particularly important in the Canadian context since Canada does not have a doctrine of copyright misuse. Copyright misuse is an equitable defence in infringe-

ment cases where the plaintiff's actions have expanded their copyright past the statutory limits (i.e., anticompetitive acts).[143] Canadian courts have not directly adopted the doctrine of copyright misuse from US courts.[144] In the United States, the doctrine was "created to address situations in which the owner of an intellectual property right used his or her legal monopoly to create such an asymmetry in the balance of rights that courts refused to enforce the normal intellectual property rights."[145]

The 1990 4th Circuit Court of Appeals decision in *Lasercomb America Inc. v. Reynolds* provides a good illustration of the doctrine's application.[146] The plaintiff, Lasercomb, developed and licensed software used to form steel dies for the paper industry. It licensed four copies of the software to Reynolds, who circumvented the protective devices and made an additional three unlicensed copies.

While there was no dispute that Reynolds had infringed copyright, it argued that Lasercomb was barred from recovery for the infringement because it included a clause in its software license that prevented the licensee from developing competing software for 100 years. The court agreed, ruling that "a misuse of copyright defense is inherent in the law of copyright just as misuse of patent defense is inherent in patent law."[147] In fact, the court's analysis indicated that copyright owners were prohibited from using their grant of a monopoly in a particular work to obtain a monopoly in a subject matter outside the rights associated with the copyright. This analysis, alongside similar decisions from the 9th Circuit Court of Appeals in *Practice Management Information Corp. v. American Medical Association*[148] and the 5th Circuit Court of Appeals in *Alcatel USA, Inc. v. DGI Technologies, Inc.*,[149] affirmed the doctrine of copyright misuse in US law and has led some experts to advocate for the application of copyright misuse to

143 See Neal Hartzog, "Gaining Momentum: A Review of Recent Developments Surrounding The Expansion of the Copyright Misuse Doctrine and Analysis of the Doctrine In Its Current Form"(2004) 10 Mich. Telecomm. Tech. L. Rev. 373, <www.mttlr.org/volten/Hartzon.pdf>.

144 A search for 'copyright misuse' in LexisNexus and QuickLaw does not return any relevant results. Similarly, there is little discussion of copyright misuse in Canadian secondary sources.

145 James A.D. White, "Misuse or Fair Use: That is the Software Copyright Question" (1997) 12 Berkeley Tech L.J. 251, 265–66.

146 *Lasercomb America, Inc. v. Reynolds*, 911 F.2d 970 (4th Cir. 1990).

147 *Ibid*.

148 *Practice Management Information Corporation v. The American Medical Association*, 121 F.3d 516 (9th Cir. 1995).

149 *Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772 (5th Cir. 1999).

anti-circumvention as part of a development of a principle of anti-circumvention misuse.[150]

There is scant jurisprudence supporting the proposition that something analogous to copyright misuse exists in Canada. It has been suggested that the Supreme Court implicitly recognized copyright misuse in the 1940 case of *Massie & Renwick Ltd. v. Underwriters' Survey Bureau Ltd.*[151] The Supreme Court commented that a plaintiff would face a barrier in bringing a copyright infringement action if their title in the copyright was the result of a criminal conspiracy under the *Criminal Code* and the *Combines Investigation Act*. This idea, however, has not been put into practice in the sixty-five years following the decision. More recently, the Federal Court of Appeal stated that it had "serious doubts" that the anti-competitive actions of the plaintiff could provide a defence against copyright infringement.[152]

In fact, while Canadian courts have yet to adopt the doctrine of copyright misuse, the principles are effectively found in section 32 of the *Competition Act*. If the Competition Bureau is precluded from applying the statute — either due to the inclusion of new para-copyrights in the *Copyright Act* or by virtue of the section 32(3) limitation on variants from international intellectual property treaties — there will be little to prevent owners of intellectual property right from using their legal monopoly to create additional monopolies or to engage in anti-competitive behaviour. Without a legal principle to mitigate against abuse, Canada would be open to the prospect for even greater abuse of anti-circumvention provisions than that found in the United States.

