ANTI-CIRCUMVENTION TECHNOLOGY LEGISLATION IN CANADA: DRAFTING A NEW LAW IN THE WAKE OF THE DMCA

By:
Natanya Garcia

A thesis submitted to the Faculty of Graduate Studied and Research,
in partial fulfillment of the requirements of the degree of:

Masters of Laws (L.L.M.)

Institute of Comparative Law
McGill University
Montreal, Quebec
Canada

September 2003

ACKNOWLEDGEMENT

My heartfelt appreciation and gratitude goes to Doctor Sunny Handa for his advice, insights and wit during the preparation of this thesis. His classes gave me impetus to begin this journey and his guidance helped me complete it.

I would also like to thank Karen Devine for the hard work she did in translating my Abstract into French.

As always, I could not have done this without my family; my papa who always believed I could do great things and my mom who is always so proud of me, and of course my Lolo, who has and always will be my wellspring of inspiration.

All this would not have been possible without my source of strength, the Lord God who helped me through difficult times when the end seemed very far away.

Last, this thesis is dedicated to Geoff, my knight in shining armour.

Abstract

In becoming a signatory to the World Intellectual Property Organization (WIPO) Treaties, Canada has undertaken the obligation to provide protection against the circumvention of technological measures designed to protect copyright works. While on its face the obligation appears simple, in reality it brings about an intersection of policy, law and technology; a complex situation with far reaching repercussions.

The U.S., a co-signatory to the WIPO Treaties, responded to this tension by enacting the *Digital Milennium Copyright Act* (DMCA), which heavily regulated circumvention technology and garnered wide-spread criticism. Critics labeled the law as unpredictable and overbroad legislation, which has chilled free speech, violated fair use, stifled research and study and encouraged monopolies by eliminating competition.

Drawing largely on the U.S. experience, this thesis aims to suggest a possible route for Canada to take when fulfilling its own obligations under the WIPO. It will begin with a review of the relevant provisions of the Treaties to determine the extent of Canada's obligation. It will then examine Canada's proposal papers and the responses of its citizens to the questioned posed regarding future anti-circumvention legislation. It will also examine the DMCA in detail and attempt to distil its flaws. Finally, it will investigate the extent of the need for new anti-circumvention legislation in Canada by examining Canada's existing laws dealing with the protection of technology measures.

Such process will provide evidence that Canada has, to a large extent, complied with its obligations under the WIPO while maintaining the delicate balance between the stakeholders of copyright law. Thus while new anti-circumvention legislation may still be in order, Canada has the latitude to craft a law that fully recognizes the rights of all stakeholders in the copyright equation and is consistent with its own copyright policies.

Résumé

En devenant un signataire des traités du World Intellectual Property Organization (WIPO, Organisation Mondiale de la Proprieté Intellectuelle), le Canada s'est engagé à assumer l'obligation de fournir une protection contre la mise en échec des mesures technologiques conçues pour protéger les oeuvres aux droits d'auteur. Malgré l'apparence simple de cette obligation, tout ceci entraine en réalité une intéressante intersection de politique, loi et technologie, menant à une situation complexe pleine de répercussions.

Les Etats-Unis, co-signataire des traités du WIPO, ont répondu à cette tension en décrétant le Digital Milennium Copyright Act (DMCA, Loi des Droits d'Auteur du Millénaire Numérique). Cette loi régule très lourdement la technologie de détournement et a obtenu par conséquent d'énormes critiques. Les critiques ont designé cette loi comme étant imprévisible et trop générale au niveau de sa législation, ce qui a pour conséquence de refroidir la liberté d'expression, d'abuser de l'usage juste, d'étouffer la recherche et les études, et d'encourager les monopoles en éliminant la compétition.

Influencée largement par l'expérience des Etats-Unis, cette thèse a pour but de suggérer une voie que le Canada pourrait prendre pour remplir ses obligations envers la WIPO. Elle commencera par la revue des dispositions des traités afin de déterminer l'étendue des obligations du Canada. Elle examinera ensuite les propositions du Canada et les réponses de ses citoyens quant aux futures législations anti-détournement. Elle examinera aussi la DMCA en détail et tentera d'en trouver les failles. Finalement, elle étudiera l'étendue du besoin de nouvelles lois anti-détournement en examinant les lois Canadiennes existantes concernant la protection des mesures technologiques.

Ce processus fournira l'évidence que le Canada a, en grande partie, rempli ses obligations envers la WIPO en maintenant un équilibre délicat entre les dépositaires des lois de droits d'auteur. Ceci étant, malgré le fait que de nouvelles lois anti-détournement soient peut-être encore requises, le Canada dispose de suffisamment de latitude pour créér une loi qui reconnaît pleinement les droits de tous les dépositaires dans l'équation des droits d'auteurs, et qui reste consistante avec les principes propres au Canada sur les droits d'auteurs.

I Introduction

"Copyright is a work in progress."[1]

As the human mind continues to invent new communication and information technologies, copyright too must continually reinvent itself or risk becoming obsolete. Each leap in technology, from the printing press to the photocopying machine to the desktop computer has had an effect on copyright, requiring a corresponding update in legislation to assure that copyright laws remained relevant. Digital technology and the internet is the newest challenge facing copyright law, and it presents a difficult problem. By allowing instantaneous transfer and dissemination of information, the internet has enabled the user to make copyrighted works available to anyone around the globe with the proverbial click of a button.

In 1997, Canada finally addressed this growing problem when it embarked on a process to change existing law and bring the *Copyright Act* into the 21st century. In its policy of "review requirement"[2] under the *Copyright Act* and partly in recognition of the "increasing impact of the Internet and other digital technological developments,"[3] a full report on the provisions and operation of the entire *Copyright Act* was set out to be tabled by the Minister of Industry by September 2002.[4] In December 1997, the Canadian government also signed two new international treaties, called the "WIPO[5] Treaties," which addressed the digital network environment, including the obligation to "prevent the circumvention of copyright protection."

---

1 *A Framework for Copyright Reform* (2001), online: Government of Canada <http://strategis.ic.gc.ca/SSG/rp01101e.html> (date accessed: 3 June 2002) [hereinafter Framework].
2 *Copyright Act of Canada*, R.S.C. 1985 (4th Supp.) § 92 [hereinafter *Copyright Act*].
Subsection 92(1) of the *Copyright Act* stipulates that:

> "Within five years after the coming into force of this section, the Minister [of Industry] shall cause to be laid before both Houses of Parliament a report on the provisions and operation of this Act, including any recommendations for amendments to this Act."

Section 92 of the Act came into force in 1997 when the Act was last amended by Parliament (Bill C-32).
3 Framework, *supra* note 1.
4 *Ibid.*
5 World Intellectual Property Organization [hereinafter WIPO].

In response to their obligations to the WIPO and Section 92 of the *Copyright Act*, the Canadian Government launched a document called *A Framework of Copyright Reform*,[6] in 2001. The Framework outlined the copyright reform process the government (through Industry Canada and Heritage Canada) would undertake to modernize the *Copyright Act*. The Framework's purpose was to inform Canadians about the objectives of the reform and outline a number of substantive issues in need of consideration through the reform process.

As a first step in the copyright reform process, the government released consultation papers for public comment, one of which, the *Consultation Paper on Digital Copyright Issues*,[7] dealt directly with Canada's obligation under the WIPO regarding circumvention technology.[8]

The paper addressed the delicate balance between protecting the creator while allowing the dissemination of information. It recognized the importance of fair dealing as a valid exception to copyright law and the fair dealing exemptions under the *Copyright Act* would be affected by future anti-circumvention legislation. It also took into account how the WIPO obligations had been enacted in other countries and its effects on their copyright regime. Finally, the government solicited submissions regarding possible amendments to the *Copyright Act* with respect to the issues described in the Consultation Paper, submissions that would allow it to "establish a legal framework which, on the one hand, covers virtually all activities that undermine the use of technological measures, but at the same time continues to reflect the policy balance currently set out in the *Act*."

In October 2002, Industry Canada concluded its hearings and submitted its report entitled "*Supporting Culture and Innovation: Report on the Provisions and Operation of the Copyright Act*." The report has since been referred to the Standing Committee on

---

6 Framework, *supra* note 1.
7 Intellectual Property Policy Directorate, *Consultation on Digital Copyright Issues* (2001), online: Industry Canada <http://www.museums.ca/copyright2001/cdnheritagepaper.pdf> (date accessed 5 June 2002). [hereinafter Consultation Paper].
8 *Ibid* at section 4.2.

Canadian Heritage. This committee is set to report to Parliament within a year after the report of the Minister so Parliament may in turn draft the final amendments to the law.[9]

On the other side of the border, the U.S. has enacted its own aggressive implementation of the WIPO, an act called the *Digital Millennium Copyright Act*[10] (the DMCA). Since then pressure has been mounting, as "there are many in the U.S. who have been pushing other countries (including Canada) to enact DMCA-like statues.[11]

Canada's task now lies in standing firm against these pressures, looking to the DMCA yet maintaining its own identity when drafting its legislation. Canada's copyright legislation has always emphasized the principle of balance; it is imperative therefore that Canada's copyright reform process "respect the underlying principle of balance between the protection provided to the creators of original content and the guarantee of reasonable access by the public that is embodied its *Copyright Act*."[12]

In light of this objective, parliament must address several issues. First, it must firmly establish the identity of Canadian copyright. Unlike the U.S., which has firmly established that its public policy behind copyright protection is primarily economic gain,[13] there is no corresponding underlying theory behind Canadian Copyright law. Aware of such pressing need, the Framework has finally addressed this issue at length. However, given that this is the first time such policies have been laid down, lawmakers must examine these policies carefully and keep them firmly in mind and at hand when drafting the new law.

---

9 Online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01106e.html> (date accessed: 15 June 2002).
10 Title 17, United States Code, Section 1201(a)(1)(A) (1998) [hereinafter DMCA].
11 S.Bonisteel, "Canada Tackles Copyright Laws For Digital Age" (2001), online: Newsbytes <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=167203> (date accessed: 10 November 2002) [hereinafter "Canada Tackles"].
12 Submission from Canadian Library Association, received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002). [hereinafter CLA].
13 Discussed *infra*, note 237 and accompanying text.

Second, parliament must take a definitive stance on the issue of reverse engineering. In *Sega vs. Accolade*, the U.S. Supreme Court explicitly stated "reverse engineering software for the sole purpose of creating a compatible package is an acceptable use" under the "fair use" doctrine.[14] There has been no corresponding declaration by the Canadian Supreme Court. Consequently, before the government implements a law that effectively "outlaws reverse engineering,"[15] it should first determine its existing policy regarding the matter.

Third, in creating new legislation parliament must continue to recognize the differences between "fair use" in the U.S. and "fair dealing" in Canada. Since the laws of fair dealing which protect the non-commercial use of the copyrighted work have been less successfully litigated in Canadian courts,[16] a law as stringent as the DMCA may render fair dealing obsolete in Canada.

Fourth, parliament should take into account how anti-circumvention legislation has affected other countries, most specifically the U.S. The chaos that has resulted from the passing of the DMCA and the chilling effect on research, education and speech should be a warning to legislators, a guide on "what not to do."[17]

Finally, parliament must examine all existing legislation and jurisprudence in Canada to determine the scope of the new legislation. There is the possibility that taken together, the laws in Canada may already be sufficient to fulfill Canada's obligations under the WIPO. Parliament's duty would then be to fill any "gaps" in the law or to incorporate existing law into any future anti-circumvention legislation.

---

14 *Sega Enterprises* v. *Accolade Inc.*, 977 F.2d 1510 (1992) [hereinafter *Sega*].
15 See "Digital Copyright Court Cases" (2001), online: <http://www.acm.org/usacm/copyright/dmca.htm> (date accessed 06 January 2003) [hereinafter "Digital Copyright Court Cases"].
16 Only in one case was "fair dealing" argued successfully. See *Allen* v. *Toronto Star* (1997), 78 CPR 3d 115 [hereinafter *Allen*].
17 M. Geist, "Canada Tackles Copyright for the Digital Age," (2001) online: <http://aix1.uottawa.ca/~geist/main.html> (date accessed: 15 October 2002). "The *DMCA* is not a workable sort of approach. The reality is that, for just about all of these kinds of technologies, there are going to be infringing and non-infringing uses, and doesn't really provide an effective means of determining when it's appropriate and when it isn't."

There is little doubt that Parliament will soon enact new amendments to Canada's copyright laws and that these laws will heavily influence the future of Canadian copyright in the digital age. The only question that remains is what type of laws they will be.

1. Definition of Terms

WPPT Treaty and the WCT Treaty – Two recent treaties drafted by the WIPO to which Canada is a signatory. The *Copyright Treaty* (WCT) and the *WIPO Performances and Phonograms Treaty* (WPPT) contain basic rules updating the international protection of copyright and related rights to the Internet age.[18]

DMCA - Short for the *Digital Millennium Copyright Act*, an act of Congress that was signed into law on October 28th 1998, by President Clinton. DMCA's purpose is to update U.S. copyright laws for the digital age.[19]

The Framework for Copyright Reform and the Consultation Paper on Digital Copyright Issues - Two documents which outline the process of copyright reform undertaken by the Department of Industry and the Canadian Heritage in making changes to the Canadian *Copyright Act* of 1924. Its purpose is to inform Canadians about the objectives, process, underlying and substantive issues which Canadian needs to consider during the reform process.[20]

Encryption/Decryption - Encryption is the process of transforming a message (called plaintext) into another message (called ciphertext) using a mathematical function and a special encryption password, called a key. Most encryption systems use the same key for both encryption and decryption, which is the process of converting the encrypted message back into plaintext.[21]

---

18 "About WIPO," online: WIPO <http://www.wipo.org/about-wipo/en/> (date accessed: 12 March 2003) [hereinafter "About WIPO"].
19 *DMCA*, online: <http://www.webopedia.com/TERM/D/DMCA.html> (date accessed: 02 April 2003).
20 Framework, *supra* note 1.
21 S. Garfinkel & G. Spafford, *Practical Unix Security* (Sabstopol, California: O'Reilly & Associates, 1991) at 359.

Reverse Engineering- The process of analysing an existing system to identify its components and their interrelationships and create representations of the system in another form or at a higher level of abstraction. Reverse engineering is usually undertaken in order to redesign the system for better maintainability or to produce a copy of a system without access to the design from which it was originally produced.[22]

2. Limits of the Study

Under the WIPO Treaties Canada committed to make various changes to the *Copyright Act,* touching on a variety of subjects such as Intermediary Liability.[23] This thesis confines its scope to Canada's treaty obligations concerning encryption technology, found under Sections 11 and 18 of the WIPO Treaties of 1996. In addition, while this paper may refer to other foreign legislation, it will concentrate mostly on analysing the DMCA since the DMCA law will most likely have the biggest impact on Canadian legislation than that of any other country.

22 Online: Dictionary.com <http://dictionary.reference.com/search?q=reverse%20engineering> (date accessed: 22 September 2002).
23 Consultation Paper on Digital Copyright Issues, *supra* note 7.

II The Law: The World Intellectual Property Organization Treaty

A. The Birth of the WIPO

The roots of the WIPO go back to Vienna, 1873. That year, the need for international protection of intellectual property became evident when foreign exhibitors refused to attend the International Exhibition of Inventions because they were afraid their ideas would be stolen and exploited commercially in other countries.[24]

These pressures and others like it eventually lead to the birth of the *Paris Convention for the Protection of Industrial Property*[25] in 1883, the first major international treaty designed to help the people of one country obtain protection in other countries for their intellectual creations in the form of industrial property rights such as trademarks, patents and industrial designs. The *Paris Convention* entered into force in 1884 with 14 member States, which set up an International Bureau to carry out administrative tasks, such as organizing meetings of the member States.[26]

In 1886, copyright entered the international arena with the *Berne Convention for the Protection of Literary and Artistic Works*.[27] The aim of this Convention was to help nationals of its member States obtain international protection of their right to control, and receive payment for, the use of their creative works such as novels, songs and paintings.[28] Like the *Paris Convention*, the *Berne Convention* set up an International Bureau to carry out administrative tasks. In 1893, these two small bureaus united to form an international organization called the United International Bureaus for the Protection of Intellectual Property (BIRPI).[29] Based in Berne, Switzerland, with a staff of seven, this small

24 "About WIPO", *supra* note 18.
25 U.N.T.S. No. 11851, vol. 828, pp. 305-388, as revised at Brussels on 14 December 1900, at Washington on 2 June 1911, at the Hague on 6 November 1925, at London on 2 June 1934, at Lisbon on 31 October 1958, and at Stockholm on 14 July 1967.
26 *Ibid.*
27 Paris Act of 24 July 1971, as amended on 28 September 1979, Berne Union, 9 September 1886, 9 September 1886, 828 U.N.T.S. 221, online: <http://www.law.cornell.edu/treaties/berne/overview.html> (date accessed: 2 April 2003) [hereinafter *Berne Convention*].
28 *Ibid.*
29 Online: <http://www.1upinfo.com/encyclopedia/W/WrldInt.html> (date accessed: 19 April 2003).

organization was the predecessor of the World Intellectual Property Organization of today - a dynamic entity with 179 member States, a staff that now numbers some 859, from 86 countries around the world, and with a mission and a mandate that are constantly growing.[30]

As the importance of intellectual property grew, the structure and form of the Organization changed as well. In 1960, BIRPI moved from Berne to Geneva to be closer to the United Nations and other international organizations in that city. A decade after the Convention Establishing the World Intellectual Property Organization came into force, BIRPI became WIPO, undergoing structural and administrative reforms and acquiring a secretariat answerable to the member States.[31]

In 1974, WIPO became a specialized agency of the United Nations system of organizations, with a mandate to administer intellectual property matters recognized by the member States of the UN.[32] WIPO expanded its role and further demonstrated the importance of intellectual property rights in the management of globalized trade in 1996 by entering into a cooperation agreement with the World Trade Organization (WTO). The impetus that led to the *Paris* and *Berne Conventions* - the desire to promote creativity by protecting the works of the mind - has continued to power the work of the Organization, and its predecessor, for some 120 years. However, the scope of the protection and the services provided have developed and expanded radically during that time.

While the cornerstones of WIPO's treaty system remain the *Paris* and *Berne Conventions*, subsequent treaties[33] have widened and deepened the protection they offer,

---

30 *Ibid.*
31 *Ibid.*
32 *Convention Establishing the World Intellectual Property Organization*, Stockholm on 14 July 1967 (as amended on 28 September 1979), online: <http://www.wipo.int/clea/docs/en/wo/wo029en.htm> (date accessed: 24 April 2003).
33 See *International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations*, October 26, 1961, 496 U.N.T.S. 43, online: <http://www.wipo.int/clea/docs/en/wo/wo024en.htm> (date accessed: 18 March 2003); See also *Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite*, May 21, 1974, Vienna Union, online: <http://www.wipo.int/clea/docs/en/wo/wo025en.htm> (date accessed: 18 March 2003); *Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms*, Geneva October 29, 1971, Phonograms Convention, Geneva, 197, online: <http://www.wipo.int/clea/docs/en/wo/wo023en.htm> (date accessed: 18 March 2003).

and have encompassed technological change and new areas of interest and concern. With the dramatic rise in Internet use, especially for e-commerce and information and knowledge exchange, the WIPO recognized that the intellectual property system had become crucial for the orderly development of a digital society. They also recognized that the Internet posed many opportunities as well as complex challenges for the intellectual property community. Under its Digital Agenda – a work program for the organization, WIPO hopes to respond to the confluence of the Internet, digital technologies and the intellectual property system.[34]

Under this agenda, the WIPO sought to revise the *Berne Convention* to meet the realities of copyright law. However, it abstained from calling for further revision, apprehensive that that it would no longer be possible to achieve the unanimity of votes required for any revision according to Article 27(3) of *the Berne Convention.*[35] Article 20 of the *Berne Convention* had provided for a special agreement that did not require the unanimous consent of all its members, however when WIPO proposed to include the protection of phonograms into this special agreement most countries objected, stating that they preferred to deal with the international protection of phonograms in a separate treaty.[36] After much deliberation, the WIPO Diplomatic Conference's final answer was to introduce two new and treaties that would both clarify existing provisions of the *Berne Convention* and establish new norms.

In Geneva, on December 20, 1996, the WIPO Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions adopted two treaties, namely the *WIPO Copyright Treaty* (WCT)[37] and the *WIPO Performances and Phonograms Treaty* (WPPT)[38] which addressed, in summary, the issue of copyright protection in the new digital environment.

---

34 "About WIPO," *supra* note 18.
35 *Supra* note 27. See also J. Reinbothe, *The WIPO treaties 1996: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: Commentary and Legal Analysis* (London: Butterworths, 2002) [hereinafter "WIPO Treaties 1996"].
36 *Ibid* citing Report on the First Sessions, Copyright 1992, at 40 & 52. paras 110 & 111.
37 *WIPO Copyright Treaty,* adopted in Geneva, 20 December 1996, online: <http://www.wipo.int/clea/docs/en/wo/wo033en.htm> (date accessed: 18 June 2002) [hereinafter WCT].
38 *WIPO Performances and Phonograms Treaty and Agreed Statements Concerning the WIPO Performances and Phonograms Treaty WIPO Performances and Phonograms Treaty*, Geneva 20 December

B. The Law

The WIPO Treaties, also referred to as the "Internet Treaties,"[39] are significant because they are the first treaties to have been tailor–made for the new environment created by digital technology. In fact, the third recital of the WCT's preamble refers to the "effects of new technologies on the creation and use of the works,"[40] indicating its focus on digital technology.

The Internet Treaties address various issues of copyright protection, both traditional[41] and novel.[42] Of the various provisions, two articles, Article 11 and 18, stand out as the basis of the obligation of member countries, such as Canada, to create laws for the protection of encryption technology.

1. Article Eleven

Article 11 of the WCT states:

> 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 restricts Acts, in respects of their works, which are not authorized by the authors concerned or permitted by law.[43] (italics supplied)

1996, online: <http://www.wipo.int/clea/docs/en/wo/wo034en.htm> (date accessed: 10 November 2002) [hereinafter WPPT].
39 See "WIPO welcomes U.S. Ratification of 'Internet' Treaties" (1999), online: Press Release <http://www.wipo.org/pressroom/en/releases/1999/p183.htm> (date accessed: 28 April 2003); see also "WIPO Internet Treaties Come Into Force" (2002), online: <http://www.kaapeli.fi/hypermail/ecup-list/0911.html> (date accessed: 28 April 2003).
40 WCT, *supra* note 37.
41 *E.g.* Moral Rights of Performers, see Art 5, WPPT, *supra* note 38.
42 Such as Intermediary Liability, see "WIPO Treaties 1996", *supra* note 35.
43 WCT, *supra* note 37.

Article 11's significance lies in the fact it constitutes the first time[44] that technological measures used to protect author's rights have enjoyed protection through a separate provision in a multilateral treaty.[45]

From the beginning, there was a clear agenda to put measures in place against the circumvention of copyright protection.[46] The member states recognized that new technology, while facilitating access to and use of protected works also multiplied the risks of piracy. They also acknowledged that effective protection measures were already available or under development which would put authors in a position to control the use of their protected work. As a result, there was a widespread agreement to give protection measures support through legislation.

There was also concern that circumvention of these protection devices could undermine the normal exploitation of the works and prejudice the interest of authors.[47] Most notable was the U.S. suggestion that anti-circumvention measures should not be made freely available to the public, defining these as "goods or services the primary purpose of which is to defeat technical security measures."[48]

2. Analysis of Article Eleven

Article 11 was drafted primarily to provide national and regional legislators with a general framework for the protection of technological measures.[49] By itself, the provision

44 Notwithstanding Article 1707 *North American Free Trade Agreement*, which provides for certain protection concerning program-decryption measures. See *North American Free Trade Agreement Between the Government of Canada, the Government of Mexico, and the Government of the United States,* 17 December 1992, Can. T.S. 1994, No.2 I.L.M. 287 (entered into force 2 January 1994), online: <http://www.nafta-customs.org/> (date accessed: 21 March 2003) [hereinafter NAFTA].
45 "WIPO Treaties 1996", *supra* note 35 at 139.
46 "WIPO Treaties 1996", *supra* note 35 at 135. "As part of the section on enforcement, the WIPO Memorandum for the Third Session of the Committee of Experts already included a proposal to oblige Contracting Parties of the future Treaty to provide criminal sanctions, civil remedies and provisional and boarder measures, in relations to the circumvention of copy-protection and for the decryption of broadcasts or otherwise communicated programs."
47 *Ibid* at 135.
48 U.S. submissions in Industrial Property and Copyright (1995), at 299 & 308, online: <http://www.anu.edu.au/caul/org/copyrdoc.htm> (date accessed: 6 August 2002).
49 "WIPO Treaties 1996", *supra* note 35 at 142.

does not enumerate any new substantive author's rights, nor does it give authors a way to enforce copyright. Instead, the law provides protection to copyright through the protection of encryption technology by providing that legal remedies be set in place against its circumvention. Also of note, is the fact the law does not prescribe any precise models towards this end. Contracting Parties legislators have a wide range of flexibility for implementing the obligations under Article 11 WCT. The tone of the article does however provide guidance by indicating the minimum obligations the legislators may follow when determining the scope of protection.[50]

The phrasing of the law itself is vague, enumerating nothing by way of substantive rights or remedies, perhaps in a deliberate move to allow the member countries maximum discretion in deciding how to protect intellectual property.

The first sentence states that the parties provide for "adequate legal protection" of technological measures as well "effective legal remedies against their abuse." The word "adequate" is indicative of the balance that domestic legislator must strive to maintain, between the interest of the authors to achieve strong protection on the one hand, and the interests of those affected by this protection on the other. The law is one which must be sufficiently strong and meaningful to serve its purpose (the protection of the rightholders rights and interests); however, in doing so the protection of the technological measures should be no be so strong that it places an undue burden on other relevant industries.[51]

The term "effective legal remedies," is the logical outcome of "adequate legal protection." The phrase necessarily implies that the rightholders must have a right of redress in the law and that this redress must, to be effective, be "expeditious so as to prevent circumvention and abuse and dissuasive so as to constitute a deterrent to further circumvention and abuse."[52]

---

50 *Ibid.*
51 *Ibid.*
52 *Ibid.* See also definition under the Agreement on Trade-Related Aspects of Intellectual Property Rights [hereinafter TRIPS], Cf Article 41 (1) TRIPS Agreement; Gervais, the TRIPS Agreement, note 2,190 which describes "effectiveness in action," online: <http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm> (date accessed: 14 August 2002).

Article 11 of the WCT also explicitly provides for protection "against the circumvention" of technological measures. What is considered "circumvention" (i.e. acts of circumvention carried out deliberately or the acts done primarily to violate copyright law) is another matter left to the member states. All that Article 11 provides is "minimum protection"[53] which domestic legislators may choose to maintain or increase in their domestic law.

It is worthy of note that preparatory acts of circumvention are not in themselves prohibited by Article 11, as they are not acts of circumvention. This means that domestic legislators have no obligation to declare illegal the manufacture, distribution or possession of devices or components made to circumvent protection technologies. Though arguments have been made that prohibiting preparatory acts forms part of providing adequate protection,[54] the fact remains that Article 11 itself as written does not prohibit these acts.

Neither does the WCT define the term "effective technological measures," in fact the only indicator of its meaning is in the provision itself, which provides the purpose for enacting said technological measures, namely protection of the rights exercised by the authors. It can be inferred from the phrase that first, the technological measures must function properly and second, that they should not prevent or interfere with the normal operation of electronic equipment and its technological development.[55] If, for instance, a copy control device interferes with the functionality of a VCR then by the definition above it is not protected against circumvention under this article.[56]

Another inference made from the term is that for these technological measures to be "effective," they must adequately carry out the function for which they are created. This means that the device must contain adequate technology to protect itself and cannot

---

53 *Ibid.*
54 CF Marks &Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses;" WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty and the WIP Performances and Phonograms Treaty, WIPO doc WCT-WPPT.IMP/3 at 6.
55 *Ibid.*
56 *Ibid.*

rely solely on the law. A device which, for instance, is so simple it cannot adequately protect the work shall be considered ineffective, and since it is ineffective, the author cannot seek redress in the law to protect the circumvention of his inferior product. Again, the measure for ineffective technology remains undefined, leaving the definition to the member states.

The law also provides that the protection must extend to the "exercise of rights under this Treaty or the *Berne Convention* which in turn refer to the protection of copyrighted works.

Finally, the article provides that these prohibited acts must be "acts not authorized or permitted by law." Consequently, acts which have the consent of the author or allowed by the domestic law of the member state concerned are not covered. In Canada for instance, Article 11 would not cover circumvention devices used fairly for private study and research, since they are exceptions to copyright and allowed under the Canadian *Copyright Act*.[57]

3. Section Eighteen

Article 18 of the WPPT, which states:

> Contracting Parties shall provide adequate legal protection and effective legal remedies *against the circumvention of effective technological measures* that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restricts Acts, in respect of their works, which are not authorized by authors concerned or permitted by law.[58] (italics supplied)

57 Copyright Act § 29, *supra* note 2.
58 WPPT, *supra* note 38.

The passage of Article 18 had its roots not at the creation of the Internet Treaties themselves but before that at the Berne Protocol,[59] an indicator of the pressing need for its passage. The proposed enforcement provisions of the Protocol contained various sanctions for certain uses of illicit devices for copy protection and for the decryption of broadcasts or otherwise communicated programs.[60] This protocol was the framework for the drafting of this particular article and until the Third Session of the WIPO, not many changes were made.

It is interesting to note that on the Fourth Session, the U.S. was the only delegation to submit a proposal specifically on the protection of technological measures and separately from enforcement measures. Under their proposal, protection included the prohibition of decoders and anti-copying prevention devices, as well as the prohibition of the making available to the public of goods and services, the primary purpose of which was to defeat technical security measures. In addition, the U.S. proposal asked for protection against the importation, manufacture and distribution of devices that defeat hardware and software-based anti-copying systems.[61] Such submissions provided a window into the U.S. digital copyright agenda, already fully formed even before the passing of the Internet Treaties. It was an agenda that would later be fulfilled with the passing of its own domestic law, the DMCA.

4. Analysis of Section Eighteen

After much debate about the language of the provision, Article 18 of the WPPT was finally drafted. Together with Article 11 of the WCT, Article 18 constitutes the first time technological measures used to protect intellectual property rights have been protected through a separate Treaty. Like Article 11 of the WCT, Article 18 does not provide performers of producers with any new substantive rights nor does it, as worded,

---

59 Memorandum for the First Session, Copyright 1993, pp 142, 155/paras 82 (proposal) and 77-78 (explanations).
60 "WIPO Treaties 1996", *supra* note 35 at 43.
61 *Ibid*, citing proposals from the Fourth Session, Industry Property and Copyright 1995, pp. 363, 378 et seq /paras 11-13.

enforce any of their existing rights. Again, it protects rightholders solely by safeguarding the technological measures they use to manage and enforce their existing rights under the treaty and the *Berne Convention*.

Article 18, like Article 11 WCT, provides the member states with a general framework for the protection of technological measures. It is a minimum standard, which allows domestic legislators flexibility on how to implement the law while providing guidelines on the principles they need to protect.

Article 18 and 11 share identical concerns, namely that technology has allowed for the easier dissemination of copyrightable materials thus increasing the risks of piracy and the consensus that the best way to control digital technology is by digital technology. The articles are also based on the belief that it is the rightholders who hold the most effective means of protecting their rights through the use of devices that control access or use of intellectual property.[62]

Thus, like Article 11 of the WCT, Article 18 aims to safeguard intellectual property rights by protecting the technology and providing remedies against the circumvention thereof.

The wording of Article 18 is identical in almost every respect to Article 11 of the WCT, except that in under Article 18 the words "performer and producers of phonograms" replace "authors," which extends the effects of the Treaty not only to literary works but copyrighted works in various mediums such as music and cinema. Article 18 also differs from Article 11 in that its wording extends the protection of the Treaty not merely to the original authors of the work but those who legally "reproduce" the work, such as publishers and recording studios. In all other aspects however, they remain identical in both purpose and form.

---

62 *Ibid.*

III The Objectives: Two Policy Papers on Digital Copyright Reform

A. The Proposal Papers

On December 1997, Canada became a signatory to the Internet Treaties, agreeing, in effect, to alter its domestic law to comply with the treaty provisions and committing not to derogate from the principles embodied therein.[63] These were the first intellectual property treaties signed by Canada that addressed the digital network environment.[64] Though Canada has not as yet ratified these treaties domestically, in 1998 the Canadian government held a consultation on amendments to the Canadian *Copyright Act* that would be required if Canada were to ratify these treaties, an indication of the government's desire to comply with the treaty provisions.

As the first step to its proposed reforms, Industry Canada released two policy papers entitled *A Framework for Copyright Reform* and the *Consultation Paper on Digital Copyright Issues* on the 22nd of June 2001 for public comment. Canadians were invited to comment on these policy papers until the 15th of September 2001.

Thereafter, the departments held consultations meetings to develop policy options, beginning early 2002.[65] The comments and consultations ended on September 2002 when the government released the Section 92 report that reviewed the *Copyright Act* and outlined a proposed agenda for copyright reform based on the principles and criteria that are set out in the policy papers. In its report, the government stated its plans to develop legislation over the next couple of years. [66]

The papers themselves introduced the reader to the concept of copyright, focusing on the impact of digital technology on copyright law.[67] They explained the purpose of the

63 Framework, *supra* note 1.
64 *Ibid.*
65 "Copyright Reform Process," online: <http://strategis.ic.gc.ca/SSG/rp01100e.html> (date accessed: 10 September 2002).
66 Framework, *supra* note 1.
67 Consultation Paper, *supra* note 7.

papers, which were to "initiate consultation on a number of issues that arise at the intersection of the new digitally networked environment with the *Copyright Act*."[68]

The Framework provided an overview of the project, enumerating its cultural and economic policy objectives as well as the project's context, stemming from its obligations under the Internet Treaties as well as its obligation to review the *Copyright Act* within five years from its enactment.[69] The government also stated its intention to embark on a process of copyright reform where it would "consider issues, consult Canadians, and propose legislative amendments... in a gradually staged manner."[70]

The Consultation Paper made available a more in-depth discussion of the issues enumerated in the Framework Paper. It aimed to explore potential solutions to key digital copyright issues, including whether to amend the *Copyright Act* to prevent the circumvention of technologies used to protect copyright material as well as the manner and extent of this new amendment.

While the government's view on the various issues remained open to both debate and response, its objective, outlined in the Speech from the Throne of 2001, was clearly stated: to "ensure that Canada's copyright framework is among the most modern and progressive in the world."[71] In that light, the objectives to be achieved through the reform process are to:

- create opportunities for Canadians in the new economy;
- stimulate the production of cultural content and diversity of choices for Canadians;

---

68 *Copyright Act*, *supra* note 2.
69 *Copyright Act*, §92, *supra* note 2. "Within five years after the coming into force of this section (i.e., no later than September 1, 2002), the Minister (of Industry) shall cause to be laid before both Houses of Parliament a report on the provisions and operation of this Act, including any recommendations for amendments to this Act."
70 Framework, *supra* note 1 at 3.
71 Online: <http://www.ic.gc.ca/cmb/Welcomeic.nsf/261ce500dfcd725985256482006 8dc6d/85256a220056c2a485256a710062b454!OpenDocument> (date accessed 5 June 2002).

- encourage a strong Canadian presence on the Internet; and enrich learning opportunities for Canadians.

B. The Relevant Provision

Section 4.2 of the Consultation Paper, entitled *Legal Protection of Technological Measures* was devoted solely to the issue of protection technologies. The Paper defined these as "technologies... to thwart the infringement of copyright materials online."[72] The Paper further raised the issue of "whether and under what circumstances copyright legislation ought to provide sanctions against persons who engage in activities related to the circumvention of... protective measures."[73]

The section began with a basic background, introducing protection technology and reasons for protecting it, principally because "once a technological measure is defeated, control over the authorized dissemination and use of works in the networked environment is effectively lost."[74] More importantly, it distinguished copyright protection technology from copyright itself. To wit:

> "Copyright law itself protects rights holders against unauthorized uses while technological measures adopted by rights holders to ensure their rights serve to provide an additional layer of protection for works. Any proposed statutory provisions to protect technological measures would in effect be a third level of protection, *albeit one that relates not to the works per se but to the technological measures in relation to the works*." (italics supplied).

The Paper also questioned the wisdom of including all protection measures under the *Copyright Act*, stating: "by providing legal recognition of technological measures, the traditional boundaries of copyright law would be extended to include new layers of

72 Consultation Paper, *supra* note 7, at 20.
73 *Ibid.*
74 *Ibid.*

protection and thus the *Copyright Act* may not be the proper instrument for protection measures which, *prima facie*, are extraneous to copyright principles."[75]

Section 4.2 specifically addressed Canada's treaty obligations under the WIPO, citing section 11 and 18 verbatim. It enumerated several jurisdictions that had implemented the WIPO provisions on protection technology into its domestic law, focusing much of its discussion on the DMCA. It acknowledged that U.S. law went further that its obligations under the WIPO by "target[ing] not only acts of circumventing technological protection measures for the purpose of gaining unauthorized access to the works, but specifically prohibit[ing] (subject to certain exceptions) the manufacture and distribution of devices and the sale of services (circumvention services) that are used to circumvent such measures."[76]

In discussing the DMCA and other similarly stringent laws such as those proposed by the EU and adopted in Japan, the Consultation Paper considered a number of issues, such as the law's effect of "overriding the traditional contours of copyright protection" and "potentially blocking all types of access and use."[77]

The Paper contrasted the above stringent laws with Australia's Copyright Amendment (Digital Agenda Bill), a law that "does not proscribe the act of circumvention, but makes it illegal to manufacture or trade in devices that circumvent 'effective technological measures.'"[78] Unlike the DMCA, Australia narrowly confined its definition of "effective technological measures," to include only "copy control mechanisms and mechanisms that provide access to work through an access code or process."[79] The Australian approach appears to fully satisfy the requirements under the WIPO because Article 11 and 18 of the WIPO themselves leave such definition of the term to domestic law.

---

75 Consultation Paper, *supra* note 7 at 20.
76 *Ibid.*
77 *Ibid.*
78 *Ibid.*
79 Ibid. See also Australian Copyright Act of 1968, Section 116A, division 2A - Actions in relation to circumvention devices and electronic rights management information importation, manufacture etc. of circumvention device and provision etc. of circumvention service.

The Paper emphasized that the wide variety of anti-circumvention legislation reflected the "flexibility of the WIPO treaty requirements."[80] It further went on to state that since there was "no clear sense of what impact technological measures will have on copyright legislation,"[81] Canada could, to a certain extent, map out its own path based on its own domestic public policy objectives. It discussed these objectives briefly, reiterating its concern that this new law may upset the delicate balance that exists between the copyright stakeholders.[82]

With this information laid out before the reader, the Paper detailed several legislative proposals, furnishing the reader with a diversity of choices. On one end of the spectrum, the Paper proposed a law prohibiting only "specific acts:"[83]

> The *Act* would specifically prohibit the circumvention, for infringing purposes, of technological measures, where such measures have been adopted *inter alia*, to restrict acts not permitted by the *Act*. [84]

On the other end, it suggested the most extensive form of prohibition, which entailed criminalizing circumvention devices in addition to a prohibition on acts. To wit, the law would provide "remedies against importing, selling, letting for hire, by way of trade exposing for sale any device whose purpose is to circumvent any technological measure used to protect right or rights conferred under the *Copyright Act*."

Given the broad range of possible legislation, Section 4.2 concluded by posing the following questions for the reader to consider:

1. "Given the rapid evolution of technology and the limited information currently available regarding the impact of technological measures on

80 Consultation Paper, *supra* note 7.
81 *Ibid.*
82 *Ibid.*
83 *Ibid.*
84 *Ibid.*

control over and access to copyright protected material, what factors suggest legislative intervention at this time?

2. Technological devices can be used for both copyrighted and non-copyrighted material. Given this, what factors should be considered determinative in deciding whether circumvention and/or related activities (such as the manufacture or distribution of circumvention devices) ought to be dealt with in the context of the *Copyright Act*, as opposed to other legislation?"

3. If the government were to adopt provisions relating to technological measures, in which respects should such provisions be subject to exceptions or other limitations?

4. Are there non-copyright issues, e.g. privacy, that need to be taken into account when addressing technological measures?" [85]

C. The Responses

1. Individual Respondents

The individual respondents though numerous,[86] were almost single minded in their answers. Most respondents were private users who saw anti-circumvention as restrictive to the legitimate use of legally purchased products; others were researchers and scientists who were concerned that the law would stifle both their research and progress in general. Still others were scholars and professors, apprehensive that the implementation of anti-circumvention law would stifle education both by making educational materials inaccessible and by prohibiting progress and free educational debate and study.

Another common thread between the individual respondents was their emphatic sometimes even violent decrying of the DMCA. Calling the law "a travesty of justice,"[87]

---

85 *Ibid.*

86 Over 700 documents submitted to the consultation process, majority of which (approximately 600) were from individual respondents. See: *Submissions Received Regarding the Consultation Papers*, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html#sub> (date accessed: 05 March 2003).

87 Submission from Dennis Grant received on July 30, 2001 12:44 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

they cited its chilling effects on education and research as well as infringement on fair use and free speech. They cited instances of this injustice in the U.S., mostly citing the litigation against Edward Felten and Dimitri Skylarov as examples. The respondents were single minded in their hope that Canada would learn what was "bad law"[88] from the U.S. example and forge a better more balanced path in line with Canadian values and goals.

The individual respondents were, as a whole, less methodic in their answers than the respondent entities, however several points were made that correspond to the government's guideline question. They are as follows:

a) Question 1

Given the rapid evolution of technology and the limited information currently available regarding the impact of technological measures on control over and access to copyright protected material, what factors suggest legislative intervention at this time?

While the majority of private respondents acknowledged the changes resulting from digital technology, very few believed there was a need for any new anti-circumvention legislation. In fact, most respondents denounced any form of anti-circumvention law as a breach of freedom of speech and an invasion of privacy.[89] Arguing against legislative intervention, many individual respondents maintained that anti-circumvention law was ineffective since such laws did little more than inconvenience the buyer from using legally purchased software. One irate respondent contended:

> As noted in the 'Consultation Paper on Digital Copyright Issues', technological measures have failed in the past and are often a serious hindrance for legitimate users. Reinforcing technological measures with the law encourages corporations to ineffectively attempt to stall infringement at the expense of legitimate users. These users become forced to endure odious constraints and

88 *Ibid.*
89 Submission from Christian Charette received on July 24, 2001 2:06 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

> limitations on the private use of media they have legally purchased and copyrighted information they have licensed.[90]

Respondents enumerated a wide range of factors against legislative intervention, such as problems with interoperability, security testing, privacy, research, weak technologies; in summary a statement of what most respondents ridiculed as obvious logic: outlawing circumvention technology criminalizes an act with a myriad of legitimate uses, which will in turn affect those legitimate users. In the words of one respondent, it is "the shackling of information which can only be detrimental to society." [91] As proof, respondents repeatedly cited the DMCA and the chaos that has resulted from its implementation in the U.S.

On the offensive, individual respondents also debunked some possible "factors" which may give rise to anti-circumvention legislation, such as loss of sales, decrying this factor as one of the myths perpetrated by corporations to justify government intervention. In support of their claim, they cited *Napster*,[92] where it was proven by the defense that "increased exposure to new music via Napster resulted in increased music sales."[93] In fact, one respondent suggested that contrary to common belief, there was an inverse relationship between music sales and government intervention. "Prior to the DMCA and its pursuant litigation," the respondent alleged, "music sales grew. This year, at the height of litigation, music sales have stagnated and declined." [94]

The sufficiency of the *Copyright Act* and the delicate balance that has been developed over decades[95] was also touched upon, as well as the argument that the onus of

---

90 Submission from Ashley George received on July 17, 2001 11:59 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
91 *Ibid.*
92 *A&M Records Inc. et al.* v. *Napster Inc.*, 54 U.S. P.Q. 2d 1746 (N.D. Cal 2000) [hereinafter *Napster*].
93 Dennis Grant, *supra* note 87.
94 Submission from Mark Cuban received on June 22, 2001 4:13 PM via e-mail online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
95 Submission from Canadian Association for Interoperable Systems received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter Interoperable Systems] - "Technological protections would only be necessary if copyright law were not sufficient and if the threat of infringement did in fact discourage the distribution of new digital works. However, as we noted above, content has been distributed in digital form for

protecting their technology should fall upon the companies themselves[96] and was not the proper subject of legislative intervention. The sentiment to Question One can be summarized by one respondent who stated adamantly, "there is no new need for new copyright law."[97]

The few individuals that allowed for some form of legislative intervention, citing factors such as the ability to make perfect copies and Canada's obligations under the WIPO treaty[98] remained wary, suggesting that any new laws should tread lightly, taking into account the rights and freedoms and punishing acts of infringement only.

b) Question 2

Technological devices can be used for both copyrighted and non-copyrighted material. Given this, what factors should be considered determinative in deciding whether circumvention and/or related activities (such as the manufacture or distribution of circumvention devices) ought to be dealt with in the context of the *Copyright Act*, as opposed to other legislation?

Many replies by the individual respondents echo the government's concern that circumvention technology can be used for both copyrighted and non-copyrighted material and thus have both legitimate and illegitimate uses.

Individual respondents, as a whole, were adamant that circumvention technology not be criminalized, citing a variety of non-infringing uses that did not interfere in any

---

decades, and copyright does provide meaningful protection notwithstanding that the content is in digital form."

96 Submission from Submission from Jakub Wojnarowicz, received on July 24, 2001 2:01 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) – "If they do not want their hardware to be modified into something they don't want, they'd better build it right."

97 Submission from Richard Anthony Hein, received on July 24, 2001 2:20 pm via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

98 Submission from Ryan McDougall received on July 30, 2001 10:52 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

way with the rights of copyright owners. The most popular argument was that circumvention allowed for the legitimate use of copyrighted material without hindrance. For instance, one respondent pointed out that if anti-circumvention technology is passed prohibiting any circumvention technology he would no longer be able to validly reverse engineer copyrighted software to make it run properly with his older CD drives.[99] Another user pointed out that it was ludicrous to be held liable for reverse engineering his software to allow interoperability between that software and a different format like Linux.[100]

Other legitimate uses were cited, such as circumventing encryption schemes employed by viruses, and worms in order to develop techniques for detecting and defeating them; detecting security problems in software deployed on Internet servers; regaining access to computer with lost passwords; ensuring products do not contain marketing data collection systems or other privacy violating measures; protecting national security by demonstrating weak technologies and countering marketing claims by companies who assert that certain secure formats are suitable for sensitive information.[101]

In that there are both legitimate and illegitimate uses for circumvention technology, many individual respondents argued the difficulty of creating a law that both allows for legitimate use and yet prevents anti-circumvention technology. In the words of one respondent:

> "It is unnecessary, it prohibits scholarly discussion about the method of protection of data (by simply making it illegal to try and circumvent that protection for any reason), and it interferes with the consumer's right to make use of what he has paid for."[102]

---

99 Submission from Jakub Wojnarowicz, *supra* note 96.
100 Submission from Ryan Peters received on July 24, 2001, 8:48 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
101 Submission from Jesse Burns received on July 24, 2001 2:34 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
102 Submission from Chris Friesen, received on July 24, 2001 10:53 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

c) Question 3

If the government were to adopt provisions relating to technological measures, in which respects should such provisions be subject to exceptions or other limitations?

Most individual respondents did not cite exceptions to possible anti-circumvention technology law, instead they suggested either that no anti-circumvention technology law be enacted or, in the alternative, that the legislation be the exception invoked in specified and defined instances.

Many individual respondents contended that prohibiting the act of circumvention is in itself wrong, and since it has so many lawful applications, criminalizing the act creates a "forbidden class of knowledge"[103] which stifles the progress of society as a whole.

Respondents cited the DMCA as a prime example, pointing out that the DMCA's list of exceptions did little to prevent both actual and threatened litigation against researchers, scientists and professors.[104] They argued the dangers of erecting nebulous barriers which, with their deep pockets and barrage of lawyers, companies could use to harass legitimate acts of circumvention.

In arguing their point, respondents distinguished between the act of circumvention, an act with many legitimate and beneficial uses, and the act of infringement, which is an illegal act. Respondents were adamant that as the act of circumvention was legal, any legislation passed should criminalize the act only if carried out in consonance with other acts of infringement. A respondent suggested passing a law in which the act of circumvention itself is not determinative of whether or not an illegal act has been

---

103 Submission from Jesse Burns, *supra* note 101.
104 Submission from Samuel Philip Lake Smith received on July 10, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

committed but affects the degree of criminal sentencing or civil damages.[105] As another respondent succinctly stated, "I think that the technology and speech should not be made illegal in anyway, but the act of pirating willfully should be."[106]

In summary, individual respondents suggested that anti-circumvention legislation be worded in a manner that allowed for acts of circumvention except when such acts were done in preparation of or in consonance with illegal acts of copyright infringement defined under the *Copyright Act*.

d) Question 4

Are there non-copyright issues, e.g. privacy, that need to be taken into account when addressing technological measures?

Issues such the loss of privacy, free speech and fair dealing were the themes most widely addressed by individual respondents who were almost unanimous in the belief that these rights would be greatly diminished by anti-circumvention legislation.

Regarding free speech, respondents were of the opinion that anti-circumvention technology legislation created an atmosphere where people could not discuss or disseminate information about circumvention devices, in effect "regulating thought."[107] Numerous respondents cited the heavily documented cases of Professor Edward Felten and Dimitri Skylarov, both of whom received criminal sanction or threat of criminal sanction for the mere dissemination of knowledge considered illegal under the DMCA, a situation aggravated by the fact that the researchers were disclosing flaws in the encryption that made the apparently secure system vulnerable. More than one respondent

105 Submission from Sandy Harris received on July 29, 2001 9:13 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
106 Submission from Hakim Sid Ahmed received on July 28, 2001 3:46 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
107 Submission from Ryan McDougall, *supra* note 98.

compared purchasing encrypted software to the purchase of a vehicle, questioning the validity of jailing someone for "pointing the flaws in a company's defective tires."[108]

Fair dealing was another issue of concern. As one individual vehemently argued, "often, technological measures are referred to as 'protection'. This is a misleading term abused for its positive connotations. Technological measures are not about protection, they are about control..."[109]. "Technological measures require users to jump through hoops to privately use their purchased media or licensed content in manners the original content authors did not foresee or personally desire."[110]

Another concern was that anti-circumvention legislation would prevent Canadians from being able to remove spyware and cookies from their computers if such software was deliberately encrypted to prevent its removal. They also noted that the exceptions for privacy provided by the DMCA were insufficient because while it exempts acts of circumvention to remove invasive software it does not allow for the distribution of software to aid in said removal. The resulting situation is one where the only option left to the user is to create the necessary circumvention software, an impossible task for all but experienced software designers.

2. Reponses from Entities

As could be expected, the responses from corporations and other interest groups varied according to the interests they sought to protect. Unlike the individual respondents who espoused a relatively uniform stance against anti-circumvention legislation, the range of the respondents covered a broad spectrum.

108 Submission from Chris Nelson received on July 24, 2001 3:30 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
109 Submission from Ashley George, *supra* note 90.
110 *Ibid.*

On the one hand, there were the staunch supporters of DMCA-like provisions, mostly video, audio and licensing companies, which emphasized the growth of piracy on the internet and the need for immediate action to protect copyright owners. On the other hand there were those, mostly educational institutions and NGO's, who remained firmly against anti-circumvention law, deeming it an improper and ineffective way of solving copyright infringement. In the middle ground were various interest groups, some of which believed in a modicum of anti-circumvention legislation and others, such as libraries and archival societies, who were mainly concerned not with the legislation itself but how the said law would affect their specific interest.

Worthy of note is the fact that aside from a few corporations which clearly had their own agenda, there was a consensus that any anti-circumvention legislation must be carefully considered with due regard for both existing copyright legislation and individual rights.

a) Question 1

Given the rapid evolution of technology and the limited information currently available regarding the impact of technological measures on control over and access to copyright protected material, what factors suggest legislative intervention at this time?

The proponents of anti-circumvention legislation brought forward, as a whole, four basic propositions in favour of legislative intervention. First, were Canada's obligations under the WIPO. Proponents emphasized that for Canada to obtain similar protection abroad, it must enact laws with equally strong anti-circumvention provisions. In the words of one proponent, "until all the provisions of the Internet Treaties are implemented,

Canadian copyright owners will continue to be deprived of the level of international protection resulting from the implementation of any of them."[111]

Second, was the fact that piracy on the internet was becoming more and more rampant and that circumvention technology was necessary to combat it. Proponents claimed "the internet presents a readily available tool for unauthorized, perfect, costless, instant, multiple, global copying and exponential worldwide dissemination that can be done in private and is difficult to detect."[112]

As a primary example, they pointed to the now defunct Napster. They also cited peer-to-peer file sharing networks that allowed individual computer users to search for and download music and other files from other users of the network.[113] They argued that technological protection measures were necessary to combat piracy and since there was no effective provision in Canadian law to prevent hackers from acting to defeat technological protection measures, there was a pressing need for legislation to enact such a law.[114]

Third was the argument that encryption technology was useless without anti-circumvention legislation. They contended that "protection 'systems' from simple passwords to complex encryption algorithms remain[ed] at the mercy of systems hackers and software code crackers."[115] Proponents espoused the need to prevent the decryption itself through legal means, and thus "it [was] incumbent on the Government to put in place legislative provisions that make it unlawful to interfere with those safeguards."[116]

---

111 Submission from Canadian Motion Pictures Distributors Association (CMPDA) received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
112 Submission from Society of Composers, Authors and Music Publishers of Canada (SOCAN) on September 18, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter SOCAN].
113 Submission from Canadian Copyright Institute (CCI), received on September 17, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter CCI].
114 SOCAN, *supra* note 112.
115 Submission from IBM Canada received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter IBM].
116 SOCAN, *supra* note 112.