b) User Right to Circumvent for Lawful Purposes

Bill C-60 should be amended to include a positive user right to circumvent a technological measure for lawful purposes. This proposal is closely linked to Professor Kerr's proposal for a positive right to circumvent to protect personal privacy, yet would extend the principle to a positive right for any lawful purpose. Although the Bill currently links circumvention to copyright infringement, the language contained in the Bill does not rise

---

150 **Above note 13.**

151 *Massie & Renwick v. Underwriters' Survey Bureau Ltd.* [1940] S.C.R. 218 [*Massie*], cited in Sunny Handa, "Reverse Engineering Computer Programs Under Canadian Copyright Law"(1995) 40 McGill L.J. 621 at 651.

152 *Bell Canada v. Intra Canada Telecommunications* (1982), 70 C.P.R. (2d) 252 (the Court allowed the claims to go forward, but there doesn't appear to be any subsequent litigation on the matter).

to the level of a user right as envisioned by the Canadian Supreme Court. That court recognized the need for copyright balance to achieve optimal innovation incentives in *Théberge*, as Justice Binnie spoke of the danger of over-compensating creators by establishing copyright protection that is too strong at the expense of the public interest. In the United States, there is no longer any pretense of a balance as courts openly acknowledge that their analysis of anti-circumvention legislation need not factor in fundamental copyright norms.

Granting users a positive right of circumvention would enable policy makers to obtain the benefits associated with TPMs (protection against large scale digital commercial piracy), while ensuring that individual users do not lose their basic user rights in the process. The *EUCD* has opened the door to such an approach, requiring member states to ensure that copyright exceptions are not lost in the rush to protect TPMs. Italy provides a good starting point for discussion as it implicitly distinguishes between personal copying and commercial infringement by including the right to make one copy for personal use notwithstanding a TPM, provided that the work is lawfully acquired and the single copy does not prejudice the interests of the rights holder.

Although the WIPO Internet Treaties represent the culmination of rights holder efforts to obtain legal protection for TPMs, the experience over the past decade suggests that consumers and the general public need protection from TPMs. This is particularly true for TPMs backed by anti-circumvention legislation, which has been consistently used to threaten individuals and businesses with litigation, segment markets, curtail innovation, and limit consumer choice. The creation of a user right to circumvent for lawful purposes would restore much needed balance to the legal rules associated with TPMs.

c) Clarification of Bill C-60 Service Provider Provision

Bill C-60's anti-circumvention service provider provision must be clarified to assure the software, security, and research communities that the provision will not be applied to technology or general service providers, but rather restricted solely to single instances of service provider circumvention with knowledge that the circumvention will result in an infringement. The current language suffers from significant uncertainty, which holds the potential to generate a chill in innovative research or product development.

E. CONCLUSION

The Competition Bureau has embraced the notion that intellectual property rights are pro-competitive for nearly two decades. That view is largely premised on copyright (and other forms of IP) as a balance to encourage innovation through economic rewards for creators and innovators, while guaranteeing access under appropriate circumstances to better distribute knowledge and contribute to future innovation. The anti-circumvention world of copyright marks a dramatic shift as it tilts the balance towards rights holders and, in doing so, risks turning the exercise of copyrights into anti-competitive behaviour.

The Canadian approach to anti-circumvention has the potential to serve as a model for many other countries around the world. The link to copyright infringement and the presumed exclusion of legislating against devices is a welcome change from a US approach that has repeatedly resulted in lawsuits and chilled innovation. While the Canadian bill is better than most, there remains room for improvement. The most urgent amendments include explicit protection for the Competition Bureau to act against abusive conduct arising from the exercise of a technological measure, the establishment of a positive user right to circumvent in appropriate circumstances, and clarification of the meaning and effect of Bill C-60's service provider provision.

Competition Commissioner Sheridan Scott's vision of the long-term impact of the Internet and technology is certainly accurate — the Internet does indeed have the potential to transform business and society. There is no guarantee that this will happen, however. If we fail to adopt pro-competitive policies that encourage innovation and competition, the Internet may devolve into a medium for the few, rather than the many. The challenge, indeed the obligation, is to identify a Canadian way that allows the country to comply with international standards while simultaneously prioritizing the national interest.