Fourth was the proposition that anti-circumvention legislation, by creating a safer haven for copyright owners, will entice more businesses. On the other hand, "without adequate copyright protection content owners [would] be reluctant to authorize distribution of their work using these new technologies." [117]

Those against anti-circumvention rebutted the above propositions with four counter-arguments:

As to the first argument emphasizing Canada's obligations under the WIPO, opponents established that the provisions set out in the Internet Treaties oblige contracting parties to provide legal protection and remedies against circumvention only to the extent that the circumvention was not authorized by the owner or permitted by law.[118] Furthermore, opponents asserted that the WIPO "does not *require* the adoption of device restrictions, and that a device-oriented approach was specifically rejected, and replaced with the more general adequate protection language that became Article 11."[119]

In rebuttal of the second argument that piracy on the internet was becoming increasingly rampant, opponents maintained that anti-circumvention legislation was an ineffective way of combating piracy on the internet. They compared this to the banning of prohibited devices as such photocopiers and VCRs in order to prevent copying.[120] In the words of one opponent, the argument "ignores the fact that there are legitimate purposes for making copies without the copyright holder's authorization and that these legitimate purposes would be frustrated by a ban on circumvention devices."[121]

---

117 Submission from Canadian Copyright Licensing Agency (CANCOPY), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter CANCOPY].
118 CLA, *supra* note 12.
119 Submission from Electronic Frontier Canada received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
120 Interoperable Systems, *supra* note 95.
121 *Ibid.*

Opponents contended that copyright laws are in fact adequate to protect digital content. They also cited *Napster*[122] and another case against MP3.com,[123] pointing out that in both decisions the U.S. Supreme Court relied on traditional copyright theories which more than "aptly accommodated the copyright owners' online infringement claims."[124] They further argued that the software industry has waged effective campaigns throughout the world against counterfeiters and corporate infringers who exceed the terms of site licenses. Though they admitted infringement still occurs, they claimed it is most virulent in countries without effective legal systems.[125]

Opponents rebutted the third argument that technology was useless without anti-circumvention legislation by contending that while technological protection measures could be defeated, even the proponents acknowledged they could not be defeated easily.[126] Opponents argued that while "while weak protections can certainly be defeated by a talented and persistent hacker, it [was] far more difficult to crack a system that uses more sophisticated measures, such as public key encryption." Furthermore, they stressed that the mere fact that technology could be circumvented did not automatically mean it would be.[127]

---

122 *Napster, supra* note 92.

123 *Chambers v. Time Warner, Inc.*, 282 F.3d 147 (2002). – Plaintiff recording artists sued defendant record companies alleging copyright infringement. The recording artists recorded performances of musical works under contracts with predecessors of the record companies. Pursuant to these contracts, the recording artists assigned ownership rights, including copyrights, in their sound recordings to the record companies. The recording artists asserted that the contracts did not authorize the sale of digitized versions of their performances on the Internet. In deciding defendants' motion to dismiss, the district court considered several unsigned drafts of a collective bargaining agreement (AFTRA Codes) between record producers and an artist organization, which was submitted by the record companies. The appellate court determined that the district court, after deciding not to convert the motion to dismiss to a motion for summary judgment, improperly considered the AFTRA Codes because the recording artists did not rely on the terms and effects of the documents in drafting the complaint. In addition, the district court erred by dismissing the Lanham Act claim without considering other conduct raised by the record artists' allegations.

124 Interoperable Systems, *supra* note 95.

125 *Ibid.*

126 IBM, *supra* note 115. "Today all protection "systems" from simple passwords to complex encryption algorithms remain at the mercy of systems hackers and software code crackers - albeit at a level of sophistication and hardware requirements beyond the means of most users."

127 Interoperable Systems, *supra* note 95. "[E]ven if stronger protections were vulnerable to circumvention, it does not necessarily follow that most users would in fact circumvent these protections. Studies reveal that the vast majority of computer and Internet users are technologically unsophisticated. While they may be willing to make a digital copy of a song or a computer program if they could do so with a single keystroke, they are far less likely to make that copy if they have to first search the Internet for a circumvention utility, download it, and then use it to defeat copy protections embedded in the song or program. True, there will always a degree of circumvention. However, in the Association's view, this amount is minimal and does not justify legislative intervention."

They rebutted the fourth proposition by contending that the enactment of anti-circumvention legislation would make little difference to the Canadian economy and that despite of lack of legislation, businesses would continue to come to Canada and distribute digital products over the internet because in the end it was more profitable to do so.[128] Opponents argued that the internet remains a profitable vehicle for most companies despite piracy problems. In the words of one opponent, "a consumer would have to download many songs and films to equal the value of one plane ticket or computer purchased over the internet."[129]

b) Question 2

Technological devices can be used for both copyrighted and non-copyrighted material. Given this, what factors should be considered determinative in deciding whether circumvention and/or related activities (such as the manufacture or distribution of circumvention devices) ought to be dealt with in the context of the *Copyright Act*, as opposed to other legislation?

A few respondents suggested that separate legislation might better address future laws on anti-circumvention.[130] However, a majority were of the opinion that since it dealt with matters of copyright protection, specifically "the protection of technological measures to restrict the unauthorized reproduction of intangible properties in digital form,"[131] the *Copyright Act* was suitable for anti-circumvention legislation, should such legislation, in fact, be enacted.

---

128 *Ibid.* "There is no denying that digital works can be reproduced at low cost with little degradation in quality and that the availability of infringing copies on the Internet is aiding in their distribution. That, however, does not necessarily mean that the threat of infringement discourages the distribution of new works. To the contrary, it appears that the content industries have decided that the profits to be made by distribution of digital content outweigh the cost of infringement."
129 Interoperable Systems, *supra* note 95.
130 *Ibid.*
131 CANCOPY, *supra* note 117.

The conflict among respondents lay mainly in how pervasive the proposed legislation should be. Predictably, the opinions covered the entire gamut of the spectrum. On the one end, there were those firmly against legislative intervention who maintained there was no need for any sort of anti-circumvention law. On the other end there were those who advocated an approach whereby "any attempt to circumvent these technological measures was prohibited and severely sanctioned."[132] The latter argued, "since the act of circumvention, which frequently is also copyright infringement, was typically immediately followed by an act of infringement, a prohibition focusing exclusively on the act of circumvention adds little to existing protections under copyright."[133]

Most respondents however were open to the idea of "some form of circumvention legislation."[134] Of those open to the idea however, many stressed the various legitimate uses for circumvention and cautioned against a blanket prohibition on the act of circumvention that would suppress many legitimate activities such as academic research,[135] access to matters that are part of the public domain[136] or the transfer of protected matter into archives.[137]

Even staunch supporters of anti-circumvention legislation admitted that circumvention could be allowed as long as "consideration [was] given to ensuring that devices, systems or processes that permit the exploitation of intellectual property without

---

132 Submission from Canadian Broadcasting Corporation (CBC) on September 17, 2001via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
133 Submission from Intellectual Property Institute of Canada (IPIC) received on September 27, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
134 Submission from Canada School Boards Association (CSBA), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter CSBA].
135 Submission from The Graduate Student Society of the University of British Columbia received on September 24, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
136 Submission from Canadian Association of Law Libraries/Association *Canadienne des Bibliothèques de Droit* (CALL/ACBD) received on September 17, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
137 Submission from Canadian Archival Community received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

the permission of the copyright owner are restricted in use to ensure there is no detrimental interference with the rights of the copyright owner."[138]

c) Question 3

If the government were to adopt provisions relating to technological measures, in which respects should such provisions be subject to exceptions or other limitations?

Again, there was an extensive range of responses to the question. The general consensus however, even from the staunchest supporters of anti-circumvention legislation, was that the law "should be crafted to incorporate well-established exceptions and limitations, including finite term, public domain, fair dealing, educational institutions, libraries, archives and museums, incidental inclusion and other exemptions."[139]

As to the enumerated exceptions themselves, the answers varied from respondent to respondent, depending on their area of interest. Libraries for instance asked that the law specifically exclude materials within the public domain while archivists asked for an exemption regarding materials that needed to be archived. Educational and research institutions were adamant that an exemption be granted for reverse engineering to enable them to continue their education and research, a sentiment echoed by small software companies who asked that the law contain exceptions to allow for the reverse engineering of software to achieve interoperability.

The major point of contention between the various respondent entities was not whether there should be limitations on circumvention technology but whether exceptions should exist in the manufacture and importation of circumvention devices. On one side were those who believed that "there should be no exceptions whatsoever allowing the

---

138 SOCAN, *supra* note 112.
139 Submission from DIRECTV INC. received in both official languages on September 15, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

manufacture circumvention devices."[140] These entities argued "any exception to the technological measures provisions would erode the benefits of the measures and gradually make them meaningless."[141]

On the other end of the spectrum were those who maintained devices should be legal to manufacture. They asserted that "introducing any sanctions that would make it illegal to manufacture or import devices that could be used to circumvent technological measures used by copyright owners to control access to their works would effectively gives the copyright owner unrestricted authority to determine the extent of protection provided to a work, irrespective of any limitations that might otherwise be provided for by statute."[142]

d) Question 4

Are there non-copyright issues, e.g. privacy, that need to be taken into account when addressing technological measures?

The respondents provided a list of issues they considered essential when addressing the protection of technological measures.

The first and most prevalent issue was that of privacy. A majority of the respondent entities agreed that the issue should not be ignored. However, there was disagreement on whether matters of privacy were relevant to the proposed legislation and, if they were, the extent to which they should be addressed. Respondents in favour of anti-circumvention legislation were logically less concerned about issued of privacy. While a few recognized "privacy was an important concern,"[143] others contended that the issue

140 Submission from Canadian Publishers' Council received on September 18, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
141 CANCOPY, *supra* note 117.
142 CLA, *supra* note 12.
143 CCI, *supra* note 113.

was irrelevant and that "issues of privacy, should they exist, be dealt with under separate privacy legislation."[144]

Respondents less in favour of anti-circumvention legislation, on the other hand, opined that privacy was an important issue that needed to be addressed. To emphasize their point, more than one respondent brought out the issue of "cookies"[145] and the fact that that the proposed legislation may result in the public losing its right to self-help methods to protect their privacy.[146]

Another concern raised by respondents was the "limitation of reverse engineering."[147] Respondents asserted that scientists and software designers often used reverse engineering to ensure the interoperability between digital products, a legal and accepted practice that could be hampered by the proposed legislation.

A related issue raised by the respondents was the "hindering of encryption research."[148] Respondents contended that engineers often test lawfully acquired encryption programs for weaknesses or to create stronger encryption systems and that it was essential for the growth of electronic commerce that they be able to continue doing this.[149]

Other issues brought to light were those of security, monitoring use on the internet and, generally, the criminalization of legitimate activities.

---

144 Submission from Canadian Recording Industry Association (CRIA), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).
145 Submission from Council of Ministers of Education Copyright Consortium (CMEC), September 14, 2001 via fax, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002) [hereinafter CMEC]; Interoperable Systems, *supra* note 95; CSBA, *supra* note 134.
146 CSBA, *supra* note 134.
147 Submission from the Association of Universities and Colleges of Canada (AUCC), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002); Interoperable Systems, *supra* note 95, CMEC, *supra* note 145; CSBA, *supra* note 134.
148 Interoperable Systems, *supra* note 95.
149 CSBA, *supra* note 134.

3. The Government's Summary of Stakeholder Submissions

On March 2002, both Industry Canada and Canadian Heritage issued their Summary of Stakeholder Submissions entitled: "An Overview of Submissions on the Consultation Paper on Digital Copyright Issues."[150] Within they outlined the conflicting concerns of the various stakeholder respondents, concentrating on four key points.

First was a general acknowledgement that the responses were based on different starting premises: access, balance, control, speech. Weighing the necessity of legislation, which balanced the rights of all stakeholders, they studied the view that any legal protection "would irrevocably alter the public policy balances in the *Copyright Act*" and emphasized that the said protections "were essential to restore the equilibrium that they perceived to have been tilted in favour of users."[151] They also restated the suggestion that more study in this area was necessary before committing to a specific legislative regime since both the concept and the law would be complex and confusing.

Second was a discussion on the act of circumvention. The Government reiterated the respondents' concern on the limits to be placed the act of circumvention. Those opposed argued that excessive restrictions on such acts would hamper innovation and research, and would discourage access to works. Further, respondents opined that technological protection measures that did nothing other than control access to technology should not enjoy protection under copyright law, and that some infringement must first occur before the law could be invoked. Stakeholders in favour, pointed to the ease of circulation of works on digital networks, and argued that ownership of the rights in works would risk becoming meaningless without them.

The Paper cited the concerns about the efficacy of technological protection and the varying responses on how stringent the legislation should be. There was a discussion on

150 Online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/rp00842e.html> (date accessed: 29 March 2003).
151 *Ibid.*

possible exceptions to a law disallowing acts of circumvention. In addition to an enumeration of possible limitations, it considered the wisdom of having itemized exceptions vis-à-vis a blanket authorization allowing all acts of circumvention for legitimate use. Finally, it deliberated the practical implications of monitoring these exemptions once they were implemented. The proposed penalties for violation of the law were also considered, mainly in terms of criminal versus civil sanctions.

The third point dealt with whether to extend legal protection to include a prohibition on devices. Considered was the oft-repeated argument that the Internet Treaties' obligation did not include any device prohibition and the inclusion of such prohibition was unnecessary to comply with treaty obligations. Also acknowledged was the claim that it was impossible for circumvention devices to distinguish infringing from non-infringing uses and that a mere blanket prohibition would let loose a Pandora's box of evils, including stifling research and innovation. Counter-arguments to the claim were also discussed, the main argument being that legal protection against acts of circumvention was insufficient without criminalizing the devices used in circumvention.

The Paper also briefly discussed other issues of concern, mainly privacy and debate of whether the issue was proper and relevant to the proposed legislation.[152]

D. The Report

In October 2002, Industry Canada submitted its report in parliamentary compliance with section 92 of the *Copyright Act* requiring the Minister of Industry table a report within five years of the coming into force of Bill C-32 in September 1997 to initiate a comprehensive review of the *Copyright Act*.

---

152 *Ibid* – "The issue of privacy was also a concern with respect to legal sanctions for TPMs.... Some submissions felt privacy was an important consideration in the context of technological measures, while others felt privacy was always present as a consideration, but irrespective of any particular copyright context."

Under section A.1.15, entitled "technological protection measures," it raised the issue of whether to amend the *Copyright Act* to provide sanctions against persons who use circumvention technologies to infringe copyright by defeating protective technologies such as encryption. The report itself did not give a definitive answer to the question, admitting that while the WCT and WPPT had provisions dealing with this issue the possible approaches to actual legislation were controversial. The report did make clear however that the *Copyright Act* would have to be amended to implement any provisions regarding technological protection measures. The government has tabled the enactment of the law regarding the protection of technological measures under its short-term agenda of 1 to 2 years.

IV Canada's Flawed Model Legislation: the DMCA

A. The Law

1. Purpose of the DMCA

The DMCA is legislation passed in 1997 by then President Bill Clinton in order to implement the United States obligations under the Internet Treaties. America's goals, as seen in their Framework for Global Electronic Commerce, are similar to Canada's own Framework for Copyright Reform. They too "aimed to promote the development of a vast global market,"[153] echoing Canada's words in the Speech from the Throne to "ensure that Canadian laws and regulations remain among the most modern and progressive in the world, including those for intellectual property and competitiveness."[154]

Similar to Canada's own principles specified in the Framework, the core principles of the DMCA, copyright protection in the digital age, sought to stem the flow of unauthorized use from threats not in existence when copyright law was first written. Lawmakers accepted the reality that revolutionary changes in technology have affected the way information is transmitted and disseminated and that doing so has affected copyright law, which deals with the protection "information-based assets."[155]

Echoing the sentiments of some respondent entities in their responses to Canada's Framework questions, copyright owners in the U.S. made the valid point that unlike analog technology in which each successive copy degrades in quality, with digital technology, a copy of a copy of a copy contains the same clarity and integrity as the original of the work. They also pointed out that in the networked environment it was possible to transmit thousands of perfect copies simultaneously across the globe with a single click of a computer mouse. As a result, copyright owners needed greater protections

153 W. J. Clinton & A.Gore, Jr., "A Framework for Global Electronic Commerce" (1997), online: <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (date accessed: 29 October 2002).
154 Gov. Gen. Adrienne Clarkson, "Address," (Speech from the Throne, Senate Chamber, 30 January 2001)online: Government of Canada <http://www.sft-ddt.gc.ca/sftddt_e.htm http://www.sft-ddt.gc.ca/sftddt_e.htm>.
155 G.S.Takach, *Computer Law*, (Toronto: Irwin Law, 1998) at 51 [hereinafter Takach].

to guard against piracy of copyrighted works in the digital networked era.[156] Legislators responded to these demands in an effort to encourage content owners to begin moving their businesses online.[157] They hoped the DMCA would provide strong incentives for companies to roll out digital products with confidence[158] by protecting the environment in which this transfer of information takes place.

2. Implementing Provisions

First, the law prohibits the circumvention of technological measures itself, penalizing the circumvention of any effective technological protection used by a copyright holder to restrict access to its materials. To wit:

> Section 1201(a) 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.[159]

Second, it prohibits the creation of the methods or tools of circumvention, penalizing the manufacture of any device, or the offering of any service, primarily designed to defeat an effective technological protection measures:[160]

Section 1201 (b)[a] and [c] Additional Violations

156 S. Vaidhyanathan, "Putting a lock on e-books: A new cold war looms over your right to read" (2001), online: MSNBC <http://stacks.msnbc.com/news/602444.asp> (date accessed: 8 December 2001) [hereinafter: "Putting a Lock on E-Books"]. – In the above statement the author acknowledges the rationale behind the law, however his paper adopts the position that the law as written is unfair.
157 B. King, "Fight Rages Over Digital Rights" (2001) online: Wired News <http://www.wired.com/news/politics/0,1283,41183,00.html> (date accessed: 1 December 2001).
158 *Ibid.*
159 DMCA, *supra* note 10.
160 DMCA,1201 (b)(1), *supra* note 10.

> "(b) 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 the 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 technical measure that effectively protects the right of a copyright owner under this title in a work or a portion thereof.[161]

Finally, it prohibits those who allow public access to either of the above, penalizing the offering to the public of products or services knowingly created to circumvent protective technologies.[162]

While its purposes might appear noble, its method of implementation is the source of much conflict. It is interesting to note that the Clinton administration's own *White Paper on Intellectual Property and the National Information Infrastructure* stated that U.S. copyright industries were thriving well under the current U.S. legal environment,[163] leading to the conclusion that they already had sufficient protection under the law. In addition, the Internet Treaties did not impose any restrictions as cumbersome as those set out under the DMCA.

U.S. legislators could have easily supported the "predictable, minimalist, consistent and simple legal rules its own Framework Principles called for."[164] Instead, legislators opted to support an "unpredictable overbroad and maximalist set of anti-

---

161 DCMA, *supra* note 10.
162 *Ibid.*
163 B. Lehman, "White Paper," (1995) online: <http://www.geog.ubc.ca/~acitpo/copyright/clinton_whitepaper.html> (date accessed: 20 May 2002).
164 P. Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised, 52 Stan. L. Rev. 1125 (2000)," online: <http://www.sims.berkeley.edu/%7Epam/papers/Samuelson_IP_dig_eco_htm.htm> (date accessed: 2 February 2002) [hereinafter Samuelson1].

circumvention regulations."[165] They scoffed at arguments made by an alliance of consumer electronic firms and by representatives of the computer and software industry about the mischief that broad anti-circumvention regulations would do in this industry.[166] They also dismissed as specious arguments made by library and educational groups about the threats to fair use and public domain arising from broad anti-circumvention regulations.[167]

The resulting law, the DMCA, effectively imposes an absolute and outright ban prohibiting any person from circumventing any technological measures that controls access to copyright works.

B. The Flaws in the DMCA

1. No Distinction between Infringing and Non-Infringing Use

While the purpose of copyright law is the protection of created works against infringement, the DMCA does not directly punish the infringement of copyrighted works, instead it criminalizes the circumvention of protected technology. In stark contrast to the laws on copyright infringement that require willful intent to infringe,[168] the language used in the DMCA is so broad that it applies to any conceivable service or matter containing copyrighted material which contains access controls, whether or not copyright infringement and theft of service are even plausible concerns.[169]

---

165 *Ibid.*

166 *Ibid*, citing testimony of Allan Adler, House Judicial hearing. See also "Statement of Allan R. Adler Vice President for Legal and Governmental Affairs Association of American Publishers before the Subcommittee on Courts, the Internet and Intellectual Property House Judiciary Committee concerning s.487: 'The Technology, Education and Copyright Harmonization Act of 2001' June 27 2001", online: <http://www.house.gov/judiciary/adler_062701.htm> (date accessed: 25 August 2003).

167 *Ibid*, citing Testimony of Michael Kirk, House Judicial hearing. See also "Statement of Michael K. Kirk, Executive Director American Intellectual Property Law Association before the Subcommittee on Courts, the internet and Intellectual Property Committee on the Judiciary United States House of Representatives at the Oversight Hearing on Reexamination May 10, 2001", online: <http://www.house.gov/judiciary/kirk_051001.htm> (date accessed: 25 August 2003).

168 DMCA § 505, *supra* note 10 - "....For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement."

169 "A Protester's Guide to the Digital Millennium Copyright Act" (2002), online: <http://www.tuxers.net/dmca/dmca-guide.html> (date accessed: 18 July 2002).

In simple terms, the mere act of circumvention of any protected technology device violates the law, whether or not the encrypted data contains a passage from the Bible or Stephen King's latest novel. Lawmakers justify this by comparing the decryption to breaking into a locked room to obtain a book.[170] While convincing, the argument is flawed on two accounts, first the "book" analogy fails to differentiate between property, which is tangible and information, which is intangible. Infringement is not the taking of property (which is limited) but of data which is limitless. Thus, while a thief who takes the book that does not belong to him transfers possession to himself and deprives the owner of both the book and all beneficial uses which come from owning the book, one who reproduces a copyright work does not automatically deprive the book's author of its beneficial use. For instance, copying a line from a book to use in a commentary takes little away from its author.

The analogy of the locked room is equally flawed, as it fails to differentiate between the author's exclusive right in a copyrighted work and his absolute right to control his work. While the law grants the author exclusive rights over his work, the law does not grant the author complete control of it. Allowances are made for fair use such as criticism and research, lawful uses which technology devices may prevent. An author is not allowed completely lock-up his work, and those who have lawful right to such work should be able to access it. Through the DMCA an author or his heirs may not only prevent fair use but block access to his work even after the expiration period provided by copyright law. Seen in that light, the locked book analogy seems directly in opposition with copyright principles.

Given the healthy state of copyright industries and the fact there was no need for emergency measures to revive a dying industry, a more sound legislation would be one penalizing the circumvention of a technical protection system for the purpose of engaging in or enabling copyright infringement, as proposed by Silicon Valley Representative Tom

170 B. F. Irwin & E. L. Rubin, *The Digital Millennium Copyright Act and the Internet* (San Francisco, New York City, Chicago: Practicing Law Institute, Patents, Copyrights, Trademarks, and Literary Property, Course Handbook Series, 2001) at 520.

Campell in an alternative bill.[171] This after all, as one critic pointed out, "was the danger that was said to give rise to the call for anti-circumvention regulation in the first place."[172]

The DMCA, by disregarding the intent to infringe, fails to protect against unseen applications and possible misapplications. This problem is compounded by the fact that the exceptions under the DMCA are so confusing they are virtually incomprehensible.

2. Narrow and Confusing Exceptions

While the DMCA does provide limited exceptions to the above provisions in the areas of security testing, encryption research, national security and privacy,[173] these exceptions are narrow and ambiguous, allowing for a myriad of interpretations and abuses by copyright owners.

From the beginning, the creation of the DMCA was filled with controversy. Public interest advocates warned that the law was too strong, that it would stifle research, free expression, scholarship, teaching, and even commerce in new technologies that had yet to emerge.[174] Others believed this was deliberate, that the DMCA was "rushed through Congress by the entertainment industry lobbyists to protect its monopoly on commercially-developed digital content, cartels, price-fixing, and maintaining its status quo."[175] Though the DMCA (through its exemptions) show signs of Congress' visible efforts to pacify its dissidents, many felt that Congress paid little heed to the public concerns at the time and were too busy "making the digital world safe for established software companies and movie studios."[176]

---

171 *Digital Era Copyright Enhancement Act*, H.R. 3048, 105th Congress., Ist Session., Section 8.
172 Samuelson1, *supra* note 164.
173 DMCA § 1201 (j) (g) (e) and (i), *supra* note 10.
174 See D. Bollier, "Stopping the Privatization of Public Knowledge" (2002), online: <http://www.tompaine.com/feature.cfm/ID/6017> (date accessed 16 October 2002); R. Petersen, "Copyright and Electronic Information Access on a Collision Course" (2001), online: <http://www.oit.umd.edu/ITforUM/2001/Fall/fair/> (date accessed 4 November 2002).
175 R. Forno, "National Security and Individual Freedoms: How the Digital Millenium Copyright Act Threatens Both," (2001), online: <http://www.fitug.de/news/horns/horns200701222636.html> (date accessed: 11 December 2001), [hereinafter "National Security"].
176 "Putting a Lock on E-Books", *supra* note 156.

In doing so Congress has left the U.S. with a law, which, though noble in purpose, has been repeatedly shown to have chilling effects on education and research. A law that not only tramples on the fair use rights and the right of freedom of speech but also imperils the very values upon which copyright law is based.

C. Effects of the DMCA

1. Overall Impact

a) Violation of the Right to Free Speech

In this day of copyright protection, one often takes for granted that copyright is not in itself inherent to the author but exists solely through legislative grant.[177] Laws on copyright must therefore not only stay true to its purpose of encouraging innovation but must be wary of trampling heedlessly on the constitutional rights such as free speech.

Free speech, one of the most sacrosanct of rights in the U.S. is protected under the First Amendment of its Constitution, which states:

> Congress shall make no law... abridging the freedom of speech or of press.... [178]

Fundamentally, the right to free speech allows individuals to express themselves without interference or constraint by the government. The Supreme Court requires the government to provide substantial justification for the interference with the right of free speech where it attempts to regulate the content of the speech. A less stringent test is applied for content-neutral legislation.[179]

---

177 *Wheaton* v. *Peters*, 33 U.S. 591 (1834). "Copyright is not a birth right, but a 'wholly statutory' grant."
178 U.S. Const. amend. I.
179 First Amendment: An Overview, online: <http://www.law.cornell.edu/topics/first_amendment.html> (date accessed: 20 January 2003).

Determining whether there has been a violation of free speech is a three-step process. First, one must ask, is it constitutionally protected speech? Second, has there been an abridgement of speech? Third, is the government justified in this abridgement?

In a recent case involving the DMCA, *Universal City Studios Inc. v Corely*,[180] the U.S. Court of Appeals decided the two first questions in the affirmative; it ruled that a computer program that gives a computer instructions is "speech" within the meaning of the First Amendment. The Court ruled that there had been an abridgement of speech though it did differentiate between speech and its "functional ability" which could be regulated without violating the First Amendment. The crux of the contention therefore was whether the government was justified in prohibiting this type of speech under the DMCA. The Court upheld the DMCA, ruling that the law "serves a substantial governmental interest, [which] is unrelated to the suppression of free expression, and ... does not 'burden substantially more speech than is necessary."

The case as decided, disregards one vital fact: the DMCA is, primarily, copyright legislation and all decisions should treat it as such. This means that freedom of speech should not be abridged unless there has been a violation of the laws of copyright, specifically infringement. In the case at bar, no infringement existed or was even alleged, all that existed were software that could be used to decrypt copyrighted works, tools which could be used for both infringing and non-infringing purposes. By preventing access to all tools of circumvention whatever its use (ie. fair use, research etc.), the Court went beyond the boundaries of copyright. Further, it provided copyright holders with complete control over their works, in direct contrast to the U.S. Supreme Court's decision in *Twentieth Century Music Corp.* v. *Aiken*[181] where it opined that Congress granted a limited monopoly to copyright holders that had to be balanced against the public interest and a broad public availability to creative works. The decision is also in opposition to the principles laid out in *Sony Corp.* v. *Universal City Studios, Inc.*,[182] where the Supreme Court held that "copyright ... protection has never accorded the copyright owner complete

180 (2001), 273 F.3d 429,2d Cir [hereinafter *Corley*] – Discussed in more detail *infra* at note: 355, 356 and accompanying text.
181 422 U.S. 151 (1975).
182 464 U.S. 417 (1984).

control over all possible uses of his work. Rather, the *Copyright Act* grants the copyright holder 'exclusive' rights to use and to authorize the use of his work in five qualified ways, including reproduction of the copyrighted work in copies."[183]

In *Corley*, the Appellate Court treats the technological measures in the DMCA as more than merely a means to prohibit infringement. Instead, through the DMCA, the Court has essentially provide the copyright owner complete control over all uses of his work. Copyright principles like fair use and exceptions for research and study are ignored, upsetting the delicate balance established between the copyright owner and public welfare which is the cornerstone of copyright law. In testament to this, the Appellate Court essentially adopted the Lower Court's distinction with respect to §1201(c)(1)[184], concluding "that fair use is not a defense to the use of, or trafficking in, circumvention devices, but only to infringing uses of copyrighted works after such works are obtained."[185] It concluded that the DMCA targets circumvention only, and "does not concern itself with the use of ... materials after circumventions has occurred."[186]

Equally confusing is the Appellate Court's ruling that technological measures might be protected under the DMCA because of their "functional ability" which does not constitute a violation of the First Amendment. Yet in *Sega v Accolade*,[187] it was precisely because of this reason that the Supreme Court allowed the copying. The Court held that the 'S-E-G-A' activation key was functional and not protected by copyright. The Court stated:

> "Where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for

183 *Ibid.*
184 Note Supra 10, - "Other Rights, etc., not Affected – (1) Nothing in this section shall affect the rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."
185 *Corley, supra* note 180 at 30-31.
186 *Corley, supra* note 180 at 31.The court went on to say that the Appellants' trafficking in circumvention devices, the Court concluded, amounted neither to circumvention of a pre-determined class of works protected by §1201(a)(1), nor to infringement of a copyrighted work, the fair use of which is protected by §1201(c)(1). Accordingly, the fair use defense was inapplicable to appellants' violation of the DMCA.
187 *Sega, supra* note 14.

> seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."

DMCA is copyright law, yet it is the "functional ability" of these technological measures that are protected, even though they are not copyrightable and within the realm of public domain free speech.[188]

If the DMCA is true copyright legislation then is it not be bound by the limits proscribed by copyright law? Since copyright law is a statutory limitation on the right to free speech, copyright only exists to the extent its use is protected by law. Use of the speech being the determining factor, the doctrine of "fair use" was developed to deal with the tension between free speech and copyright protection.[189] By asserting that the provisions of the DMCA legitimately prohibited the act of circumvention whether or not the act was done in accordance with the rights of fair use, the Appellate Court allowed the DMCA's reach to extend beyond the boundaries of copyright law and upset the balance. The DMCA in *Corley* remains essentially unchecked, conferring upon the owners of encryption devices the right to prevent any type of copying, without the countervailing right of society to legitimate use of these works.

b) Violation of the Right of Fair Use

Under section 107 of Title 17 of the U.S. Code, the fair use of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research are allowed under certain conditions.[190] The fair use doctrine has long been in

---

188 See M. Karsten, "Functionality Doctrine" (2001), online: <http://zork.net/pipermail/free-sklyarov/2001-September/004128.html> (date accessed: 26 June 2002). "I believe the "functionality doctrine" is a very good reason why the DMCA is not a proper exercise of a valid congressional power. In the copyright context this lives in the idea/expression dichotomy and the merger principle, both of which are Constitutional limitations. A patent is the only government security that can protect functional ideas."

189 S. Zimmermann, "A Regulatory Theory of Copyright: Avoiding a First Amendment Conflict" (1966) 35 Emory L.J. 163 at 165.

190 Under U.S. law, the factors used to determine fair use are:

(1) Purpose and character of the use, including whether such use is of a commercial nature or is for
(2) Nonprofit educational purposes;
(3) Nature of the copyrighted work;
(4) Amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

existence under U.S. law. Derived from the right of free speech, the doctrine emphasizes the necessity of promoting "the Progress of Science and the useful Arts" (U.S. Constitution, Article 1, 8). The fundamental nature of fair use is underscored in the words of Justice O'Connor:

> "The author's consent to a reasonable use of his copyrighted works had always been implied by the courts as a necessary incident of the constitutional policy of promoting the progress of science and the useful arts, since a prohibition of such use would inhibit subsequent writers from attempting to improve upon prior works and thus . . . frustrate the very ends sought to be attained."[191]

Yet Section 1201 (a) of the DCMA as written threatens to make "fair copying" obsolete. The law is based on the assumption that all circumvention technology is aimed at the infringement of copyright and that any person who "provides"[192] anti-circumvention technology by any means disseminates an evil with no noble purpose. Consequently, the language of the law is sweeping, prohibiting the circumvention of any technological protection measure that guards access to copyright work, for whatever reason it is created. There is no requirement under Section 1201 that the circumvention be for the purpose of infringing a copyright or using the work for commercial purposes. Under this provision, any action of circumvention without the consent of the copyright owner is criminalized,[193] whether or not copyright law gives the owner the right to exclude the use of such copyrighted work.

Commentary and research, two well-accepted limitations to copyright law are especially at risk. In fact, the wording of the DMCA[194] seems designed for the express purpose of allowing private parties to suppress legitimate public debate about their products. It serves little purpose that section 1201 (c)(1) the DMCA does not limit the

---

(5) Effect of the use on the potential market for or value of the copyrighted work.
191 *Harper & Row* v. *Nation Enterprises,* 471 U.S. 539 (1985).
192 DMCA,1201 (b)(1), *supra* note 10.
193 *Ibid.*
194 *Ibid* at (a)(1)(A): "No person shall circumvent a technological measure that effectively controls access to work protected under this title...."

defense of fair use or other defenses to copyright infringement[195] since the law does not punish infringement but circumvention.

Moreover, any exceptions provided by the DCMA permitting the circumvention of technological protections are so narrowly restrictive they do little more than cloud the issue. The provision exempting research, for instance, allows the research[196] but does not automatically allow the dissemination of that research,[197] leaving the researcher with work he can neither benefit from nor publish. Another provision provides that, in order to benefit from an exception, security testing must have authorization from the creator producer.[198] Thus, anyone wanting to test the security of computer software held out to secure must first obtain permission from the author before reverse engineering any software.

The exceptions also ignore many legitimate non-infringing uses. A cryptographer, for instance, might suspect that another person is infringing his work. The only way to test his assumptions would be to bypass the encryption scheme of the suspected work to assess the material. Since reverse engineering this software neither reveals flaws not directly

---

195 *Ibid* at (c)(1), reproduced *supra* note 182.

196 *Ibid* at (g)(2) Permissible Acts of Encryption Research – Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance or display of a published work in the course of an act of good faith encryption research if –

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of published work;
(B) such act is necessary to conduct such encryption research;
(C) the person made a good faith effort to obtain authorization before circumvention; and
(D) such act does not constitute infringement under this title of a violation of applicable law other than this section, including 1030 of title 18...."

197 *Ibid* at (g)(3) Factors in Determining Exemption – In determining whether a person qualified under the exemption under paragraph (2) [*supra* note195], the factors to be considered shall include –

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section including a violation of privacy or breach of security,'
(B) whether the person is engaged in legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology; and
(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is approved."

198 *Ibid* at (J)(1): "Definition – For the purposes of this section the term 'security testing' means accessing a computer, computer system or computer network, solely for the purpose of good faith testing, investigating or correcting a security flaw or vulnerability, *with the authorization of the owner or operator* of such computer, computer system, or computer network." (emphasis supplied).

improves the state of encryption,[199] then under the DMCA, the owner is not allowed to do so. A law meant to protect against copyright infringement thus has unwittingly become a pawn in its favor. Stranger still, because computer viruses are software programs and thus copyrightable expression, if a virus writer were to use encryption to hide the code of a virus then, theoretically, since it is not encryption research as defined[200] an anti-virus company is forbidden from reverse engineering the encryption wrapped around the virus without permission.

In addition, while traditional copyright law punishes the violation of the copyright owner's exclusive rights,[201] the DMCA proceeds a step further by criminalizing the creation of any tool that allows a copyrighted work to be copied if the copyright holder has used encryption to protect the work and reverse engineering is needed to make the copy. The law is comparable to one penalizing locksmiths on the principle that some of his keys are used for breaking into locked doors;[202] or, to draw a parallel in copyright law, prohibiting the manufacture of photocopying machines because some of them are used to infringe literary works. The simple truth is that merely providing the means to commit a crime, whether it be infringement, trespass or murder, does not automatically result in liability. If the opposite were true then no keys, photocopy machines, or guns would ever be produced.

In example of the above, Russian cryptographer Dimitri Skylarov and Elcomsoft were indicted for selling AEBPR solely because the device could be used to break into Adobe's E-Book reader. It is of little importance that AEBPR was also used by parents who download books to move them to their children's computers, or by those who needed

---

199 *Ibid* at (g)(1)(A) "the term 'encryption research' means activities necessary to identify the flaws and analyze the vulnerabilities of encryption technology applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."
200 *Ibid.*
201 See Title 17, United States Code, § 106 and § 501.
202 A penalty the U.S. Supreme Court held as invalid. See *Harris* v. *State*, 790 S.W.2d 778(1990). "[A]... necessary element of the offense with which appellant was charged is that the instrument in question constituted a criminal instrument... testimony showed that the key has lawful uses." See also *Eodice* v. *State*, 742 S.W. 2d 844 847 (1987); and *Nobby Lobby, Inc.* v. *Dallas,* 767 F. Supp. 80 (1992).

to access the books by "unconventional" means such as braille output devices and specialized screen readers.

By criminalizing circumvention tools, it becomes superfluous to ask, "is it fair use?" since the mere manufacture and sale of the tools for public distribution is a violation of the law. This includes entities permitted to circumvent copy-protection schemes such as nonprofit libraries, archives, and educational institutions. [203] Since the DMCA bans equipment and services designed to enable circumvention, the prohibition of the manufacture, import, and use of tools necessary to enable circumvention essentially annuls the means to legitimately obtain access to a work for legitimate use, even if allowed by the DMCA itself.

The DMCA also dilutes the potency of landmark Supreme Court decisions such as *Sega v Accolade*[204] and *Atari v Nintendo of America Inc.*[205] In each case, the Court found that reverse engineering was fair use, even though verbatim copies of the entire code for a game or game console were made as intermediate copies in the reverse engineering.

While there is a reverse engineering exemption under section 1201(f) of the DMCA, it is narrow, limited[206] and when combined with other provisions of the DMCA, might as well not exist. In fact, in *Universal City Studios, Inc.* v. *Reimerdes*,[207] the U.S. District Court of New York rejected the applicability of section 1201(f) to reverse engineering of DVDs, disregarding *Sega*, *Atari* and copyright principles. In its surprising decision, the District Court concluded that "*fair use is not a defense to violations of the DMCA.*"[208] The Court applied a plain meaning construction to section1201(c)(1) and determined it preserved fair use as a defense to *copyright infringement only*, while the

203 DMCA, §1201(d) and § 404, *supra* note 10.
204 *Supra* note 13 at 31.
205 (1992), 975 F.2d 832.
206 See §1201(f) DMCA, *supra* note 10, which permits engineering with respect to computer programs to achieve interoperability under certain circumstances to the "extent any such acts of identification and analysis do not constitute infringement under said title."
207 F.Supp 2d 294 (SDNY 2000) [hereinafter *Reimerdes*].
208 *Ibid* at 321 "If Congress had meant the fair use defense to apply to such actions, it would have said so."

defendants in this case were guilty of circumventing technologies that protect copyrights, not of infringing copyrights themselves.[209] Finding this distinction determinative, the Court reasoned that Congress could have explicitly allowed a fair use defense to anti-trafficking actions under the DMCA, but failed to do so, which meant that no such defense could be had outside of the limited exception crafted solely for section 1201(a)(1)(A).[210] [211]

A worrisome trend is developing from decisions such as *Corley* and *Reimerdes*, and threatened actions against researchers like Dimitri Skylarov; a trend that is eroding the principles of fair use, the cornerstone of copyright law, and the very scales that balance the rights of the owner with the rights of society. As for the outcome of such unjust legislation, there is little need to speculate, the effects are already evident.

2. Overall Impact of the DMCA

a) Unfair Advantage

One of the most profound effects of the DMCA is the newfound ability of software companies to render their products immune to criticism. Skylarov, for instance, was arrested for developing and selling products designed to circumvent Adobe E-Book's security measures. His talk was a technical discussion on how Adobe used an easily cracked algorithms and a weak encoding system.[212]

Adobe's E-Book security is marketed as a 'secure' feature of its product. Anything contrary to that marketing claim threatens its market influence and corporate profits. Hence, corporations such as Adobe immediately invoke intellectual property claims to protect their vulnerable positions whenever someone makes a verifiable public claim.

---

209 *Ibid* at 322.
210 Supra, note 10. "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."
211 "Universal City Studios, Inc v. Corley: the Constitutional Underpinnings of Fair Use Remain Open to Question," online: Duke Law and Technology Review <http://www.law.duke.edu/journals/dltr/articles/2002dltr0003.html> (date accessed: 15 February 2003).
212 "National Security", *supra* note 175.

The difficulty of battling large corporation with their deep pockets and battery of lawyers is undisputed. Now, using DMCA as a sort of a U.S. federal litigant welfare program, these same corporations receive free support of the federal government, turning U.S. taxpayer assets - federal agents, attorneys, and paralegals - into *de facto* temporary help for the company, hired to fill the position of "Copyright Cops" as part of the "Corporate Censorship Brigade."[213] Under DMCA, both the entertainment industry and software vendors use federal law enforcement agents as a federally funded extension of their corporate legal office. With DMCA in place, corporations do not have to pay exorbitant outside counsel fees to litigate such cases, the government will do the job for them.

b) Elimination of Competition

The DMCA also creates a harsher environment for newer companies, preventing other start-up corporations from building competing devices or software, vying for the favor of the consumers in the free market. Instead their creators are threatened and the software censored and driven underground. Before the DCMA disallowed anti-circumvention technology, reverse engineering was a common way to improve technology or make use of a similar idea, as long as the expression of the idea was not reproduced.

With the advent of the DMCA, copyright owners now possess unrestricted authority to determine the extent of protection provided to a work, irrespective of any limitations otherwise provided for by statute. They have a monopoly of rights akin to that of a patent but even more so because, while in patent law the idea is made available to the public, under the DMCA the very act of breaking encrypted software and offering it to the public is in itself a crime, whether or not it is viewed or used. Yet the Supreme Court, in allowing reverse engineering in *Sega*, opined:

---

213 *Ibid.*

> "[I]f disassembly of copyrighted object code is per se an unfair use, the owner of the copyright gains a de facto monopoly over the functional aspects of his work - aspects that were expressly denied copyright protection by congress...."[214]

Under the DMCA, copyright owners enjoy an unassailable means of maintaining a patent-like monopoly on their expression: encryption. In such a case, even though the use of the expression is permissible under copyright law, the act of decryption is punishable.

As succinctly written by a critic of the DCMA, "since these companies can't eliminate that right legally, because it would violate too many of the fundamentals of our society, they are restricting the technology so this right cannot be exercised. In the process they are violating the fundamentals on which a stable and just society is based."[215]

c) Uncertainty in Scientific Research

On September 2001, a music industry group sought to test the security of a handful of watermarks by establishing a contest for cryptographic researchers. A cash prize was offered to those who could break the codes. A team of researchers led by Princeton University computer science professor Edward Felten accepted the offer and broke the code but did not to accept the cash, deciding to publish their results instead. The music industry group threatened against the presentation of the code-breaking paper, warning that publication would violate the DMCA.[216] In the end, Felten decided it was safer not to release his paper and pulled it out of circulation.

---

214 *Sega*, *supra* note 14.
215 National Security, *supra* note175.
216 "Academic Freedom and the Digital Divide" (2001), online: CFIF.ORG <http://www.cfif.org/5_8_2001/Free_line/current/free_line_academicfreedom.htm> (date accessed: 12 December 2001).

Arguably, since the DMCA has provisions exempting fair use,[217] Felten could have continued with his publications and pleaded the exception if sued by the music industry group. Such a line of reasoning however seriously mischaracterizes the practical reality of lawsuits between individuals and corporations. The fact is that it matters little whether corporations have a winnable case, with their deep pockets all they need is a reason to file suit; the DMCA has given them that reason. This problem is aggravated by the fact that while provisions in the DMCA allow for exemptions, the exemptions are so limited and the wording of the law so vague and encompassing that it opens the door, providing corporations with sufficient ground to file frivolous suits against any researcher who breaks their code. It does not take any stretch of the imagination to conclude that most researchers will act similarly to Felten and will simply stop researching and publishing their work. That is the reason why the U.S. Supreme Court has ruled that:

> "A statute will be considered unconstitutionally vague 'if it fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute... and if it encourages arbitrary and erratic arrests and convictions....'"[218]

In words of anti-DCMA org coordinator Mark Smith, "you shouldn't have to hire a lawyer to make sure you are not breaking a law."[219]

The scales are already tilted in favor of large corporations, considering most researchers of encryption and software controls are academics and students with little money or manpower to fight a court case. This is not a situation of Microsoft cracking Adobe's software where Adobe stands to win a sizable amount in addition to major press coverage. The simple fact of the industry is that security vulnerabilities are found by individuals and small groups of hackers-- the people without the deep pockets to fend off a lawsuit or hire lawyers to review research prior to its release.

---

217 DMCA, 1201(c)(1), *supra* note 10.
218 *Carrasco* v. *State,* 712 S.W.2d 623 (1984). See also *Goocher* v *State,* 6 SW.2d 860 1982).
219 R. Lemos, "Security workers: Copyright law stifles," CNET News.com (2001), online: <http://news.cnet.com/news/0-1003-200-7079519.html?tag=tp_pr> (date accessed: 1 December 2001) [hereinafter "Copyright Stifles"].

"That pretty much turns the question of publishing into a business decision," Fred Cohen stated, explaining the withdrawal of his evidence gathering software called Forensix,[220] "from a risk-management standpoint, I can't afford to deal with the issue. Some big businesses can afford to sell the product. I can't."[221] With Skylarov's arrest and detention the "risk" increased tenfold; the U.S. government made clear that researchers may be deprived of their liberty as well as their property for publishing research in violation of the DMCA.

d) Stifling Innovation and Promotion of Inferior Products

Copyright industries, and the software industry in particular, "have thrived under a regime of partial intellectual property protection and robust criticism and competition."[222] Yet, the draconian criminal measures imposed for violation of section 1201 have become the single most effective measure in deterring individuals from conducting bona fide forms of science and technology research that are fundamental to innovation. In doing so, the DMCA stifles not only the growth of the technological sector but makes it easier for corporations promote inferior products. Dutch encryption expert Niels Ferguson's paper "Censorship in Action"[223] is a prime example of this.

On August 15 2001, Ferguson discovered a major flaw in that Intel's encryption scheme for Firewire connections, known as the high-bandwidth digital content protection (HDCP) system. He was about to publish his works when he heard of Skylarov's arrest and decided not to publish his findings. "I travel to the U.S. regularly, both for

220 "EFF Whitepaper: Unintended Consequences," online: Electronic Frontier Foundation <http://www.eff.org/IP/DMCA/20020503_dmca_consequences.html> (date accessed: 11 December 2002).
221 "Copyright Stifles", *supra* note 220.
222 J. Cohen "Call it the Digital Millennium Censorship Act" (2000), online: The New Republic Online <http://www.thenewrepublic.com/cyberspace/cohen052300.html> (date accessed: 14 December 2001).
223 N. Ferguson, "Censorship in action: why I don't publish my HDCP Results" (2001), online: MacFergus <http://www.macfergus.com/niels/dmca/cia.html> (date accessed: 12 December 2001) [hereinafter "Censorship in Action"].

professional and for personal reasons," he said in an online statement. "I simply cannot afford to be sued or prosecuted in the U.S."[224]

Corporations are in the business of profit- their aim is to reach the market before their competitor. The DMCA provides them with the opportunity to litigate away their vulnerabilities instead of taking the time to ascertain whether what they advertise as a secure product is in fact so. With the advent of the DMCA, it has become easier to threaten action against those who want to publish the flaws in their product than to provide for security testing which requires a more scarce expertise.[225]

"Under the DMCA," Jay Dyson, Senior Security Consultant for Treachery Unlimited observes, "we are now in a situation wherein those who point out that the Emperor's New Clothes are nonexistent are the ones who will be punished; not the self-proclaimed 'tailor' of such illusory raiment." [226]

The examination and peer review of technologies, especially those used in protecting privacy and security, are crucial to consumer protection; the only other option would be to assume all claims made by the seller are accurate. Corporations are in effect coercing the consumer to "trust" their claims because the consumer does not have the legal right to reverse engineer the product and test its vulnerabilities. This is unacceptable.

Scientists like Ferguson, Felten and Skylarov are the guardians of information protection, reliability and security. By circumventing access technologies, they are able to underscore shortcomings in security systems and in doing so force vendors to examine and address flaws in these products marketed to the public as secure products. If companies like Microsoft, Intel and the RIAA were truly concerned about consumer welfare, they would applaud these researchers instead of condemning them, accepting this

---

224 *Ibid.*
225 While security testing is allowed under Section 1201(g) of the DMCA, it must be done with the consent of the owner. DMCA, *supra* note 10.
226 J. Dyson, "Ugly Mistake for Pretty Good" (2001), online: Treachery Unlimited <http://www.treachery.net/articles_papers/crypto.html> (Date accessed: 9 December 2001).

type of "ethical hacking"[227] as a service; a means for them to improve their product for the sake and safety of the public,[228] and perfect the product before it is attacked by "unethical hackers." Yet, rather than redefining themselves, maintaining their standing in the digital market through creativity and quality products and services, through the DMCA corporations can now preserve their status by mounting an all-out legal attack against anyone advancing new models.[229]

D. The Future under the DMCA

If critics of the DCMA are to be believed, the future under the law looks decidedly grim. Fundamental freedoms such as free speech, the cornerstone U.S. Constitution, will eventually be eroded. Copyright principles, such as fair use, shaped from centuries of experience, will be rendered obsolete, throwing the delicate balance between society and the copyright owner into chaos.

The result will be a society where technology moves at a turtle pace because of corporate monopolies and the elimination of competition; where scientists, unwilling to face litigation, choose not to publish their papers or research; where flawed products used to protect the most sensitive information are peddled as completely secure.

Even more troubling is the extensive reach of the DMCA, including the right to hold Internet Service Providers (ISPs) liable for hosting a site with offending information. Although the law has been crafted to protect ISPs and web-hosting sites from any responsibility, this protection does not shield them from suit once they are given knowledge of the offending site refuse to remove it.[230] Should the ISP or web host choose

227 See V. Capello, "Being a Hacker" (1999), online: <http://www.astalavista.com/library/basics/guides/beinghacker.shtml> (date accessed: 9 December 2001).
228 J. Mathesson, "Fair Use is Dead" (2001), online: Computer User <http://www.computeruser.com/articles/daily/8,6,1,0427,01.html> (date accessed: 9 December 2001).
229 National Security, *supra* note175.
230 *Cubby Inc.* v. *Compuserve, Inc.*, 776 F.Supp. 135 (1991).

not to shut the site down, it may be treated as an accessory to the transgressing site, and subject to criminal and civil punishment.

Fortunately, Canada has the option of choosing a different path. Extensive study of its obligations under the WIPO, careful analysis of the ill effects DMCA, and a full understanding of its own copyright policy should enable Canada to create protection technology legislation which fulfills its obligations under the Internet Treaties yet remains faithful to the *Canadian Charter of Human Rights and Freedoms*[231] and to copyright principles, allowing it to maintain the delicate balance between the different stakeholders of copyright law.

231 R.S.Q. c. C-12 [hereinafter the *Charter*].

V Anti- Circumvention Technology Legislation in Canada

A. The Questions:

1. Groundwork: Raison *d'etre* behind Canadian Copyright Law

In using the DMCA as a basis of comparison for Canada's own copyright legislation, it is essential to recognize that U.S. and Canadian laws do not stem from identical value systems. Consequently, it is only by determining their differences that it is possible to distill the essence of Canadian legislation, which in turn will determine how to proceed with future copyright legislation (and anti-circumvention) legislation.

a) The Rationale of Copyright

Copyright is defined as the exclusive right of the author or creator of a literary or artistic property to print, copy, sell, license, distribute, transform to another medium, translate, record or perform or otherwise use and to give it to another by will.[232] Copyright law is the protection of these rights by punishing unauthorized use or infringement. The law's protection extends only to the expression of the work, and not to the ideas, which remain in the public domain.[233]

While the reasons behind copyright law protection are complex, the simplest explanation is that copyright is considered property and thus protected by law. However, because "intellectual property" is intangible, it is not property in the traditional sense. It is the ephemeral nature of intellectual property that is the root of its problems.

---

232 "Copyright," online: Law.com <http://dictionary.law.com/definition2.asp> (date accessed: 17 April 2002).
233 *Moreau* v. *St. Vincent* (1950), 1950 C.R. 198 at 203. "An elementary principle of copyright law [is] that an author has no copyright in ideas but only in his expression of them. The law of copyright does not give him any monopoly in the use of the ideas with which he deals or any property in them, even if they are original. His copyright is confined to literary work in which he has expressed them. The ideas are public property, the literary work is his own."

Tangible property is capable of exclusive possession; in fact, the ability to exclude was the traditional basis of ownership.[234] Mere ownership of a tangible object allows its owner to exclude others from its possession.[235] The same does not hold true for intangible objects. There is no natural scarcity in information-based products, which by their very nature can be available to everyone. A thousand people singing the same song at once, for instance, is an example of simultaneous possession of a single intangible object. Unlike tangible property therefore, intellectual property protection such as copyright must rely solely on the law to give creators a monopoly over their creations. Furthermore, since the exclusion is fictional, this exclusion creates complexities non-existent in ownership of tangible properties.[236]

Accepting the supposition that the scarcity of intangible property is one made exclusively by law, the question becomes, *why does law protect the owners of intangible property*? There have been various legal, social, economic and political theories to explain copyright, though in essence, it must be because there will be some benefit (whether it be moral or economic) to protecting the dissemination of information and allowing creators to profit from their endeavors.

Consequently, the tension of copyright exists in protecting copyright holders sufficiently to encourage them to continue creating but not becoming so stifling that the law undermines the values it seeks to protect. Legislators must continue to walk that tightrope, balancing the needs of the creator on the one hand and society on the other. When creating new copyright legislation, lawmakers must ensure that these laws do not suffer from over-breadth, or impede the very purpose for which copyright laws were created.

---

234 Takach, *supra* note 155 at 52.
235 *Ibid.*
236 While both intangible and tangible property have a bundle of rights attached to their ownership, their natures tend to diverge because property is limited while intellectual property is not. Theft of property for instance is limited to stealing a book. Copyright infringement of the same book involves questions such as: what if the thief did not steal the book but copied a few sentences? Or what if he does not steal the book but uses the ideas in the book? Or what if he uses the ideas in the book as a springboard for a new set of ideas?

b) Divergent Histories: Canada and the U.S.

(1) Canada

Copyright began in Canada as early as 1709 with the enactments such as the statute of Anne.[237] However, it was only in 1842 that the *Copyright Act* was passed, effectively replacing its predecessors.[238]

Canadian copyright history, much like the rest of its past is relatively less turbulent than its US counterpart and "remained largely in step with Britain."[239] The Federal Parliament was given the exclusive domain over copyright as early as 1867.[240] Nevertheless, in 1872 attempts at Canadian copyright legislation were disallowed by the U.K. Parliament. Further attempts at copyright legislation were made in Canada in 1868, 2872 and 1875; however Canada's exclusive federal legislation was not created till 1924. Until that time imperial and provincial legislation, in force during that period, continued to apply. Canada's early legislation, mostly from Imperial Britain, remained limited to specific categories of works. [241] This fragmented body of works taken together formed Canada's copyright regime. In fact, only the *Copyright Act* of 1842, which applied broadly to literary works, holds some semblance to today's *Copyright Act*.[242]

In 1911, Britain amended its own *Copyright Act*, providing therein that dominion states such as Canada were free to repeal all existing Imperial copyright laws that applied within the Dominion to date. Britain's new copyright provisions gave impetus to the Canadian Parliament to repeal all Imperial copyright legislation and enact its own copyright law, known then and now as the Canadian *Copyright Act*. Having come into force in 1924, the *Copyright Act* maintained, as it does now, exclusive jurisdiction over

---

237 A. Birrell, *Seven Lectures on the Laws and History of Copyright in Books* (New York: G.P. Putnam's Sons, 1899), as reprinted (New Jersey: Rothman Kelley, 1971).
238 *Ibid.*
239 S.Handa, *Understanding the Modern Law of Copyright in Canada* (1997), McGill Thesis, McGill University Institute of Comparative Law at 70 [hereinafter Handa1].
240 Constitution Act 1867, (U.K.), 30 & 31 Vict c., c 3 s. 91(23), reprinted in R.S.C. 1985, App II, No. 5.
241 Handa1 at 70, *supra* note 239.
242 *Ibid* at 70.

copyright. A law modeled after Britain's *Copyright Act* of 1911, it continued the tradition of Britain's theoretical stance and hard rules.[243]

Two points are worthy of note in Canada's copyright history. First, copyright in Canada "is a creature of statute and the rights and remedies it provides are exhaustive."[244] Second, while Canadian copyright law aims mainly to protect economic rights, it is heavily influenced by the French *droit de auteur,*[245] which is more concerned with the rights of the author then the economic value of the work.[246] The Canadian *Copyright Act* has evolved into "an author-based statute, i.e. rights flow from the creator of the work."[247] Such preference towards the author can be seen in the *Copyright Act* itself which has continued to expanded author's rights.[248]

(2) The United States

Like Canada, the United States too had its origins in British law; since both were British colonies it was logical that their copyright laws mirrored Britain's own. However, by 1786, all the U.S. states except Delaware had enacted their own copyright legislation.[249] Official federal recognition of intellectual property arrived when the U.S. later on enacted Article 1, Section 8 of its Constitution giving Congress rule over Intellectual Property by stating that Congress had the power:

---

243 *Ibid* at 73.
244 *Compo Co.* v. *Blue Crest Music Inc.* (1980), 1 S.C.R. 357, at p. 373; *R.* v. *Stewart* (1988), 1 S.C.R. 963; Bishop v. Stevens (1990), 2 S.C.R. 467, at p. 477.
245 French translation of the *Copyright Act*, supra note 2.
246 Moyse, Pierre-Emmanuel. "La nature du droit d'auteur : droit de propriété ou monopole ?" (1998), 43 McGill L.J. 507. "It is an exclusive right and, as it applies to the part that relates to the commercial exploitation of the work, a true monopoly on reproduction. . . . Canadian law inherited that aspect while remaining receptive to the French doctrines, particularly because of Quebec's influence."
247 Handa1, *supra* note 239 at 73.
248 Such as the definition of performance under the *Copyright Act* which has widened to include "any acoustic or visual representation of a work, performer's performance, sound recording or communication signal, including a representation made by means of any mechanical instrument, radio receiving set or television receiving set." *Copyright Act*, *supra* note 2.

249 P. Goldstein, *Copyright's Highway*, (New York: Hill and Wang, 1995) at 51 [hereinafter Goldstein].

> To promote the progress of science and the useful arts, by securing for limited times to author and inventors the exclusive right to their respective writings and discoveries.

Aside from providing a concrete constitutional basis for U.S. copyright, the provision also imparted the ideology that "the power to enact laws concerning copyright derives from a utilitarian mindset,"[250] a marked difference from the Canadian *Copyright Act*, which is a more complex combination of theories and ideals.

In response to this new directive under the Constitution, the American Congress enacted the federal *Copyright Act* in 1790.[251] Though based in statute (much like its Canadian counterpart), the debate and Supreme Court decisions about unpublished works added a common law aspect to American copyright law. In *International News Service* v. *Associated Press*,[252] the U.S. Supreme Court extended intellectual property to uncopyrightable materials based on the common law notion of "unfair competition" or the notion that one should not reap where one has not sown. The case illustrates of the tension between America's utilitarian belief of economic freedom and its theories about individual rights and privacy.

In 1870, The U.S. *Copyright Act* was consolidated, then again overhauled and revised in 1874.[253] Despite the many changes however, foreign authors were not granted any protection of their work until 1891 under the *Chase Act*,[254] since legislators believed that any foreign protection would be contrary to American interests. Even the *Chase Act* did little to aid the foreign authors, requiring them to apply with all the formalities required of domestic authors such as registration and providing copies for deposit, and requiring the work be typeset in the U.S.[255] These stringent requirements continued till 1989 when the U.S. joined the *Berne Convention*. Worthy of note is the fact that as net

250 Handa1, *supra* note 239 at 60.
251 1 U.S. Stat. 124.
252 248 U.S. 215 (1918).
253 T.E. Scrutton, *The Law of Copyright* (London: Willima Cloes and Sons Limited, 1903) at 51.
254 *Ibid* at 229.
255 *Ibid.*

c) Conclusion: The Essence of Canadian Copyright

(1) Before the Consultation Paper

Canadian copyright history has lead to a form of legislation that is as unique as it is complex. Unlike the U.S., whose utilitarian core was clear from the beginning (that the purpose of the law was to promote the progress of scientists and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries), Canada "lack[ed] a similar purposive mission statement in its law."[263] Historical turn of events has unfortunately left Canada without a clear theoretical model. Consequently, Canadian copyright at present remains a miscellany of theories and concepts, incorporating into its law both its diverse background and the influences of America, Britain and France. The multifaceted nature Canadian copyright is explained thusly:

> "At its most basic level, Canadian copyright law does not derive from a singular underlying theory of protection. It is more complex. It is pluralistic. Theories of property, liberty and privacy each contribute to the basis of the law. To some degree these theories are complimentary, whereas in other cases they conflict."[264]

The recent case of *Théberge* v. *Galerie d'Art du Petit Champlain Inc.*,[265] resulted "out of the conceptual differences between the *droit d'auteur* of the continental *civiliste* tradition and the English copyright tradition." At issue was whether art galleries transferring authorized reproductions of painter's works from paper-backed posters to canvas for purposes of resale "copied" artist's works and whether the new artistic work was produced "in any material form" within meaning of s. 3(1) of *Copyright Act*. The

---

263 *Ibid* at 150.
264 S.Handa, *Copyright Law in Canada*, (Ontario: Butterworths, 2002) at 70 [hereinafter "Copyright Law in Canada"].
265 (2002) 2002 SCC 34, online: <http://www.lexum.umontreal.ca/csc-scc/en/rec/html/laroche.en.html> (date accessed: 6 April 2003).

Supreme Court, which found that the respondent was in fact asserting a moral right in the guise of an economic right, held there was no infringement on the part of the art galleries.

In its decision, the majority characterized the *Copyright Act* primarily as a statute economic in nature, emphasizing that it had been traditionally more concerned with economic rather than moral rights. [266] Taking a bright line traditional approach, the Court opined that Parliament intended for two separate structures to exist under the Act, one for economic rights the other for moral rights.[267] The purpose of moral rights was limited, existing only "only if the work is modified *to the prejudice of the honour or reputation of the author* (s. 28.2(1))."

In his dissenting opinion, Justice Gonthier took a decidedly different view of the *Copyright Act*. He opined that, contrary to being a purely economic statute, Parliament intended:

> "...to establish both a right that is centered on the person of the author, this being derived from the civil structures of the right of ownership, and a definitely dynamic right centered on its economic function, which reflects the theories underlying the concept of monopoly ."[268]

He also opined the moral rights concepts espoused by the majority were in fact inapplicable and that the case should to be determined solely from the aspects that derive from the English concept of copyright.[269]

The justices were split 4 to 3 in their decision, indicative of the Court's continuing struggle to reconcile complex and at times contradictory theories of copyright law.

---

266 *Ibid.* "[Canada's] original Act, which came into force in 1924, substantially tracked the English *Copyright Act, 1911* (U.K.), 1 & 2 Geo. 5, c. 46 at par 12. The principal economic benefit to the artist or author was (and is) the "sole right to produce or reproduce the work or any substantial part thereof in any material form whatever" (s. 3(1)) for his or her life plus fifty years (s. 6). The economic rights are based on a conception of artistic and literary works essentially as articles of commerce. (Indeed, the initial *Copyright Act, 1709* (U.K.), 8 Anne, c. 21, was passed to assuage the concerns of printers, not authors.)"

267 *Ibid* at par 59. "Separate structures in the Act to cover economic rights on the one hand and moral rights on the other show that a clear distinction and separation was intended. "

268 *Ibid* at par 116.

269 *Ibid* at par 121.

(2) After the Consultation Paper

The Consultation Paper is the government's first in-depth discussion of the "core" of Canadian copyright, at least in relation to the digital environment. In a section called "Implications for Copyright Policy", the government stated:

> The *Copyright Act* serves to promote and protect intellectual expression, as well as encourage and enable access to and dissemination of such expression. It achieves this by granting various rights and exceptions, including the right to reproduce works, the right to communicate works to the public by telecommunication, and the right to authorize these acts.

The statement is a reflection of Canada's history as well as how, in light of its reliance of many legal theories, the importance of the general principles of balance and fairness are emphasized more than any one set of factors.[270] Equally apparent is the government's emphasis on the balancing of interests, the protection of intellectual expression and access and dissemination of the work. Economic rights are not underscored as much as knowledge as a value to be both protected and disseminated.

In applying these principles to future anti-circumvention law, it is important for lawmakers to strive to achieve the balance emphasized in the policy. The government must ensure that any legislation prohibiting acts of circumvention allow for both the protection of copyrighted works and the protection of the right to circumvent when legally justifiable. It must ensure that preventing access to copyrighted works does not unduly impede legitimate access to these works. Consequently, before embarking on the drafting of any law, it is paramount that legislators take into consideration all other the factors that will be affected by an anti-circumvention statute Like pieces of a jigsaw puzzle, Canada's

---

270 See Consultation Paper, *supra* note 7 at 6. In fact in stating the issues the government stated that it was concerned with a number of fundamental questions such as:

> What are the appropriate balances in the digitally networked environment?
> Does the environment created... upset these balances?
> If so, does it do so in such a way as to impede legitimate dissemination of content information?

international treaty obligations, *Charter*, criminal, civil and copyright statues and even the mindset of its citizens all have a potential impact on the digital copyright equation; determining the scope and breadth of future legislation. Only when legislators are fully cognizant of all sides of the equation can they draft anti-circumvention legislation fulfills Canada's obligations yet is consistent with the policy of copyright stated in its Consultation Paper.

2. Obligation: Our Obligation under the Internet Treaties

a) The Law:

As discussed in length in Chapter I, the obligations of a member state under the WIPO are to 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.*"

b) Enumeration of Canada's WIPO Obligations

Framework of Protection - The provisions were drafted to provide national and regional legislators with a general framework for the protection of technological measures.[271] It is a push to give circumvention devices support under legislation.

No New Substantive Rights – The Internet Treaties themselves do not enumerate any new substantive author's rights, nor do they give authors a way to enforce copyright. Instead, the Treaties provide protection to copyright through the protection of encryption technology by providing that legal remedies be set in place against its circumvention.

---

271 "WIPO Treaties 1996" *supra* note 35 at 142.

Importance of Balance - The word "adequate" appears indicative of the balance that domestic legislator must strive to maintain. The law must be one sufficiently strong and meaningful to serve its purpose but not so draconic that it places an undue burden on other relevant industries.[272]

Effective Redress - The term "effective legal remedies," is the logical outcome of "adequate legal protection." The phrase necessarily implies that the rightholders must have a right of redress in the law and that this redress must, to be effective, be "expeditious so as to prevent circumvention and abuse and dissuasive so as to constitute a deterrent to further circumvention and abuse."[273]

No Set Definition of Circumvention - What is considered "circumvention" (i.e. acts of circumvention carried out deliberately or the acts primarily to violate copyright law) is a matter left to the member states. All that Article 11 provides is "minimum protection.

Preparatory Acts - Preparatory acts of circumvention are not in themselves prohibited by Article 11, not being acts of circumvention themselves. This means that domestic legislators have no obligation to declare illegal the manufacture, distribution or possession of devices or components made for circumventing protection technologies.[274]

3. Balance: Issues Important to Individuals and Entities under the Framework

a) The Starting Point

272 *Ibid.*
273 *Ibid.*
274 CF Marks &Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences' in: WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty and the WIP Performances and Phonograms Treaty," WIPO doc WCT-WPPT.IMP/3 p6.

After reviewing the comments of both individual respondents and respondent entities on the issues raised in the Consultation Paper, Industry Canada and Heritage Canada released their summary of the these responses in a paper called "An Overview of Submissions on the Consultation Paper on Digital Copyright Issues."[275] They defined these responses as "starting point for introducing this issue was the definition provided in the WIPO Treaties."[276] They opined that the crux of the argument was the degree of regulation sufficient to constitute an "adequate" level of protection and an "effective" level of remedy, as well as on what would be an "effective" technological measure. With technological protection measures (TPM's) as their focus point, they proceeded with their summary of the stakeholder submissions, reproduced here for clarity in table form.

b) Key Issues and Arguments

Issue	Arguments of Those In Favour Of TPMs	Arguments of Those Opposed to TPMs
Access Control of Technological Protection Measures	1. Controls are essential to ensuring authorized use. 2. Controls are essential for the development of all online dissemination schemes, including e-commerce, and encouraging rights holders to make content available online.	1. Legitimate possession for authorized uses does not require access controls. 2. Too much control will hamper innovation and research, and discourage access to works. 3. Control will amount to the creation of a new right with no corresponding policy balance, and potentially without expiry. 4. Control will have a potential negative effect on access extending to altering the mandate under Copyright law of institutions such as libraries and archives.
	1. Circulation of works on digital networks are easy, thus ownership of the rights in works would risk becoming meaningless if acts of circumvention are not prohibited.	Disallowing acts of circumvention only makes sense if the legal protection is recognized for copyrighted works to begin with; otherwise, technological protection

275. Online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/rp00842e.html> (date accessed: 29 March 2003).
276 *Ibid.*

Prohibiting Acts of Circumvention	2. Without some protections, the ability to disseminate works digitally worldwide would be unchecked. Furthermore, some protections are necessary to create friction or disincentive to the easy, illegitimate dissemination of works. 3. Much current circumvention is done for commercial purposes.	measures used for non-copyrighted works would create a blanket prohibition that would extend, for example, to works in the public domain or to currently legitimate uses and exceptions.
Importance of the Inherent Quality of Technological Protection Measures	No matter how good the technology it will always be inadequate to the continuous new ways to circumvent it. Therefore, there must be laws to protect the technology.	1. A strong system will be robust enough to withstand circumvention, and that it is a matter of investment in security resources rather than in legal measures to achieve a measure of protection that will discourage most potential infringers. 2. Creators of inferior technological protection devices use copyright protection to protect their technology instead of improving the technology. 3.Clear definition of these measures should be adopted, with further criteria for legitimate circumvention, in order to protect against spurious applications that may qualify as 'anti-circumvention measures" simply from their nature as digital code.
Canada vs. Countries with TPM Legislation	Canada's anti-circumvention provisions should be consistent with other jurisdictions in order to avoid creating a "haven" for circumvention in Canada.	1. Current measures in effect in the United States under the DMCA constituted a serious disincentive to research and development in certain fields of study. 2. Canada stands to gain from the current difference in laws between Canada and the U.S. because it would attract researchers in encryption and other computing science fields.
Legitimate Access	1. There should be a blanket prohibition against circumvention of TPMs and the *Copyright Act* should enumerate the exceptions to the law. 2. Admission: The need for	1. Instead of exceptions, there should be other mechanisms put in place by rights holders to ensure access for all legitimate uses beyond authorized uses. 2. Flexibility is necessary to ensure

	flexibility is important to allow for legitimate access to the works (agreeing with those opposed to legal protection that there should be access to works for legitimate purposes). 3. Exceptions like fair dealing, should continue to apply. However, the right to legitimate access of the works can be accommodated within any regime that recognizes this new layer of protection.	circumvention for legitimate purposes. 3. Circumvention is necessary for non-copyright reasons such as to ensure interoperability and privacy, education and research.
Enforcement	Admission: Intent should be an important part of any prohibition on devices, and it should be limited to the purpose of copyright infringement (agreeing with those who opposed such legal protections on the basis that without intent the law was too powerful and a threat to innovation and research).	1. The law should define which acts of circumvention are carried out solely for the purpose of infringement. Such definition could be extended to circumvention devices, but should be clearly associated with the purpose or intention of the act and not simply with the act itself. 2. It may be easier to define "infringement" than a "technological measure," which means it is easier to define circumvention when the intention of infringement ties the act explicitly to the underlying copyright legislation.
Outlawing Devices	1. Protecting against acts alone would not be enough to provide "effective" protection required by the Internet Treaties. 2. Legal protection against acts of circumvention are insufficient protection without protecting at the same time against the devices that may be used in circumvention. 3. Limiting the availability of devices would make the prohibition on acts more effective, and without a reasonable assurance of maximum protection, the potential for rapid dissemination of copyrighted works remains strong.	1. Not part of the Internet Treaties' obligation, and so should be evaluated strictly on its own policy merits 2. Risks an evolution towards 'authorized' devices, which goes beyond the scope with copyright law since under copyright law, the work is copyrighted and not the device used to access it. 3. Prohibition against devices that may have non-infringing purposes is debilitating and unfair for research. 4. Impossible for circumvention devices to be able to distinguish infringing from non-infringing uses. Rights holders have recourse already under the current *Copyright Act* both against acts of circumvention and against manufacturers

		of devices.
Penalties	1. Without accompanying legislation, TPMs cannot sustain their function to prevent the broad and rapid dissemination of works online. 2. In order to be effective, legal protections must allow for criminal as well as civil penalties.	1. Criminal sanctions are excessive for this type of activity because as circumvention is endemic to many computer activities including study and research, a criminal penalty would identify many computer users as criminals. 2. Proposed Solution: a purpose or intention to infringe component should be essential to criminal liability
Fundamental Rights	Privacy is always present as a consideration, but that irrespective of any particular copyright context.	1. Protection of TPMs can affect free speech and access to cultural heritage, including the public domain. They may also affect copyright-related protections such as the right of first sale and fair dealing. 2. Ownership of a legitimate copy of a work allows enjoyment of that work in a device or platform of the user's choosing according to the policy objectives of Canada's copyright regime. 3. Individuals right to privacy are violated when they are forced to accept cookies in order to access or use certain services on the internet. 4. DMCA-type legislation requires a high degree of monitoring of citizen behavior, which make privacy concerns more prominent. 5.The DMCA makes it illegal to publish or demonstrate the weaknesses of encrypted software, a clear violation of free speech.

B. Canadian Legal Environment

Before creating new anti-circumvention laws to comply with Canada's WIPO obligations, legislators first need to purvey the existing Canadian legal environment, taking into consideration the following factors: first, the scope of existing legislation. Existing laws, individually or jointly, may result in the control of access to technological

measures or the protection of technological measures in fulfillment of Canada's obligations under the WIPO. Should there be a need for new legislation, either because present law is insufficient or there are gaps that need to be filled, it must be read in tandem with the existing laws and be tempered accordingly.

Second, certain fundamental rights are affected. Anti-circumvention legislation may inadvertently diminish the rights granted under the *Charter*, which should be avoided not only to prevent the law from being struck down by the courts but so that even if the law is upheld, it will continue to operate within the spirit of the Charter and will not ultimately result in depriving Canadians of their fundamental freedoms.

1. Existing Legislation

a) Canadian Copyright Act

Computer programs are protected through various intellectual property regimes such as semi-conductor chip laws or even patent, however these programs find their most comprehensive protection under the *Copyright Act*. Section 2 of the *Act* specifically extends copyright protection over computer programs by classifying them as literary works.[277] This allows creators of these programs the right to make copies of the work and prohibit others from infringing upon that right by making unauthorized copies.[278]

It is exclusive in its sphere, providing explicitly that "no copyright or similar right shall exist in Canada other than the *Copyright Act*."[279] While the increase of digitized works lead to a corresponding uncertainty on whether a new type of legislation was needed to handle this new technology, the Copyright Subcommittee (the "Subcommittee") of the Information Highway Advisory Council (IHAC), indicated in their report that the

277 *Copyright Act*, § 2, *supra* note 2.
278 H.G. Fox, "*The Canadian Law of Copyright and Industrial Designs 2nd edition*," (Toronto: Carswell, 1967) at p.2 [hereinafter Fox]. "The essential characteristic [of copyright] is the sole right to produce or reproduce any such work or any substantial part thereof in any material form whatsoever."
279 *Copyright Act*, § 63, *supra* note 2.

"existing definitions in the *Copyright Act* are sufficient to protect the digitization of works. [280] They maintained that since copyrighted works are afforded protection "in any material form whatever,"[281] no new copyright law was required.

The basics of copyright protection in Canada remain as they have for more than a 100 years. To receive copyright protection, work must fall within one of the established categories under section 5(1) of the *Copyright Act*, which include original literary, dramatic, musical and artistic works.

Canadian law requires no registration or marking requirement for to be copyrightable as copyright subsists from the moment of creation of the work.[282] The term of protection exists for the life of the author plus fifty years.[283] The author of the work is presumed to be the owner of the copyright except if the work was commissioned in accordance with the Copyright Act[284] or done in the employment of another.[285]

The works must also fulfill the traditional requirements of: originality[286] referring, in general terms, "to the degree of author's creative or inventive thought"[287]; fixation, meaning the work must be "expressed in some material form capable of identification, and having more or less permanent character."[288] Note that where fixation was not explicitly required by the *Copyright Act*, it has been inferred as existing by the courts."[289] Though the concepts behind the terms themselves have changed, especially with the advent of

---

280 Subcommittee Report, *Copyright and the Information Highway: Preliminary Report of the Copyright Subcommittee* (Ottawa: Information Highway Advisory Council Secretariat, 1194) [hereinafter Subcommittee Report].
281 *Copyright Act*, § 3(1) *supra* note 2.
282 *Copyright Act*, § 5, *supra* note 2.
283 *Copyright Act*, § 6 & 9, *supra* note 2.
284 *Copyright Act*, § 13 (2), *supra* note 2
285 *Copyright Act*, § 13 (3), *supra* note 2.
286 *Copyright Act*, § 5, *supra* note 2. Copyright shall subsist in Canada, "in every original literary, dramatic, musical, artistic work...."
287 Handa Sunny, "*Reverse Engineering Computer Programs under Canadian Copyright Law*," (September 1994), McGill Thesis, McGill University Institute of Comparative Law. See also Copyright Act § 5, *supra* note 2.
288 J.S. McKeown, "*Fox Canadian Law of Copyright and Industrial Designs 3rd Edition*" (Ontario: Carswell, 2000) at 200 [hereinafter "Fox1"].
289 *Canadian Admiral Corp. Ltd v. Rediffusion Inc.*, (1954), E.x. C.R.382 at p. 394 – "for copyright to subsist in a 'work' it must be expressed to some extent at least in some material form, capable of identification and having a more or les permanent endurance."

digitization, they remain the basis of determining whether copyright subsists over certain works.

Infringement of copyright occurs when "any person who, without the consent of the copyright owner, does anything that by the *Copyright Act* only the owner of copyright has a right to do."[290] There are a limited number of exceptions to infringement which have been explicitly enumerated under the *Copyright Act*.[291]

Despite the immovable facade of copyright law however, the *Copyright Act* has not been stagnant. Since its introduction as federal legislation in 1924, it has undergone several revisions by means of various amendments to respond to the technological and social changes in Canada.

In 1988, for instance, amendments created exhibition rights for artistic works, improvements in moral rights, a new Copyright Board, as well as additional criminal sanctions, and eliminated compulsory licenses for recording musical work. More significantly, it provided protection for computer programs, expressly designating the programs copyrighted works. After the NAFTA in 1989, further changes were made to ensure that cable and satellite companies paid royalties for retransmissions. Another significant change took effect in 1993 when the *Copyright Act* was amended to included graphic and acoustic representations as musical works and ensured broadcasters, televisions and cable system operators were liable for royalties. [292]

One of the latest changes was the enactment of Bill C-32[293], which altered the *Copyright Act* by reinforcing neighboring rights and providing owners additional rights for performances of their work. More importantly in terms of protection of circumvention technology, and it introduced a "blank tape levy" on anyone buying blank tapes,

290 *Copyright Act*, § 27, *supra* note 2.
291 *Copyright Act*, §29.4 to 30.6. Discussed *infra*, note 310 to 312 and accompanying text.
292 See J. Melnitzer, "New Copyright Leaves Some Work Undone," Law Times (15 September 1997) at 1017. See also Copyright Act § 2 and §19 respectively, *supra* note 2.
293 Canada's Bill C-32 and Archival Research, online: Achive Society of Alberta <http://www.archivesalberta.org/dec96/c32.htm> (date accessed: 23 March 2003).

videocassettes, CDs or anything else holding a recording. [294]. It also strengthened the powers of the Copyright Board, which has become a major force of copyright legislation in Canada.

The existence and decisions of the Copyright Board assist in clarifying any ambiguities regarding infringement, posting up web content, computer programs and other matters. Their decision expands the interpretation of existing law, allowing the law to remain current with existing technology. In its report[295] in 1997, for instance, it extended the *Copyright Act's* definition of "communications to the public" to include information available "on demand." The report stated that whether this information was by email, newsgroup or other form as long as it was performed "outside a domestic setting" it was a communication to the public.[296] Though these tribunals do not carry the same weight as courts, they play a major part in ensuring that copyright law is not mired by traditional definitions.

While no specific anti-circumvention provisions exist within the *Copyright Act*, the owner of encrypted data may still find recourse within its provisions, not because of the presence of specific directives but because of the lack of them. Two primary examples of such deficiency are reverse engineering and fair dealing, which will both be discussed in detail below.

(1) Reverse Engineering and Section 30.6

Protection technology is mostly "cracked" through reverse engineering, which is the process of "going backwards from a finished product and determining how the product works,"[297] to obtain access to the encrypted works within. When reverse engineering a

294 "The Latest on the Recordable Media Levy," online: PC Buyer's Guide.com <http://pcbuyersguide.com/hardware/storage/cdr-levy.html> (date accessed: 28 January 2003).
295 Information Highway Advisory Council (IHAC), *Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council* (Ottawa, Industry Canada, 1997) [hereinafter The Report].
296 *Ibid* at 444.
297 *Sega, supra* note 14, at 1441.

computer program, a machine called the decompiler[298] disassembles the encrypted data. Before doing so however, the decompiler must first load a copy of the program into another computer that it will use to disassemble said program. This first act of copying could logically be categorized as infringement, since it is technically unauthorized copying of the work.

The disassembling computer continues the decompilation by making passes over the program it is seeking to reverse engineer, producing multiple copies of the program each time in simpler language as it breaks down the complex code. The series of simpler code may also be considered as translations[299] of the work, and thus infringement under Section 3(1)(a) of the *Copyright Act*.

In *Atari*,[300] the U.S. Supreme Court settled the question of whether such acts gave rise to an action for copyright infringement when it ruled that such "intermediate copies[301] constituted fair use and were therefore not infringing. However, there has been no counterpart decision in Canada. Compounding such uncertainty is the fact that, while U.S fair use provisions are broad, Canada's fair dealing provisions provide a definite and arguably exhaustive list.

The *Copyright Act* has recently[302] addressed the issue of reverse engineering, allowing for limited copying and reverse engineering of computer programs under Section 30.6:

> **30.6** It is not an infringement of copyright in a computer program for a person who owns a copy of the computer program that is authorized by the owner of the copyright to:

298 See D. I. Bainbridge, "Computer Programs and Copyright: More Exceptions to Infringement", (1993), 56 Modern Law Review 591, at 593. "A decompiler converts the machine code version of the program into a high level language."
299 *Apple Computer Inc.* v. *Mackintosh Computers Ltd* (1986), 10 CPR (3d) at 20-21, 28 DLR (4th) 178 (FCTD).
300 *Atari Games Cop* v. *Nintendo of America Inc.*, (1992) 975 F. 2d 832 at p 842.
301 *Ibid.*
302 1 September 1997.

> (a) make a single reproduction of the copy by adapting, modifying or converting the computer program or translating it into another computer language if the person proves that the reproduced copy is:
>
> (i) essential for the compatibility of the computer program with a particular computer,
> (ii) solely for the person's own use, and
> (iii) destroyed immediately after the person ceases to be the owner of the copy; or
>
> (b) make a single reproduction for backup purposes of the copy or of a reproduced copy referred to in paragraph (a) if the person proves that the reproduction for backup purposes is destroyed immediately when the person ceases to be the owner of the copy of the computer program.

On the one hand, the provision allows for reverse engineering for purposes of interoperability and allows for the maintenance of a backup copy, both of which are essential to computer programming. However, the section is so restrictive, it is almost impossible to copy (and thus reverse engineer) the software for any other purpose.[303] In fact, by enumerating with minute specificity the circumstances under which reverse engineering can take place, the provision may have effectively outlawed all other types of copying of computer programs.

It is arguable therefore that given 1) Canada's fair dealing provisions and limitations under section 30.6; 2) the lack of any Supreme Court decisions on the legality of reverse engineering and 3) the technological protection demands on Canada under the WIPO; reverse engineering may very well be considered an infringement of copyright if brought before Canada's Supreme Court today.

There have been numerous arguments made in favour of reverse engineering, and few can question its role in maintaining software compatibility, computer security testing

303 S.Handa, "Reverse Engineering Computer Programs under Canadian Copyright Law" (1995) 40 McGill L.J. at 621- 642. "Although it can be argued that section 27(2)(1) [now Section 30.6] protects against a computer program's use being declared as infringing, it is more tenuous to argue that this section also applies where a program is copied into RAM and subsequently onto more permanent media for the purposes of dissection by a disassembler, a necessary step in the disassembly of a computer program."

as well as in research and development. In passing any legislation on circumvention technology therefore, legislators must consider both reverse engineering's importance and its vulnerability under Canada's laws. It would also be prudent for legislators to consider the chilling effect the DMCA has had in reverse engineering, despite the U.S's expansive fair use principles, its decisions legitimizing reverse engineering and the reverse engineering exceptions within the DMCA itself.

(2) Fair Dealing

Similarly, owners of encryption software may find protection under Canada's fair dealing provisions, not because of any specific section in their favour but because of the law's explicit limitations on what constitutes legal copying.

Akin to the U.S's fair use, the *Copyright Act's* fair dealing provisions establish freedom from liability for copyright infringement in certain instances. Though both laws have striking similarities, such as exemptions for news reporting, research, private study or criticism, they remain two divergent pieces of legislation. The heart of the difference lies in the fact that fair use is "a statutory recognition of a judge-made rule."[304] As a result, the language[305] used under the fair use doctrine is expressly permissive; the listed enumerations not limitations as much as mere examples of fair use exemptions.[306] In determining whether fair use exists, legislature has given the courts the discretion to

304 Fox1, *supra* note 288 at 547, citing Nimmer on Copyright at 130-150.

305 17 USCS §107 (2002). Limitations on exclusive rights: Fair use- Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include--

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

306 17 USCS § 107 (2002). "... for purposes such as criticism, comment, news reporting, teaching...." The words "such as" is a clear indication of the permissive language of the law.

determine which activities are permissible and which are not.[307] In doing so the court may consider various factors, such as the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use on the potential market, as well as any other factors it sees fit to include.[308]

In contrast, fair dealing under *Copyright Act* is a product of statute, and contains provisions that are specific, express, and limited in scope. The list is exhaustive, as the use made of the work must fall within one of the stipulated categories – research, private study, criticism or review or news reporting.[309] Specific exceptions are also made for educations institutions, libraries, archives and museums,[310] and more recently, computer programs.[311] Further, the actions must be undertaken without motive of gain[312] before the "infringer" can raise the fair dealing defenses under sections § 29, 29.1 and 29.2 of the *Copyright Act*[313]. While courts are given authority to determine what is "fair," their decision is limited to the categories provided under the law.

In addition (or perhaps as a result of the above), there have been only a few cases of note under Canadian law,[314] a sharp contrast from the rich body of judicial decisions concerning fair use under U.S. law. Such scarcity makes it difficult predict the sentiment of the Canadian judiciary in the arena of fair dealing.

There is little doubt that the provisions on fair dealing are more favourable to copyright holders than fair use. Fair dealing's exhaustive list of exceptions remove a number of arguably legitimate reasons for infringing copyright to circumvent encrypted technology. Copyright infringement of a computer program to obtain interoperability and security testing, for instance, are not exempted under fair dealing, unless of course it also

---

307 See *Campbell* v. *Acuff-Rose Music Inc.*, 510 U.S. 576 (1994). "...the role of the courts is to distinguish between biting criticism that merely suppresses demand and copyright infringement, which usurps it.
308 17 USCS § 107 (2002). "In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include...."
309 *Copyright Act*, § 29 to §29.2, *supra* note 2.
310 *Copyright Act*, § 29. 4 and §30.1 to §30.3, *supra* note 2.
311 *Copyright Act*, § 30.6, *supra* note 2.
312 *Copyright Act*, § 29.3, *supra* note 2.
313 *Supra* note 2.
314 I.e. *Allen*, *supra* note 16, *MCA Canada* v. *Gillberry & Hawke Advertising Agency* (1976), 28 CPR 2d 52 (FCTD).

fits into the exempted categories of research or private study.. More importantly, fair dealing provisions do not allow intermediate copying necessary to reverse engineer encrypted material even if it would result in obtaining work exempted under the said provisions. Should a library, for instance, desire to make a copy of a currently encrypted journal,[315] it would have no right to reverse engineer the work to enable it to do so. The library's only legal option would be to ask for the encryption key from the copyright holder who, in turn, has no obligation to provide it.

Library and archival groups echo similar concerns in responding to the questions posed by the Framework,[316] apprehensions that legislators should consider before enacting any anti-circumvention legislation. Failure to resolve these issues may result in legislation, which, by controlling legal access to the work, defeats the entire purpose for which the fair dealing provisions were enacted. This in turn may result in fair dealing principles that have become little more than antiquated provisions without power to affect real world dilemmas.

Such sentiment is reflected by the IHAC committee, which, while stating that "there appears to be no need to import into Canadian fair dealing concept elements as contained in the U.S. fair use provisions"[317] cautioned that:

> "given the growing concerns regarding the future of technology, the government should review the situation on a regular basis to ensure that the fair dealing provisions are appropriate the context of the information highway."[318]

In light of Canada's obligations under the WIPO, it may be time for legislators to re-evaluate Canada's fair dealing legislation.

315 An act permitted under Section 30.2 of the *Copyright Act, supra* note 2.
316 Framework, *supra* note 1.
317 Information Highway Advisory Council, *Copyright and the Information Highway: Final Report of the Copyright Subcommittee*, (Ottawa: Supply and Services Canada, 1995) at 31.
318 *Ibid.*

b) Bill C-32 – Blank Media Levy

In 2000, Bill 32-C[319] introduced a levy on blank media in Canada to compensate music artists for lost royalties due to the copying of music by individuals. The notes on the provision read as follows:

> "Pursuant to Part VIII of the *Copyright Act*, every person who for the purpose of trade, manufactures a blank audio recording in Canada is liable to pay a levy on selling or otherwise disposing of that medium in Canada...."

The Copyright Board is responsible for setting the levy rates and deciding to which forms of media the levy applies. The Canadian Private Copying Collective (CPCC) is the body in charge of proposing the new tariff rates and collecting the levy paid by all manufacturers and importers of blank media in Canada. The CPCC then distributes the monies collected, less any administration fees, to registered artists. The CPCC has recently[320] proposed substantially higher rates for the levy and asked it be applied to a larger range of media, including Mp3 players, memory cards (including flash cards), and DVD-R/DVD-RW.[321]

While the Bill does not directly provide for protection against anti-circumvention technology, it nevertheless provides a plausible alternative to penalizing circumvention by charging a fixed rate on all blank tapes and distributing these fees to the authors and publishers. In doing so, the Bill achieves the same end as anti-circumvention legislation, preventing the use of copyrighted works without compensation. The law neither allows nor encourages piracy,[322] but admits to the truth that first, most blank media is copying copyrighted work and second, that piracy does exist and will continue to exist despite laws

319 Bill C-32, *An Act to amend the Copyright Act*, 2d Sess., 35th Parl., 1996 cl 8 [hereinafter The Bill].
320 It proposed new levy rates and scheme in the year 2003.
321 "Blank Media Levy," online: <http://www.sycorp.com/levy/> (date accessed: 19 February 2003).
322The Blank CD-R Tax FAQ, online: <http://neil.eton.ca/copylevy.shtml#copy_for_friends, citing footnote 4 of a Copyright Board Ruling> (date accessed: 01 March 2003). "Section 80 does not legalize (a) copies made for the use of someone other than the person making the copy; and (b) copies of anything else than sound recordings of musical works. It does legalize making a personal copy of a recording owned by someone else."

that forbid it.[323] Therefore, instead of controlling access to circumvention devices or creating unreasonable barriers to prevent any form of copying, the Bill's solution is to charges a fee for all blank media bought in Canada.

Placing the levy squarely in the context of circumvention technology protection, a person downloading movies or music from the internet would be unable to reproduce another copy (other than the one on his hard drive) without paying for that copyrighted work because any blank media purchased to copy the "pirated work" on would be covered by a tariff. The copyright holders would therefore be compensated for any economic loss suffered because of the "piracy." In fact, a future alternative might be to expand Bill 32-C further and place a significant tariff on the encryption devices themselves, other than just the blank media on which the disks are recorded.

Clearly, the Bill is not a panacea for all copyright ills in the digital domain, nonetheless it appears to strike a better balance between copyright owner and user. Admittedly, the levy is similar to the DMCA in the sense that it takes a "shotgun approach" to the problem of infringement, effectively penalizing all persons buying blank media, whether or not they use said media to infringe copyright. However, it is not nearly as invasive as the DMCA, at most, users will be charged a few cents,[324] infinitesimal compared to the cost of court fees, thousands of dollars in penalty and the possible loss of liberty under the U.S. alternative.

The rationality and balance of the law is evidenced by the public's response to the levy. While the DMCA has been greeted with a frenzy of anger in the U.S., both proponents and opponents of the levy agree, "piracy in understandably a problem and

---

323 *Copyright Board's Decision, Private Copying 2001-2002*, online: <http://www.cb-cda.gc.ca/news/c20012002fs%2De.html> (date modified: 07 July 2001). "Before the Copyright Act was amended in 1998, copying any sound recording for almost any purpose infringed copyright, although, in practice, the prohibition was largely unenforceable. The amendment to the Act legalized private copying of sound recordings of musical works onto audio recording media - i.e., the copying of pre-recorded music for the private use of the person who makes the copy. In addition, the amendment made provision for the imposition of a levy on blank audio recording media to compensate authors, performers and makers who own copyright in eligible sound recordings being copied for private use."

324 "Blank 'Audio' Media Levy?" online: <http://www.musicbymailcanada.com/article2.html> (date accessed: 02 March 2003)."$0.60 per blank audiocassette of 40 minutes or more." [hereinafter "Blank Audio"].

most consumers would accept a reasonable compensation scheme."[325] Accordingly, despite the constant bickering about the amount of the levy, the notion of the levy itself is generally considered a good idea.[326]

Though the levy has a finite coverage and alone may be inadequate to fulfill Canada's obligations under the WIPO, it covers many of the "gaps" which may in turn allow Parliament to enact a less stringent, less all encompassing, less DMCA type legislation.

c) Criminal Code[327]

As cyberspace law is relatively new ground, Canadian legislators have remained fairly conservative in acting on any perceived need for specific criminal legislation directed at novel wrongdoings characteristic of the computer age.[328] Legislators are particularly cautious in the area of criminal law since "criminalization is generally reserved for conduct that is demonstrably harmful and not simply a nuisance.[329] Nevertheless, technology specific provisions do exist in the *Criminal Code* and as cyberspace continues to pervade modern life, new laws will arise to meet the challenges of technology.

Two relatively new additions, section 342.1 (unauthorized use of computers) and section 430 (mischief to data)[330] reflect Parliament's need to enact laws specifically for

---

325 *Ibid.*
326 T. Trottier "Canada Blank Media Levy Only Benefits the US" (2003), online: <http://www.straightgoods.ca/ViewLetter.cfm?REF=1071> (date accessed: 13 March 2003). "The notion of a levy on blank media to compensate various creators is a good idea. But the proposed levy is so high (e.g. 59 cents on a CDR that costs 20 cents wholesale) that Canadians will have a very strong incentive to buy their media from the U.S., because the price, even with shipping, will be less than 20% of the price in Canada. This will only get worse as media gets cheaper and more spacious because the proposed levy is a flat rate that varies with the number of bytes stored. The levy should be a small percentage of the cost."
327 R.S.1985, c. C-46.
328 R. W. Davis & S. C. Hutchison, *Computer Crime in Canada: An Introduction to Technological Crime and Related Legal Issues* (Ontario: Carswell, 1997) at 163 [hereinafter "Computer Crime in Canada"], at 160.
329 *Ibid*, quoting the English Law Commission which has adopted the view that new crimes should only be created where (1) the behaviour in question goes beyond that which might be properly addressed by civil law (2) no other, less drastic means of redress is available, (3) the new offence must be enforceable.
330 *Criminal code of Canada,* R.S. C. 1985, c. C-46.

the misuse of computers. Even more relevant are sections 342.1(d)[331] which is aimed at "ensuring that the criminal law is available to protect the integrity of encryption regimes,"[332] and section 342.2 which (in the manner provided under the *Criminal Code*) prohibits the possession of circumvention devices used to commit the offences under section 342.1.

These provisions are explained in detail below.

(1) Unauthorized Use of Computer

Under Part IX of the *Criminal Code* entitled "Offenses against Rights of Property:" [333]

> **Unauthorized Use of Computer**
>
> 342.1 (1) Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
>
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

331 Enacted in 1997. See *Criminal Code of Canada*, R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.
332 Computer Crime in Canada, *supra* note 328 at 168.
333 R.S. C. 1985 c C-9.

The section creates three separate offences relating to the unauthorized use of a computer service or system,[334] all of which may also be used by copyright holders to prevent the circumvention of protection technology. For any argument to prosper however, the circumventor must be acting fraudulently and without the colour of right.

Fraud occurs when there is a dishonest act in the sense reasonable people familiar with normal business dealings in such things would find them dishonest.[335] The mental elements of fraud further require the subjective knowledge 1) of the prohibited act and 2) performance of the prohibited act could have as a consequence deprivation, including pecuniary interest or other. [336] The expression "without the colour of right" is "frequently found in Canadian criminal law provisions creating property offences."[337] It allows the accused to use as a defense the fact that "he or she had some legal right to engage in conduct said to constitute the offence."[338]

Section 342.1 (a) creates the offence of fraudulently obtaining a computer service. Computer service is defined to include matters such as data processing and the storage and retrieval of data.[339] As an anti-circumvention measure, this section may provide, among others, a right of action against those who offer encrypted software on the internet.

For instance, Company A allows its members to download music at its site for a fixed monthly fee. The music is accessed by the members who have been given the decryption code. Should a non-member illegally break the code and download the music, he may be guilty under this section for obtaining a computer service.

---

334 D. Watt & M. Fuerst, *Tremeerar's Criminal Code* (Ontario: Carswell Publishing,1996).
335 *R* v *Zlatic* (1993), 79 C.C.C. (3d) 466 (S.C.C).
336 *R* v. *Théroux* (1993),19 C.R. (4th) 194, 79 C.C.C. (3d) 449 (S.C.C.).
337 Computer Crime in Canada, *supra* note 329 at 163.
338 *Ibid* at 163, citing *R* v *Jones* (1991), 66 C.C.C. (3d) 512 (S.C.C.).
339 *Criminal Code* Section 342.1 (a), definition of computer service, R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.

There are two matters worthy of note in this section. First, the action will not prosper unless the service is able to prove it has suffered some form of deprivation,[340] thus free services may find it difficult to prosecute under this section unless it is able to prove it has suffered some tangible loss. Second, as the statute is new, courts will be inclined interpret it narrowly, they may for example, hold liable only those directly responsible for the crime. In the case of *R* v. *Forsythe*,[341] the defendant was employed as a former officer in the Edmonton Police service. He was accused of brining with him a civilian who could access the computerized online services of the Canadian Police Information Computer (CPIC) criminal recorders. This material was then alleged to have been provided to the defendant in a printout form. The judge ruled that contrary to the prosecution's allegation, Forsythe had not "obtained the computer service," that is, the CPIC record access. While the Judge acknowledged that the defendant obtained the computer printout, he believed that Parliament did not intended to make criminal all those who come into possession of these CPIC printout. He stated that the aim of the law was to catch only those who actively obtained them in a fraudulent manner.[342]

Section 342.1 (b) penalizes directly or indirectly intercepting any function of a computer system, through electro-magnetic, acoustic, mechanical or other devices. A computer system, in turn, is defined in the section as "a device... that (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other functions."

As an anti-circumvention measure, this provision can be used to allow copyright holders the right of action against illegal circumvention of copyrightable material available for a specific purpose online (as this arguably intercepts the function of the computer system).

340 See *supra* note 336, which describes deprivation as an element fraud, fraud being necessary for an action to prosper under Section 342.1 of the *Criminal Code*.
341 *R* v *Forsythe* (1991), 137 A.R. 321 (Prov Ct.).
342 *Ibid* at 321. "As pointed out earlier, s 342.1(1)(c) describes a crime where one uses a computer as the instrument of a crime."

In addition, it may give rise to an action against a person who circumvents an encrypted computer system in his possession, such as an e-book reader or a DvD, since these systems perform the functions enumerated by the section. For example, Company A provides a software program that allows readers to read online books encrypted by Company A and compatible only with its software program. Should D attempt to reverse engineer said software program Company A may have a right of action against D on the ground that D has intercepted with the Company A's computer system without the right to do so in violation Section 342.1 (b).

Whether such an argument will prosper is dependent first, on whether D has some colour of right, and second, whether D intended to defraud Company A. Since ownership of the device has already passed from Company A to D, D may defeat Company A's claim on the ground that as possessor of the item, ownership has passed to him and thus he has the colour of right to intercept the computer system. However, if the software license specifically prohibits reverse engineering, Company A may defeat D's argument by proving that D surrendered right to intercept the software's functions upon its purchase.

Company A must also prove that D intended to prejudice Company A's economic interests (though proof of any actual loss is unnecessary[343]). If, therefore, D reverse engineered the system for research or interoperability, Company A cannot make any claim under this section because there is no intent to defraud it. Only if Company A can prove that D has intercepted the computer system to deprive Company A of economic value, will Company A have a right of action under this section.

Section 342.1 (c) penalizes the person who uses or causes to be used a computer system to obtain a computer service or intercept a computer system in violation of the section.

343 *R* v *Campbell* 29 (1986), C.C.C. 3d 9 (S.C.C.).

This section criminalizes the use of a computer system to violate sections (a) and (b) of section 342.1 and Section 430 (1.1). The language of the section is broad, and would seem to cast a fairly wide net, including encouraging others to use computers to the prohibited ends.[344] For instance, in the case of Company A as given above, Company A may also file suit against D on the ground that D's intent in buying its software program was not to make lawful use of it but to reverse engineer the program and distribute the encrypted data, in violation of sections (a) and (b) of this section. Again, the double requirements that the D was without colour of rights and that he intended to defraud Company A by doing so must exist for the action to prosper.

The newest addition to Section 342.1 is most relevant to the protection of technological measures. Section 342.1 (d) seeks to punish those who use, possess, traffic or permit other people to have access to computer passwords that enable them to either obtain a computer service or intercept a computer system. This provision (tacked on to Section 342.1 in 1996[345]) was created to ensure that criminal law would be available to protect the integrity of encryption regimes.[346] This aim is reflected in the provisions expansive definition of "computer password."

Under this section, computer password is defined as "any data by which a computer service or computer system is capable of being obtained or used." Though couched in broad terms, this definition is the very definition of a "decryption key." Encryption protects information by transforming data into non-recognizable and unreadable form. Decryption keys (also known as the "encryption password") are used to change the unintelligible markings back into readable information,[347] thus allowing access to the information.

In simple terms, this section provides the owner of an encryption device the right to file an action against anyone who uses, possess, distributes or sells said owner's

344 Computer Crime in Canada, *supra* note 328 at 167.
345 Bill C -17, *An Act to amend the Criminal Code and certain other Acts*, 2d Sess., 35th Parl., 1996, § 18.
346 Computer Crime in Canada, *supra* note 328 at 168.
347 *Ibid* at 122-123.

decryption code, since the code allows the user to obtain the computer service or intercept the computer system. Akin to the provisions before it, the twin requirements of no colour of right and fraud must exist for the action to prosper.

Since the above sections provide a definitive process for filing suit, a remedy to the legal system and a suitable penalty for the crime, Canada has arguably provided "adequate legal protection" and an "effective legal remedy," to safeguard technological protection measures, fulfilling, at least in part, its obligations under the WIPO.

In addition, unlike the DMCA's broad-brush legislation, section 342.1 takes into account "intent," essential in differentiating between legitimate and illegitimate acts. The twin requirements of no colour of right and intent to defraud also provide exceptions for legitimate acts done in good faith. This in turn affords leeway to researchers, students and others who have no intent to deprive the owner of the device of any economic gain, or who believe they have the right to decrypt or copy the work under the *Copyright Act* or other laws.

Nevertheless, the statute's requirement that there be "intent to defraud", while valuable in maintaining the balance between the stakeholders, leads to legislation that does not protect all types of circumvention, a gap in Canada's obligations under the internet treaties. Since the section penalizes only acts done with intent to defraud, which in turn involves prejudice to the exercise of the copyright holder's economic interest, [348] a copyright holder who derives no tangible gain from his work has no claim under this section.

Should Company X for instance provide free virus software online to enhance the goodwill of their company and Company Y breaks Company X's encryption code and begins selling Company X's virus software as its own, Company X may find it difficult to prosecute an action against Company Y under this section (or under 342.1 (b)), except in

348 *R* v *Campbell*, *supra* note 343. "An essential element of fraud is actual risk of prejudice to the economic interest of the alleged victim."

an ordinary action for copyright infringement. Since Company X derived no economic gain from the computer service, there was, to all intents and purposes, no fraud necessary to give rise to a cause of action under 342.1.[349] Though Company X could raise the issue that goodwill itself has some inherent value, given the court's narrow interpretation of new legislation (such as seen *in R* v. *Foresythe*[350]), it may be difficult to prove the claim. Future anti-circumvention legislators would therefore be prudent address this gap by focusing their legislation specifically on acts of circumvention that infringe copyright, whether or not the owner is deprived of economic value.

Another problem is the potential confusion that may result in mixing a criminal statue with matters falling exclusively under the domain of the *Copyright Act*. For instance, many "colour of right" defences would most likely hedge on whether the accused committed the aforementioned acts because he believed he had the right to infringe on the work under Copyright law, forcing courts to consider the merits of the defendants rights under the *Copyright Act* before moving on to the *Criminal Code*. Future legislation should therefore attempt to reconcile the two provisions and address how 342.1 and the *Copyright Act* function in relation to each other.

(2) Possession of device to Obtain Computer Service

Possession of device to obtain computer service

> 342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

349 Said persons may also have a cause of action under section 430 of the *Criminal Code* "Mischief in Relation to Data" under limited circumstances, discussed *infra*, note 353 and accompanying text.
350 *Supra* note 341.

> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
>
> (b) is guilty of an offence punishable on summary conviction.
>
> **Forfeiture**
> (2) Where a person is convicted of an offence under subsection [1], any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.
>
> **Limitation**
> (3) No order of forfeiture may be made under subsection [2] in respect of any thing that is the property of a person who was not a party to the offence under subsection [1].

The above section prohibits the possession, sale, offer for sale or distribution of a device "the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable interference that the... device... has been used or is to intended to be used to commit an offence contrary to that section." Used as an anti-circumvention measure, this section allows the owner of a circumvention device the right of action against owners or distributors of anti-circumvention devices under the circumstances provided under said section. Comparable with the DMCA anti-circumvention device prohibition,[351] section 342.2 criminalizes the possession or sale of the device, in effect addressing the issue of "device protection" which many copyright owners believe is essential to providing "adequate protection"[352] against the circumvention of effective technological measures.

The main distinction between 342.2 and its DMCA counterpart however is that while the DMCA immediately brands as criminal the creation of any anti-circumvention devices for whatever purpose, 342.2 does not. Instead, it sets out conditions precedent that

---

351 1201 (b) [a] and [c].
352 §11 WCT, *supra* note 37 & §18 WPPT, *supra* note 38.

give rise to the cause of action against the creation of said devices. These are: 1) the accused must have no lawful justification and excuse 2) the device must be primarily used for committing an offence under 342.1 and 3) the act must be under circumstances that give rise to a reasonable inference that the device or component has been used or is or was intended to be used to commit an offence contrary to 342.1.

The first condition, that the accused must act "without justification" implies that the law exempts the many legitimate uses of circumvention devices from research to security testing, interoperability and privacy protection. The condition is also sufficiently broad to allow for unforeseen unique uses for these devices, which would not be exempted by a blanket prohibition with enumerated exceptions (as seen in the DMCA).

Through the second condition, that "the device must be primarily used for committing an offence under 342.1," Parliament has provided another reasonable limitation. In recognizing that not all circumvention devices will be used illegally, it further restricts the grounds that can be used by owners of technological measures to file suit. Such definitive conditions under the law may act as a deterrent against harassing and frivolous lawsuits so often seen under the DMCA.

The final condition, that the act must be "under circumstances that give rise to a reasonable inference that the device or component has been used or is or was intended to be used to commit an offence contrary to section 342.1" asks the court to examine the state of affairs surrounding the creation of these devices. The condition gives the court the freedom to analyse each offence in context and not in a vacuum. For instance a software company who manufactures devices as part of its research program in a University (and is thus protected under fair dealing) will be less likely to be held liable than shady garage in a back alley that sells encryption codes of all sorts to equally shady characters in the dead of the night.

Given that there is no specific obligation to protect devices under the WIPO and blanket device protections are viewed by many to be harmful to research and study, the

conditions under Section 342.2 offer a more appropriate balance than the all-inclusive provisions of the DMCA. The key to the balance is the fact that, like section 342.1, this section takes "intent" and "context" into consideration. By doing so, Parliament has impliedly acknowledged that anti-circumvention devices have legitimate and illegitimate uses and each offense should be examined according its own merits. Equally apparent is Parliament's desire to prevent the manufacture and sale of devices which have no laudatory purpose or which have been created solely to further criminal activity.

Section 342.2 strengthens the effective legal remedies available against the circumvention of technological measures, in compliance with Canada's obligation under the Internet Treaties.

If there is any weakness in Section 342.1 and 342.2, it is the potential confusion that may result in mixing a criminal statue with matters falling exclusively under the domain of the *Copyright Act*. It is most likely that the "justifications" of the accused will proceed from his rights under fair dealing or other provisions of copyright law. Future legislation concerning circumvention should therefore attempt to reconcile the disparity and address how 342.2 and the *Copyright Act* function in relation to each other.

(3) Mischief in Relation to Data

Part XI of the *Criminal Code* entitled "Willful and Forbidden Acts with Respect to Certain Property" also criminalizes the alteration or destruction of data. It reads:

> Section 430. (1) Every one commits mischief who willfully:
>
> (a) destroys or damages property;
> (b) renders property dangerous, useless, inoperative, ineffective
> (c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

> (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.
>
> (1.1) Every one commits mischief who willfully:
> (*a*) destroys or alters data;
> (*b*) renders data meaningless, useless or ineffective;
> (*c*) obstructs, interrupts or interferes with the lawful use of data; or
> (*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Under this section, mischief may be committed in a number of ways, including the obstructing, interrupting or interfering with the lawful use of data. Used as a technology protection measures, copyright holders may have a right of action on the ground that the circumvention of technological measures is an act of mischief, since it interferes with the lawful use of the encryption technology, mainly to protect the copyrighted work. This is a particularly potent argument when the person circumventing the technology has no reasonable grounds to circumvent the technology,[353] other than to distribute the copyrighted work. Under this section, the copyright holder only has to prove that the person circumventing the technology acted "willfully."

The copyright holder may also attempt to link Section 430 (1.1) of the *Criminal Code* with the previous section and argue that because of such interference the property has become "ineffective," since once the encryption code is broken and distributed it ceases to be an effective way of preventing the circumvention of the copyrighted work.

Though the criminal provision does not directly relate to circumvention of protection technology, it offers an alternative for the copyrighter holder to protect his work. It arguably also fills the gap left by section 342.1 of the *Criminal Code*, since it prohibits any obstruction or interference with the lawful use of data without the requirement that there be fraud, the threshold under this section being mere mischief.

---

353 *R* v. *Surette* (1993), 82 C.C.C. (3d) 36 (N.S.C.A) – "An honest belief by D based on reasonable grounds that he or she had a total interest in the property damaged, affords a defense to the charge...."

A point of interest is the fact that Section 430 of the *Criminal Code* (1.1) (d), which holds liable for mischief any person who "obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto,"[354] may be used against copyright holders who employ technology protection measures to deny access to data which the public is otherwise entitled to these uses under the Copyright Act. If interpreted in this light, subsection (1.1) (d) offers some recourse to copyright users against copyright holders who use technology protection measures to prevent lawful access to their work.

C. Other Matters

This section approaches the dilemma of future anti-circumvention legislation from the opposite side of the spectrum. Instead of merely listing statutes that assist in satisfying Canada's obligations under the WIPO, it addresses certain fundamental rights threatened by DMCA-like legislation. In enacting future anti-circumvention laws, legislators must take into account not only how to fulfill Canada's obligations under the WIPO, but ensure that in creating these laws they do not inadvertently deprive Canadian citizens of basic freedoms that form the cornerstone of a free and democratic society.

1. Canadian Charter of Freedoms

In the face of unjust legislation, citizens find refuge in laws that uphold their fundamental rights. In Canada these rights are enumerated in the *Canadian Charter of Rights and Freedoms*,[355] in the U.S. they are found in the *U.S. Bill of Rights*.[356] However, there are fundamental structural difference between these two pieces of legislation and regarding certain rights, the *Charter* is not as robust as its U.S. counterpart.

---

354 *Criminal Code*, *supra* note 330.
355 Part I of the *Constitution Act, 1982*, being Schedule B to the Canada Act 1982 (U.K.), 1982.
356 U.S Const, Amendments 1 to 10 [hereinafter The *Bill of Rights*].

The presence of sections 1 and 33 of the *Charter* are examples of the sentiment of judicial deference present in the *Charter*. These sections explicitly allow government to limit and even override rights; consequently, unlike the Bill of Rights, Canada's judiciary does not have the last word on controversial issues of social policy.[357]

In light of such differences, it is important to examine, if only in brief, the extent of protection of certain vulnerable rights under the *Charter*. The court's application of the *Charter* in protecting rights which may be infringed by future circumvention legislation will in turn indicate both how future anti-circumvention law should be drafted as well as the degree of vigilance required during the process of drafting this new law to assure it conforms with the fundamental principles the *Charter* attempts to foster.

a) Right to Free Expression

The right of self-expression is one of the most pressing concerns of those opposed to anti-circumvention legislation. It has been recognized by the Canadian courts as instrumental in promoting the free flow of ideas essential to the functioning of democratic institutions, a means of promoting a marketplace of ideas to the end of attaining the truth and intrinsically valuable in itself. It is also one of the freedoms threatened by anti-circumvention legislation. In the U.S., many opponents claim that the law has all but obliterated the right to free speech in the digital context.[358]

---

357 Elliot, Robin et al. eds., *Canadian Constitutional Law 3rd Ed.* (Toronto: Emond Montgomery Publications Limited, 2003). [hereinafter "Canadian Constitutional Law"]. See also *R v Keegstra* (1990), 3 SCR 697 [hereinafter *Keegstra*]; where Dickson CJC rejects the applicability of the US Constitutional Doctrine in the case, noting that the Canadian Charter, unlike the US Bill of Rights, contains an express limitation clause.
358 See M. Gardiner," Copyright Wrongs" (2002), online: <http://www.msen.com/~mwg/copyright-wrongs.html> (date accessed: 4 March 2003). See also "DMCA Seen Denying Free Speech Rights in Cyberspace," online: YubaNet.com <http://yubanet.com/artman/publish/article_79.shtml> (date accessed: 4 March 2003); "EFF Report, 4 Years Under the DMCA," online: Slashdot <http://slashdot.org/articles/03/01/12/0233222.shtml?tid=153?> (date accessed: 6 March 2003),

In the latest decision involving the DMCA, *Universal City Studios Inc. v Corely*,[359] Universal Studios brought a suit to prohibit parties from posting on the Internet software that enabled users to decrypt digitally encrypted movies on DVDs, and from including links to other websites that made the decryptions software available. The Second Circuit Court affirmed a permanent injunction issued by the District Court.

The defendants in the case argued that the anti-circumvention provisions of the DMCA were unconstitutional because they interfered with their right to free speech as provided under the First Amendment of the *Bill of Rights*. The Appellate Court agreed with the defendants that a computer program that gives a computer instructions is "speech" within the meaning of the First Amendment. The Court held the fact that a program has the capacity to direct the functioning of a computer does not mean it lacks the additional capacity to convey information. In fact, it is that very act (relaying of information to the computer) that renders such instructions "speech" for the purposes of the First Amendment protection.

The Appellate Court then proceeded to address the scope of protection for computer code. Under U.S. law, the scope of protection for speech depends on whether the restriction is imposed because of the content of the speech.[360] A content neutral restriction is permissible if certain conditions are met. A restriction is "content neutral" if it is justified without reference to the content of regulated speech. Content neutral restrictions are permissible if they serve a substantial government interest unrelated to the suppression of free expression, and the regulation does not burden substantially more speech than is necessary to further government's legitimate interests, as the Court decided

---

359 273 F.3d 429 (2d Cir. 2001). Discussed *infra*, note 180 and accompanying text.

360 X. Wang, "'Freedom of Speech' in the United States Constitution" (2002), online: <http://www.oycf.org/Perspectives/11_043001/freedom.htm> (date accessed: 30 February 2003). "The Supreme Court has recognized that the government might adopt content-neutral regulations involving restrictions which, without regard to the message being communicated, may accidentally interfere with First Amendment expression. For example: the government may remove newspaper racks because they block the sidewalk, or the government may prohibit distribution of leaflets in the downtown area for environmental and sanitary reasons. In consideration of societal interests such as public safety, the Supreme Court upheld rules that might limit our freedom of speech-not because of a message's content but because of its context." See also *Kovacs* v. *Cooper*, 336 U.S. 77 (1949); *Metromedia* v. *San Diego*, 453 U.S. 490 (1982).

was the case in *Corley*. In addition, the Court also found that computer code includes a functional non-speech component as well as speech component.

Given its findings, the Court ruled that the restriction against posting circumvention software is content neutral. Further, the DMCA and the posting prohibition in the Lower Court's injunction targeted only the non-speech component of the decryption software. The DMCA and the posting prohibition could therefore be justified solely based on the functional capability of the decryption program without reference to the content of the regulated speech. Given that the type of regulation was content neutral and met the requirement of a substantial government interest, the Court ruled against *Corley* and upheld the DMCA regulation.

Similar precepts exist in Canada, which too gives credence to content neutral speech and the balancing of interests.[361] If DMCA type legislation were enacted and challenged in Canada as being violative of freedom of expression however, the Canadian Supreme Court's decision-making process would differ from its U.S. counterpart. Instead of relying on judge made law, the Court would focus on whether the law was permissible under section 1 of the *Charter*.[362] This in turn would be determined by analysing the law under what has become commonly known as the "*Oakes* Test."[363]

In *Irwin Toy Ltd.* v. *Quebec*,[364] the Court enumerated the steps in determining whether section 1 should apply. The first step is to ask whether the activity was within the sphere of conduct protected by the freedom of expression. The second step is to ask whether the government's purpose was to restrict the freedom of expression. The third

---

361 *Irwin Toy Ltd.* v. *Quebec (AG)* (1989), 1 SCR 927; 58 DLR (4th) 577. [hereinafter *Irwin Toy*].
362 *Constitution Act* 1982 "The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in its subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."
363 *R.* v. *Oakes* (1986), 1 SCR 103; 26 DLR (4th) 200. See also "Canadian Constitutional Law", *supra* note 353 at 759. The tests are as follows:
(1) Pressing and Substantial Purpose
(2) Rational Connection and Minimal Impairment
(3) Final Balance
(4) Standard of Proof
364 See *Irwin Toy Ltd*, *supra* note 361. This case was one of the first to apply the Oakes Test to freedom of expression.

step is to go into the details of the law itself and ask whether the limit of freedom of expression imposed in the anti-circumvention legislation is justified under the *Charter*.

Given its history, it is almost certain the Supreme Court will find that the computer language is expression and within the conduct protected by the *Charter*. The Court has always been liberal in its interpretation of what constitutes expression, furthermore the *Copyright Act* recognizes computer programs as a "literary work," and literary work in turn is a traditionally accepted form of speech.

However, note that in *Michelin* v. *Caw*,[365] the Supreme Court ruled that "private property cannot be used as a location or forum for expression" and disallowed the submission of the labour union that their posters and leaflets depicting the company's slogan 'Bibendum' are forms of expression protected by paragraph 2(b) of the Charter. The decision quoted an earlier Charter case, where Justice Thurlow opined:

> The freedom guaranteed by the Charter is a freedom to express and communicate ideas without restraint, whether orally or in print or by other means of communication. It is not a freedom to use someone else's property to do so. It gives no right to anyone to use someone else's land or platform to make a speech, or someone else's printing press to publish his ideas. It gives no right to anyone to enter and use a public building for such purposes.[366]

Based on the above decision, proponents of DMCA-like regulation would argue that the reverse engineering of the copyrighted work to create the resulting circumvention software is use of private property and as such should not come under the ambit of protected expression. The difference in the two types of use however is that while the union in Michelin directly infringed on the company's slogan, ridiculing it and making it a platform for their own expression, in the creation of circumvention devices the only "copying" occurs during the reverse engineering process. The resulting software itself is a unique and original work. Thus, though the Court's decision will rest largely on whether

365 [1997] 2 F.C. 306.
366 *Ibid.*

it considers the copying which occurs during the reverse engineering process as sufficient to constitute infringement and, in turn, use of the copyrighted work, it seems more than likely the Court will find there is insufficient use of the copyrighted work and rule the derivative software as protected expression.

In the second question, "content of expression" is paramount. If the purpose of the government is to restrict content (or suppress attempts convey a meaning) then it automatically limits the freedom of expression. However, if the government's aim is "to control the physical consequences of certain conduct regardless of whether that conducts attempts to convey meaning" then this will not automatically lead to an infringement of expression. In *Irwin Toy*, this is referred to as laws "neutral as to content," echoing the U.S. Supreme Court in *Corley*. However, even if the government's purpose is not to control content, the Court's may still decide against the law if its effect is to restrict free expression.

In applying the second step to future anti-circumvention legislation, it is necessary to divide the resulting circumvented computer code into two categories. First, there is the code as expression in itself (such as posting decryption data on the internet) and second, the code as used in other forms of expression (such as papers or lectures) where the code is contained as part of the subject matter. In the former, the Court may decide that since the expression does not further the principles and values underlying the protection of free expression[367], it is not expression that falls under the rubric of the *Charter*. Opponents may of course argue that anti-circumvention legislation inhibits self-fulfillment and that "cracking the code" is the art form. However, since computer code does not convey much meaning, the Court will probably relegate it to expression of lower value.

---

367 *Irwin Toy*, *supra* note at 361. The court summarized these values as (1) seeking and attaining the truth is an inherently good activity; (2) participation in social and political decision making is to be fostered and encouraged; and (3) the diversity in forms of individual self-fulfillment and human flourishing ought to be cultivated in an essentially tolerant and indeed welcoming environment not only for the sake of those who convey a meaning but also for the sake of those to whom it is conveyed. The court then went on to say that In showing that the effect of the government action's was to restrict her free expression, one must demonstrate that the activity promotes at least one of these principles and that it was not enough that it had an expressive element. One must show that the aim was to convey a meaning reflective of the principles underlying freedom of expression.

On the other hand, code used in other more traditional forms of expression (such as in literary works) may be afforded a higher degree of protection because it conveys a more immediate meaning. One example is Dimitri Skylarov's controversial paper against Adobe. Skylarov decrypted Adobe's software in the course of writing his PhD thesis called "E-book Security: Theory and Practice, which argued that the security behind Adobe's Document Format, known as PDF, was inherently flawed[368]. In the above example, the decryption performed by Skylarov was not primarily for the purpose of breaking into Adobe's software but to further the subject matter of his thesis.

In either case however, given the Court's record of leniency in determining what constitutes free speech, it will more than likely rule that freedom of expression has been breached and proceed to the third step. In this final step, the Court must deal with whether the legislation is within the limits "prescribed by law." To do this the Court must ask whether the government has a pressing and substantial objective and whether the means are proportional to the ends (again a sentiment similar to the U.S. Court in *Corley*). The Court's decision in this regard will be difficult to predict as its decision will be based on the actual provisions of the proposed legislation. On the one hand, the Court has shown a great deal of deference to Parliament in matters of *Charter* rights. On the other hand, the Court has done so mostly in matters where Parliament's aim was to protect a vulnerable group targeted by the expression.[369] If Canada follows the U.S. trend, anti-circumvention legislation suits will likely involve large corporations filing suit against small interest groups or individuals, thus there will no "vulnerable group" (since corporations are not considered as such) to protect against expression. In making its decision, the Court will likely consider various matters, such as the copyright aspect of the law; the importance of computer speech to education, research, growth and self-expression; whether the law complies with the Internet Treaties; the rational connection and minimum impairment between the freedom of expression and the specific provisions of the law itself.

---

368 A. Creed, "Skylarov Indicted, Could Face 25 Years In Jail" *Newsbytes* (20 July2001), online: <http://www.newsbytes.com/news/01/169504.html>.

369 See *Irwin Toy*, *supra* note 361, *R* v. *Keegstra*, *supra* note 357; *R* v. *RJR Macdonald Tobacco* (1995), 3 SCR 199; *R* v. *Butler* (1992), 1 SCR 452.

In summary, the Court's decision will rest mainly on where it believes balance exists between individual and state interests, where this line will be drawn however is impossible to predict. Nevertheless, given the DMCA's far reaching consequences, its chilling effect on freedom of expression and its wholly negative impact on study and research in the U.S., should DMCA-like legislation be passed by Parliament it would be more in line with Canadian ideals under the *Charter* for the Supreme Court to rule that this legislation is a violation of the spirit of the *Charter* and disallow the law in favour of a more moderate version.

b) Privacy

The right to privacy is a double-edged sword that is used by both proponents and opponents of anti-circumvention legislation. Proponents hail protection technology measures and legislation as a means to prevent breaches in privacy, opponents predict that the same technology can be used to defeat the right to privacy. Whatever the argument on both sides, so pressing is the concern that the government itself addressed the issue in the Consultation Paper.[370]

There are two main reasons for concern: First, there are the continued and unrelenting attempts of advertisers and computer industries to monitor the activities private persons. Companies such as Pentium[371] and Microsoft[372] have attempted to install software that continually relays information to them once the user connects to the internet, allowing them to monitor their customer for their own ends. There is also the presence of devices commonly known as "spyware" programs contained within other programs, which users unknowingly install on their computer systems when they install the main program. This hidden program has the ability to track the user's activities on the internet, relay information about the user to software company and even relay the user's private

370 Consultation Paper, *supra* note 7 at 25. The government asks "Are there any non-copyright issues e.g. privacy, that need to be taken into account when addressing technological measures?"
371 See "Damn that Spyware" (2000), online: <http://www.jello.net/report/Issues/2000/11/25/20001125.asp> (date accessed: 12 October 2002).
372 See "Microsoft, Real Face 'Spyware' Probe," online: CNN.com <http://www.cnn.com/2002/WORLD/europe/06/17/eu.cookies/> (date accessed: 7 November 2002).

documents. Cookies are a less nefarious form of spyware, since the users are informed these devices will be installed on their computer before they are able to progress further into a website. In all these cases however, it is logical to assume that most people would like the option of being able to remove these invasive programs from their computers.

Second is the lack of robust protection of privacy under the Canadian legal system. The *Charter*, the document recognized to be the source of fundamental rights, does not explicitly recognize the right to privacy, though certain *Charter* rights have an impact on privacy. Section 7 states that "everyone has the right to life, liberty and security of person...." Arguably, privacy is necessary to ones security of person. In addition, section 8 provides that "everyone has the right to be secure against unreasonable search and seizure." However, such sections do not have the same impact as a provision expressly stating the right to privacy as a fundamental right.

While Parliament has enacted a *Privacy Act,*[373] "to extend the present laws of Canada to protect the privacy of individuals..." the act is limited to "personal information... held by a government institution..."

Criminal Code provisions relating to privacy are limited to disallowing intercepting private communications,[374] and provides no protection against spyware and cookies. Some province have laws alluding to a citizen's right to privacy,[375] however Quebec is the only province with forceful privacy protection laws. Quebec's *Charter of Rights and Freedoms* secures the right to privacy for residents of the province. This express recognition of the right to privacy is bolstered in its *Civil Code* that provides residents of Quebec with a right of action in cases where their informational, territorial or personal privacy is violated.[376]

---

373 *Privacy Act*, Chapter P-21, online: http://laws.justice.gc.ca/en/P-21/92468.htm (date accessed: 19 March 2003).
374 *Criminal Code*, § 184, *supra* note 327. Additionally, § 184.5 applies specifically to radio based telephone communications.
375 See the Consumer Reporting Act of Ontario, which limits the kind of information which can be gathered and restricts anyone not specifically listed in the act from knowingly obtaining information from files of a consumer reporting agency respecting a consumer.
376 *Civil Code of Quebec*, S.Q., 1991, c. 64, Title 1, chapter 3.

Though the U.S. also has no comprehensive legal protection of privacy as between individuals, privacy is well protected under U.S. common law. In his landmark article in the University of California Law Review, Professor William Prosser found four actionable torts for the invasion of privacy in the U.S., some of which do "not exist in any form in Canadian law."[377]

Proponents of circumvention technology argue that allowing for the circumvention of encrypted data violates the right to privacy, citing the simplified analogy of laws that prevent thieves from the breaking into a locked safe, a phrase oft use in defense of anti-circumvention legislation. However, the problem is not as black and white as it appears to be, and the knife, to coin another phrase, cuts both ways.

At present, and despite the weak protection on Canadian right to privacy, there has been no conflict regarding the removal of cookies and spyware or the right of Canadians to legally remove or block such software. However, should a blanket prohibition against circumvention of encrypted data be passed, creators of these devices merely need to wrap the devices in encrypted technology to prevent the public removing these files to protect their privacy. Further, even if an exception were made to allow for the removal this invasive software, the exception would be rendered meaningless if the law does not permit developers to manufacture and distribute devices to enable circumvention of encrypted technology.

Future anti-circumvention legislation should address the problem of privacy, not by prohibiting the manufacture and sale of circumvention devices, but by holding accountable those who collect and use personal data without the permission or sell data they are supposed to hold in trust by laws. Laws such as the *Protection and Electronic Documents Act*,[378] are a good beginning to this trend.

---

377 David Johnston et al., *Getting Canada Online: Understanding the Information Highway* (Toronto: Stoddart Publishing Co. Ltd., 1995) at 203 [hereinafter "Getting Canada Online"].
378 S.C. 2000 c.5.

Thus, while circumvention should be controlled to some extent because, admittedly, it can be used for illegal acts, a distinction must be made between circumvention that violates privacy and circumvention that furthers it. For instance, a law disallowing circumvention of TPMs must also provide a self-help provision allowing for circumvention if the TPMs are contained in privacy invading software. Furthermore, the government must refrain from legislation banning the manufacture and distribution of circumvention devices with impunity, unless these devices are proven to have little to no value other than as tools for illegal acts of infringement or invasion of privacy. In summary, the government should take measures to ensure the law protecting the citizenry from illegal acts of circumvention do not also prevent the legitimate use of circumvention, in effect defeating the right it hopes to protect.

VI Conclusion

With the advance of information technology, copyright limitations have become increasingly difficult to enforce. Copyright owners hailed Technological Protection Measures as the technological solution to a technological problem. However, TPMs are not in themselves invulnerable and can be defeated through circumvention. In response to this dilemma, WIPO adopted the Internet Treaties, obliging member states to provide effective legal remedies against the circumvention of effective technological measures used to violate copyright law.

At its face, the Treaties appeared relatively straightforward, unfortunately the ensuing legislation from countries such as the U.S. proved otherwise. The controversial DMCA is overbroad and ill conceived, and has resulted in the erosion of fundamental rights and the criminalization of much legitimate research and study. Decisions from U.S. courts have made it patently clear that the DMCA reaches far beyond the limitations of copyright law, placing basic copyright principles such as fair use in peril.

The principal problem with protecting TPMs is that while copyright is limited in many ways (such as its term, object and scope of restricted acts), exclusivity gained through technology is potentially unlimited.[379] The U.S.'s answer to the problem of TPMs has been an almost complete prohibition against the circumvention of copy-protection technology, with disastrous results.

In the wake of such chaos, Canada too is preparing to enact its own copy protection technology legislation. Its dilemma is creating legislation that fulfills its obligations under the WIPO all the while maintaining the delicate balance between the different stakeholders of copyright law. Central to the issue of the type of legislation to enact are the public's responses to the questions posed in the Consultation Paper. Though the comments were varied, three basic arguments have emerged:

---

379 K. Koelman, "The Protection of Technological Measures Versus the Copyright Limitations," Copyright World 122 (August 2002) 18 at 18 [hereinafter "Copyright World"].

First, circumvention of TPMs is not copyright infringement – it is not copying- it is merely accessing an existing copy of published work in an alternate manner.[380] Second, Parliament must be wary of a law that "gives far too much power to publishers, at the expense of the rights of the individual," and that not only individual users but also schools, libraries, museums and archives are in jeopardy with DMCA style legislation.[381] Third, the Internet Treaties do not to require national legislation to enact provisions that sanction the legitimate use of technological measures by copyright owners or restrict uses permitted by law.[382] The Consultation Paper also establishes that "by providing legal recognition of technological measures, the traditional boundaries of copyright law will be extended to include new layers of protection" and thus the *Copyright Act* may not be the proper instrument for protection measures which, *prima facie*, are extraneous to copyright principles."[383] These comments provide valuable insight to minds of Canadians and assist in drawing the line between acceptable and unacceptable legislation.

However, in light of the basic limitations as stated above, a more fundamental issue arises: does Canada need new legislation at all?

Despite external pressure, especially from the United States, to codify new anti-circumvention law in Canada, thorough examination proves there is no pressing need for such measures at present. Canada's various and extensive pockets of legislation form a protective weave around copyright protection technology measures since they prevent many illegal uses of the technology and compensate copyright owners for potential infringement of their works.

First, are the comparatively restrictive clauses under the *Copyright Act* regarding both reverse engineering and fair dealing. Section 30.6 of the *Copyright Act* is clear, allowing reverse engineering for stated purposes only. Further, since no Supreme Court doctrine exists in Canada which situates reverse engineering under the rubric of fair

380 Samuelson1, *supra* note 164.
381 P.Tatham, "Response to The Consultation Paper on Digital Copyright Issues" (11 September, 2001), online: MLUG <http://zope.mlug.ca/paul/Response_CPDCI_html>.
382 CLA, *supra* note 12.
383 Consultation Paper, *supra* note 7 at § 4.2.

dealing,[384] any reverse engineering done outside Section 30.6 may be assailed as copyright infringement. Fair dealing itself is limited in Canada, being a product of statute and not judge made law as fair use is in the U.S., which may encourage Canadian courts to be less liberal in deciding what constitutes fair dealing.

Second, are the provisions under the *Criminal Code*[385] prohibiting certain unauthorized uses of a computer. Section 342.1 makes it illegal for persons to, fraudulently and without the colour of right, obtain a computer service, interfere with a computer system, or use or permit others to have access to a computer password for any of the enumerated offences. Still, it is section 342.2, which provides the most encompassing protection for technological circumvention measures since it effectively prevents the use, distribution, possession or sale of circumvention devices for illegal purposes. Admittedly, as these devices may be used for both legal and illegal means, the law remains imperfect since it cannot ascertain which devices have been used to perform illegal acts.[386] However, given the difficulties of legislating on copy-protection technology, the law is a good compromise, providing copyright owners with some recourse against both acts of circumvention and circumvention devices, without undue oppression of the rights of legitimate users. Section 430 has the potential to fill the gap left by section 342.1 by prohibiting the obstruction of or interference with the lawful use of data without the requirement that there be fraud, the threshold under this section being mere mischief.

Third, are mechanisms such as the Blank Media Levy that aim to compensate copyright owners for their work, not by prohibiting circumvention, but by placing a small fee on all blank media bought in Canada and distributing the proceeds to the copyright owners affected. The major failing of the DMCA is that by prohibiting the act of circumvention as well as the use of circumvention devices, it prohibits access to copyright materials in digital form, even for arguably legal acts. The Blank Media Levy does not prohibit access to copyrighted materials but takes steps to compensate copyright owners

384 In the same way *Sega*, *supra* note 14, does in the U.S.
385 *Supra* note 327.
386 E.g. should future device be invented which, for instance, is intelligent enough to block transmission of the data after infringing acts are performed on the copyrighted work, then the law may properly declare illegal all attempts to circumvent this device.

against possible infringement. While, like the DMCA, the levy also takes a broad brush approach to protecting the rights of copyright owners, the relatively small cost to the buyers of the media seem more balanced then possible criminal and heavy civil sanctions for a violation of the DMCA.

Taken as a whole, a set of laws exist in Canada which provide effective legal remedies against the circumvention of technological measures by prohibiting the acts of circumvention and circumvention devices where such acts or uses are illegal in nature, and further compensates affected copyright owners for possible infringement of their work. Yet the laws do not prohibit legitimate access to copyrighted work in digital format or place an undue burden on the copyright user by automatically labeling as criminal said uses or acts, as the DMCA does. Through these various pockets of legislation, Parliament has competently complied with Canada's obligations under the WIPO without unduly restricting the rights of Canadian users under the fair dealing provisions of the *Copyright Act.*

While there is no further need for all encompassing, DMCA-like legislation, for purposes of clarity, Parliament should take steps to unify the various existing legislation on protection technology or, at the very least, clarify how the *Criminal Code* and *Copyright Act* provisions function in relation with each other. For instance, can fair dealing be used as a "lawful justification" against violation of Section 342.2 of the *Criminal Code*? What is the role of copyright infringement in determining whether there has been a violation of Section 342.1?

Anti-circumvention legislation is inherently difficult to legislate because present technology is simply too crude to accommodate all the subtleties of the law.[387] As a result, the options open to legislators regarding future legislation in this matter are limited and it is often difficult to find the balance between the various stakeholders of copyright. Despite these challenges however, Parliament has succeeded in its task of enacting protection technology measures and maintaining the balance between the various

387 "Copyright World", *supra* note 379 at 18.

copyright stakeholders. It is not difficult to foresee a comprehensive law in the future incorporating the different pieces of legislation enumerated herein. However, it serves Parliament well to proceed slowly, taking account both the realities of technology as well as the balance between the stakeholders.

As technology progresses, so will the laws seeking to cope with it. The Canadian Parliament must continue to eke out its own path regarding the protection of technology measures, taking into consideration the rights of the various stakeholders as well as the principles of copyright law.

BIBLIOGRAPHY

A. LEGISLATION

1. Canada

Bill C-32, *An Act to amend the Copyright Act*, 2d Sess., 35th Parl., 1996 cl 8.

Bill C -17, *An Act to amend the Criminal Code and certain other Acts*, 2d Sess., 35th Parl., 1996, § 18.

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being schedule B to the Canada Act 1982 (U.K.), 1982.

Civil Code of Quebec, S.Q., 1991, c. 64.

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

Copyright Act of Canada, R.S.C. 1985 (4th Supp.).

Criminal Code, R.S.C. 1985.

Privacy Act, Chapter P-21, http://laws.justice.gc.ca/en/P-21/92468.html.

Protection and Electronic Documents Act, S.C. 2000 c.5.

2. U.S.A

Bill of Rights, U.S Constitution, Amendments 1 to 10.

Copyright Act, Title 17, United States Code.

Digital Era Copyright Enhancement Act, H.R. 3048, 105th Congress., 1st Session., Section 8.

The Digital Milennium Copyright Act, Title 17, United States Code, Section 1201(1998).

B. INTERNATIONAL TREATIES

Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979, Berne Union, 1886, 828 U.N.T.S. 221, online: <http://www.law.cornell.edu/treaties/berne/overview.html> (date accessed: 2 April 2003).

Convention Establishing the World Intellectual Property Organization, Stockholm, 14 July 1967 (as amended on 28 September 1979), online: <http://www.wipo.int/clea/docs/en/wo/wo029en.htm> (date accessed: 24 April 2003).

International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, 26 October 1961, 496 U.N.T.S. 43, online: <http://www.wipo.int/clea/docs/en/wo/wo024en.htm> (date accessed: 18 March 2003).

Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite (Brussels on May 21, 1974), Vienna Union, online: <http://www.wipo.int/clea/docs/en/wo/wo025en.htm> (date accessed: 18 March 2003).

Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms, Geneva October 29, 1971, Phonograms Convention (Geneva, 1971) online: <http://www.wipo.int/clea/docs/en/wo/wo023en.htm> (date accessed: 18 March 2003).

General Agreement for Tariff and Trade, (Geneva: GATT Secretariat, 1994) 365-403, reprinted in 1994), 33 I.L.M. 1197-1225 GATT, online: <http://www.ciesin.org/TG/PI/TRADE/gatt.html> (date accessed: 24 February 2003).

North American Free Trade Agreement Between the Government of Canada, the Government of Mexico, and the Government of the United States, 17 December 1992, Can. T.S. 1994, No.2 I.L.M. 287 (entered into force 2 January 1994), online: <http://www.nafta-customs.org/> (date accessed: 21 March 2003).

Paris Convention for the Protection of Industrial Property, U.N.T.S. No. 11851, vol. 828, pp. 305-388, as revised at Brussels on 14 December 1900, at Washington on 2 June 1911, at the Hague on 6 November 1925, at London on 2 June 1934, at Lisbon on 31 October 1958, and at Stockholm on 14 July 1967.

WIPO Copyright Treaty, Geneva, 20 December 1996, online: <http://www.wipo.int/clea/docs/en/wo/wo033en.htm> (date accessed: 18 June 2002).

WIPO Performances and Phonograms Treaty and Agreed Statements Concerning the WIPO Performances and Phonograms Treaty WIPO Performances and Phonograms Treaty, Geneva 20 December 1996, online: <http://www.wipo.int/clea/docs/en/wo/wo034en.htm> (date accessed: 10 November 2002).

Universal Copyright Convention, January 27, 1902, 35 Stat 1934.

C. GOVERNMENT MATERIALS

A Framework for Copyright Reform, 2001, online: Government of Canada <http://strategis.ic.gc.ca/SSG/rp01101e.html> (date accessed: 3 June 2002).

An Overview of Submissions on the Consultation Paper on Digital Copyright Issues, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/rp00842e.html> (date accessed: 29 March 2003).

Copyright Reform Process, online: <http://strategis.ic.gc.ca/SSG/rp01100e.html> (date accessed: 10 September 2002).

Copyright Board's Decision, Private Copying 2001-2002, online: <http://www.cb-cda.gc.ca/news/c20012002fs%2De.html> (date modified: 07 July 2001).

Consultation on Digital Copyright Issues, Intellectual Property Policy Directorate (2001), online: Industry Canada <http://www.museums.ca/copyright2001/cdnheritagepaper.pdf> (date accessed: 3 June 2002).

Information Highway Advisory Council, *Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council* (Ottawa, Industry Canada, 1997).

Information Highway Advisory Council, *Copyright and the Information Highway: Final Report of the Copyright Subcommittee*, (Ottawa: Supply and Services Canada, 1995).

Submissions Received Regarding the Consultation Papers, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html#sub> (date accessed: 05 March 2003).

Subcommittee Report, *Copyright and the Information Highway: Preliminary Report of the Copyright Subcommittee* (Ottawa: Information Highway Advisory Council Secretariat, 1194).

D. TABLE OF CASES:

1. Canada

Allen v. *Toronto Star* (1997), 78 CPR 3d 115.

Apple Computer Inc. v. *Mackintosh Computers Ltd* (1986), 10 CPR (3d) at 20-21, 28 DLR (4th) 178 (FCTD).

Bishop v. *Stevens* (1990), 2 S.C.R. 467.

Canadian Admiral Corp. Ltd v. *Rediffusion Inc.*, (1954), E.x. C.R. 382.

Compo Co. v. *Blue Crest Music Inc.* (1980), 1 S.C.R. 357.

Irwin Toy Ltd. v. *Quebec (AG)* (1989), 1 SCR 927; 58 DLR (4th) 577.

MCA Canada v. *Gillberry & Hawke Advertising Agency* (1976), 28 CPR 2d 52 (FCTD).

Michelin v. *Caw* (1997), 2 F.C. 306.

Moreau v. *St. Vincent* (1950), 1950 C.R. 198.

R. v. *Butler* (1992), 1SCR 452.

R. v. *Campbell* (1986), 29 C.C.C. 3d 9 (S.C.C.).

R. v *Forsythe* (1991), 137 A.R. 321 (Prov Ct.).

R. v *Jones* (1991), 66 C.C.C. (3d) 512 (S.C.C.).

R. v. *Keegstra* (1990), 3 SCR 697.

R. v. *Oakes* (1986), 1 SCR 103; 26 DLR (4th) 200.

R. v. *RJR Macdonald Tobacco* (1995), 3 SCR 199.

R. v. *Stewart* (1988), 1 S.C.R. 963.

R. v. *Surette* (1993), 82 C.C.C. (3d) 36 (N.S.C.A).

R. v. *Théroux* (1993), 19 C.R. (4th) 194, 79 C.C.C. (3d) 449 (S.C.C.).

R. v *Zlatic* (1993), 79 C.C.C. (3d) 466 (S.C.C).

Théberge v. Galerie d'Art du Petit Champlain Inc, (2002) 2002 SCC 34, online: <http://www.lexum.umontreal.ca/csc-scc/en/rec/html/laroche.en.html> (date accessed: 6 April 2003).

2. U.S.A

A&M Records, Inc. et al. v. *Napster Inc.*, 54 U.S. P.Q. 2d 1746 (N.D. Cal 2000).

Atari Games Cop v. *Nintendo of America Inc.*, 975 F. 2d 832 (Fed Cir. 1992).

Campbell v. *Acuff-Rose Music Inc.*, 510 U.S. 576 (6th Cir. 1994).

Carrasco v. *State,* 712 S.W.2d 623 (1984).

Chambers v. *Time Warner, Inc.*, 282 F.3d 147 (2002).

Cubby Inc. v. *Compuserve, Inc.*, 776 F.Supp. 135 (1991).

Eodice v. *State*, 742 S.W. 2d 844 847 (1987).

Goocher v *State,* 6 SW.2d 860.

Harper & Row v. *Nation Enterprises,* 471 U.S. 539 (1985).

Harris v. *State,* 790 S.W.2d 778 (1990).

International News Service v. *Associated Press,* 248 U.S. 215 (1918).

Kovacs v. *Cooper,* 336 U.S. 77 (1949).

Metromedia v. *San Diego*, 453 U.S. 490 (1982).

Nobby Lobby, Inc. v. *Dallas,* 767 F. Supp. 80 (1992).

Sega Enterprises v. *Accolade Inc.*, 977 F.2d 1510 (1992).

Sony Corp. v. *Universal City Studios, Inc.*, 464 U.S. 417 (1984).

Twentieth Century Music Corp. v. *Aiken* , 422 U.S. 151 (1975).

Universal City Studios Inc. v. *Corely* , 273 F.3d 429 (2d Cir 2001).

Universal City Studios, Inc. v. *Reimerdes*, F.Supp 2d 294 (SDNY 2000).

Wheaton v. *Peters*, 33 U.S. 591 (1843).

E. SECONDARDY MATERIALS:

1. Articles:

Birrell, A., *Seven Lectures on the Laws and History of Copyright in Books* (New York: G.P. Putnam's Sons, 1899), as reprinted (New Jersey: Rothman Kelley, 1971).

Davis, R.W. & Hutchison, S.C., *Computer Crime in Canada: An Introduction to Technological Crime and Related Legal Issues* (Ontario: Carswell, 1997).

Elliot, R. et al. eds., *Canadian Constitutional Law 3rd Ed.* (Toronto: Emond Montgomery Publications Limited, 2003).

Fox, H.G., *The Canadian Law of Copyright and Industrial Designs 2nd edition*, (Toronto: Carswell, 1967).

Garfinkel, S. & Spafford, G., *Practical Unix Security* (Sabstopol, California: O'Reilly & Associates, 1991).

Goldstein, P., *Copyright's Highway*, (New York: Hill and Wang, 1995).

Handa, S., *Copyright Law in Canada*, (Ontario: Butterworths, 2002).

Irwin, B. F. & Rubin, E. L., *The Digital Millennium Copyright Act and the Internet* (San Francisco, New York City, Chicago: Practicing Law Institute, Patents, Copyrights, Trademarks, and Literary Property, Course Handbook Series, 2001).

Johnston, D. et al., *Getting Canada Online: Understanding the Information Highway* (Toronto: Stoddart Publishing Co. Ltd., 1995).

McKeown, J.S., *Fox Canadian Law of Copyright and Industrial Designs 3rd Edition* (Ontario: Carswell, 2000).

Reinbothe, J., *The WIPO treaties 1996: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: Commentary and legal Analysis* (London: Butterworths, 2002).

Scrutton, T.E., *The Law of Copyright* (London: Willima Cloes and Sons Limited, 1903).

Takach, G.S., *Computer Law*, (Toronto: Irwin Law, 1998).

Watt, D. & Fuerst, M., *Tremeerar's Criminal Code* (Ontario: Carswell Publishing,1996).

2. Journals:

Bainbridge, D.I., "Computer Programs and Copyright: More Exceptions to Infringement," (1993), 56 Modern Law Review 591.

Handa, S., "Reverse Engineering Computer Programs under Canadian Copyright Law" (1995) 40 McGill L.J.

Melnitzer, J., "New Copyright Leaves Some Work Undone," Law Times (15 September 1997).

Patterson, R., "Free Speech, Copyright and Fair Use" (1987), 40 Vand.L. Review 1 at 62.

Samuelson, P., "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised," 52 Stan. L. Rev, online: <http://www.sims.berkeley.edu/%7Epam/papers/Samuelson_IP_dig_eco_htm.htm> (date accessed: 2 February 2002).

Zimmermann, S., "A Regulatory Theory of Copyright: Avoiding a First Amendment Conflict" (1966) 35 Emory L.J. 163.

3. Thesis:

Handa, S., *Reverse Engineering Computer Programs under Canadian Copyright Law*, (1994), McGill Thesis, McGill University Institute of Comparative Law.

Handa, S., *Understanding the Modern Law of Copyright in Canada* (1997), McGill Thesis, McGill University Institute of Comparative Law.

4. Magazines:

Koelman, K., "The Protection of Technological Measures versus the Copyright Limitations," *Copyright World* 122 (August 2002) 18.

F. INTERNET

1. Articles with Authors:

Bollier, D., "Stopping the Privatization of Public Knowledge" (2002) online <http://www.tompaine.com/feature.cfm/ID/6017> (date accessed 16 October 2002).

Bonisteel, S., "Canada Tackles Copyright Laws For Digital Age" (2001), online: Newsbytes <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=167203> (date accessed: 10 November 2002).

Capello, V., "Being a Hacker" (1999), online: <http://www.astalavista.com/library/basics/guides/beinghacker.shtml> (date accessed: 9 December 2001).

Clinton, W. J. & Gore, A. Jr., "A Framework for Global Electronic Commerce" (1997), online: <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (date accessed: 29 October 2002).

Cohen, J., "Call it the Digital Millennium Censorship Act" (2000), online: The New Republic Online <http://www.thenewrepublic.com/cyberspace/cohen052300.html> (date accessed: 14 December 2001).

Dyson, J., "Ugly Mistake for Pretty Good" (2001), online: Treachery Unlimited <http://www.treachery.net/articles_papers/crypto.html> (Date accessed: 9 December 2001).

Ferguson, N., "Censorship in action: why I don't publish my HDCP Results" (2001), online: MacFergus <http://www.macfergus.com/niels/dmca/cia.html> (date accessed: 12 December 2001).

Forno, R., "National Security and Individual Freedoms: How the Digital Millenium Copyright Act Threatens Both," (2001), online: <http://www.fitug.de/news/horns/horns200701222636.html> (date accessed: 11 December 2001).

Gardiner, M., "Copyright Wrongs" (2002), online: <http://www.msen.com/~mwg/copyright-wrongs.html> (date accessed: 4 March 2003).

Geist, M., "Canada Tackles Copyright for the Digital Age," (2001) online: <http://aix1.uottawa.ca/~geist/main.html> (date accessed: 15 October 2002).

Karsten, M., "Functionality Doctrine" (2001), online: <http://zork.net/pipermail/free-sklyarov/2001-September/004128.html> (date accessed: 26 June 2002).

King, B., "Fight Rages Over Digital Rights" (2001) online: Wired News <http://www.wired.com/news/politics/0,1283,41183,00.html> (date accessed: 1 December 2001).

Lehman, B., "White Paper," (1995) online: <http://www.geog.ubc.ca/~acitpo/copyright/clinton_whitepaper.html> (date accessed: 20 May 2002).

Mathesson, J., "Fair Use is Dead" (2001), online: Computer User <http://www.computeruser.com/articles/daily/8,6,1,0427,01.html> (date accessed: 9 December 2001).

Petersen, R., "Copyright and Electronic Information Access on a Collision Course" (2001), online: <http://www.oit.umd.edu/ITforUM/2001/Fall/fair/> (date accessed 4 November 2002).

Lemos, R.,"Security workers: Copyright law stifles," CNET News.com (2001), online: News.Com <http://news.cnet.com/news/0-1003-200-7079519.html?tag=tp_pr> (date accessed: 1 December 2001).

Tatham, P., "Response to The Consultation Paper on Digital Copyright Issues" (2001), online: MLUG <http://zope.mlug.ca/paul/Response_CPDCI_html>.

Trottier, T., "Canada Blank Media Levy Only Benefits the US" (2003) online: Straight Goods <http://www.straightgoods.ca/ViewLetter.cfm?REF=1071> (date accessed: 13 March 2003).

Vaidhyanathan, S., "Putting a lock on e-books: A new cold war looms over your right to read" (2001), online: MSNBC <http://stacks.msnbc.com/news/602444.asp> (date accessed: 8 December 2001).

Wang, X., "'Freedom of Speech in the United States Constitution'" (2002), online: <http://www.oycf.org/Perspectives/11_043001/freedom.htm > (date accessed: 30 February 2003).

2. Articles without Authors:

"A Protester's Guide to the Digital Millennium Copyright Act" (2000), online: <http://www.tuxers.net/dmca/dmca-guide.html> (date accessed: 18 July 2002).

"About WIPO," online: WIPO <http://www.wipo.org/about-wipo/en/> (date accessed: 12 March 2003).

"Academic Freedom and the Digital Divide" (2001), online: CFIF.ORG <http://www.cfif.org/5_8_2001/Free_line/current/free_line_academicfreedom.htm> (date accessed: 12 December 2001).

"Blank 'Audio' Media Levy?" online: <http://www.musicbymailcanada.com/article2.html> (date accessed: 02 March 2003).

"Blank Media Levy," online: <http://www.sycorp.com/levy/> (date accessed: 19 February 2003).

"The Blank CD-R Tax FAQ," online: <http://neil.eton.ca/copylevy.shtml#copy_for_friends, citing footnote 4 of a Copyright Board Ruling> (date accessed: 01 March 2003).

"Canada's Bill C-32 and Archival Research," online: Archive Society of Alberta <http://www.archivesalberta.org/dec96/c32.htm> (date accessed: 23 March 2003).

"Canadian 'DMCA' in the Works - Short Deadline: Tell Canada to Reject Anti-Technology Bans," (2001), online: Electronic Frontier Foundation <http://www.eff.org/alerts/20010907_eff_canada_cpdci_alert.html> (date accessed: 19 September 2002).

"Copyright" online: Law.com <http://dictionary.law.com/definition2.asp> (date accessed: 17 April 2002).

"Damn that Spyware" (2000), online: <http://www.jello.net/report/Issues/2000/11/25/20001125.asp> (date accessed: 12 October 2002).

"Digital Copyright Court Cases" (2001), online: <http://www.acm.org/usacm/copyright/dmca.htm> (date accessed 6 January 2003).

"DMCA Seen Denying Free Speech Rights in Cyberspace," online: YubaNet.com <http://yubanet.com/artman/publish/article_79.shtml> (date accessed: 4 March 2003).

"EFF Report, 4 Years Under the DMCA," online: Slashdot <http://slashdot.org/articles/03/01/12/0233222.shtml?tid=153?> (date accessed: 6 March 2003).

"EFF Whitepaper: Unintended Consequences," online: Electronic Frontier Foundation <http://www.eff.org/IP/DMCA/20020503_dmca_consequences.html> (date accessed: 11 December 2002).

"Microsoft, Real Face 'Spyware' Probe" (2002), online: CNN.com <http://www.cnn.com/2002/WORLD/europe/06/17/eu.cookies/> (date accessed: 7 November 2002).

"Reverse Engineering," online: Dictionary.com <http://dictionary.reference.com/search?q=reverse%20engineering> (date accessed: 22 September 2002).

Statement of Allan R. Adler Vice President for Legal and Governmental Affairs Association of American Publishers before the Subcommittee on Courts, the Internet and Intellectual Property House Judiciary Committee concerning s.487: "The Technology, Education and Copyright Harmonization Act of 2001", online: <http://www.house.gov/judiciary/adler_062701.htm> (date accessed: 25 August 2003).

"Statement of Michael K. Kirk, Executive Director American Intellectual Property Law Association before the Subcommittee on Courts, the internet and Intellectual Property Committee on the Judiciary United States House of Representatives at the Oversight Hearing on Reexamination May 10, 2001", online: <http://www.house.gov/judiciary/kirk_051001.htm> (date accessed: 25 August 2003).

"The Latest on the Recordable Media Levy," online: PC Buyer's Guide.com <http://pcbuyersguide.com/hardware/storage/cdr-levy.html> (date accessed: 28 January 2003).

"WIPO Internet Treaties Come Into Force" (2002), online: <http://www.kaapeli.fi/hypermail/ecup-list/0911.html> (date accessed: 28 April 2003).

"WIPO welcomes U.S. Ratification of 'Internet' Treaties" (1999), online: Press Release <http://www.wipo.org/pressroom/en/releases/1999/p183.htm> (date accessed: 28 April 2003).

"Universal City Studios, Inc v. Corley: the Constitutional Underpinnings of Fair Use Remain Open to Question," online: Duke Law and Technology Review <http://www.law.duke.edu/journals/dltr/articles/2002dltr0003.html> (date accessed: 15 February 2003).

G. SUBMISSIONS TO FRAMEWORK QUESTIONS

1. Individual Respondents:

Submission from Hakim Sid Ahmed received on July 28, 2001 3:46 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Jesse Burns received on July 24, 2001 2:34 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Christian Charette received on July 24, 2001 2:06 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Mark Cuban received on June 22, 2001 4:13 PM via e-mail online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Chris Friesen, received on July 24, 2001 10:53 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Ashley George received on July 17, 2001 11:59 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Dennis Grant received on July 30, 2001 12:44 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Sandy Harris received on July 29, 2001 9:13 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Richard Anthony Hein, received on July 24, 2001 2:20 pm via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Ryan McDougall received on July 30, 2001 10:52 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Chris Nelson received on July 24, 2001 3:30 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Ryan Peters received on July 24, 2001, 8:48 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Samuel Philip Lake Smith received on July 10, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Submission from Jakub Wojnarowicz, received on July 24, 2001 2:01 PM via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

2. Respondent Entities:

Submission from the Association of Universities and Colleges of Canada (AUCC), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Archival Community received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Association for Interoperable Systems received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Association of Law Libraries/Association Canadienne des Bibliothèques de Droit (CALL/ACBD) received on September 17, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Broadcasting Corporation (CBC) on September 17, 2001via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Copyright Institute (CCI), received on September 17, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Copyright Licensing Agency (CANCOPY) received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Library Association, received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Motion Pictures Distributors Association (CMPDA) received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Publishers' Council received on September 18, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canadian Recording Industry Association (CRIA), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from DIRECTV INC. received in both official languages on September 15, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Electronic Frontier Canada received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from The Graduate Student Society of the University of British Columbia received on September 24, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from IBM Canada received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Intellectual Property Institute of Canada (IPIC) received on September 27, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Canada School Boards Association (CSBA), received on September 14, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).

Submission from Society of Composers, Authors and Music Publishers of Canada on September 18, 2001 via e-mail, online: <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01105e.html> (date accessed: 14 December 2002).