Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses, and Technological Protection Measures

Alex Colangelo and Alana Maurushat*

Is computer code speech? While this question has received much consideration in the United States, the issue has yet to come to the forefront in Canada. Considering the nature of software code and its expressive qualities, the authors argue that Canadian courts should take a broad approach with respect to the recognition of software as a protected form of expression under the *Charter of Rights and Freedoms*. The critical question for Canadian courts should not be whether code is a protected form of expression but, rather whether government regulation of software that impedes freedom of expression, is justifiable under section 1 of the *Charter*.

The first part of this article considers the historical underpinnings and policy objectives supporting freedom of speech in the United States and freedom of expression in Canada. Second, the article considers what is meant by computer code. The third part examines the ways in which the court has approached freedom of expression under the *Charter* in cases involving private property and economic rights. Finally, the article critically explores the Canadian approach to freedom of expression and compares it to the American approach using the regulation of three types of technologies: computer viruses, encryption, and technological protection measures.

Un code informatique constitue-t-il une forme d'expression? Alors que cette question a mérité beaucoup d'attention aux Etats-Unis, elle n'a pas encore atteint un tel niveau de popularité au Canada. Considérant la nature du code informatique et ses qualités expressives, les auteurs proposent que les cours canadiennes prennent une approche large lorsqu'il s'agit de la reconnaissance des logiciels comme une forme d'expression protégée par la *Charte canadienne des droits et libertés*. Les cours canadiennes ne devraient pas s'attarder à la question de savoir si le code est une forme d'expression protégée, mais bien à celle de savoir si la réglementation gouvernementale des logiciels, qui entrave la libre expression, est justifiée en vertu de l'article 1 de la *Charte*.

La première partie de cet article considère l'historique et les objectifs des politiques de protection de la libre expression aux Etats-Unis et au Canada. Deuxièmement, l'article considère la signification de «code informatique». La troisième partie de l'article étudie les approches de la Cour à la liberté d'expression protégée par la *Charte* dans les cas impliquant la propriété privée et les droits économiques. Finalement, l'article explore de façon critique l'approche canadienne à la liberté d'expression et la compare à l'approche américaine en utilisant trois types de technologie : les virus, le chiffrement, et les mesures de protection technologiques.

* Alex Colangelo, LL.B. 2001 (University of Western Ontario), LL.M. with Concentration in Law and Technology 2002 (University of Ottawa). I would like to thank my co-author, Alana Maurushat, for her insightful ideas and persistence in preparing this paper for publication. Alana Maurushat, B.A. (University of Calgary), B.C.L. (McGill), LL.B. (McGill), LL.M. with Concentration in Law and Technology (University of Ottawa), joined the University of Hong Kong in 2002 as an Assistant Professor and Deputy Director of the LL.M. in Information Technology and Intellectual Property Programme. She is currently working as an Adjunct Professor at the University of Hong Kong residing in Canada. Prior to taking up an appointment with the HKU Faculty of Law, she worked on several projects with the Government of Canada concerned with adapting intellectual property laws to address the demands and issues of digital technologies, most notably in the areas of digital rights management, centralized electronic licensing, and technological circumvention measures. Her current research is focused on the implications of national firewalls, Smart identity cards, PKI, and other surveillance technologies on free expression and privacy. The authors would also like to thank the editors of the *McGill Law Journal* for their hard work and meticulous attention to detail.

To be cited as: (2006) 51 McGill L.J. 47

Mode de reference : (2006) 51 R.D. McGill 47

Introduction

Is computer code speech? This question has received much consideration in the United States, where courts have wrestled with the issue of whether, and under what circumstances, one should extend First Amendment protection to computer software code. The issue, however, has yet to come to the forefront in Canada. Considering the nature of software code and its expressive qualities, we argue that Canadian courts should take a broad approach in recognizing software as a protected form of expression under the *Charter of Rights and Freedoms*.[1] The critical question for Canadian courts should not be whether code is a protected form of expression, but rather whether government regulation of software that impedes freedom of expression is justifiable under section 1 of the *Charter*.

The first part of this article considers the historical underpinnings and policy objectives supporting freedom of speech in the United States and freedom of expression in Canada. In the American context, freedom of speech has typically meant, in the widest sense, the freedom to publish, which in turn includes the freedom to speak, write, and print.[2] Freedom of expression in Canada, while containing many of the basic elements of freedom of speech, is a consciously broader and more expansive notion. Freedom of expression, as promulgated under the *Charter*, not only protects the right to speak, write, print, and publish but also protects the communication of ideas or opinions through purely physical acts, such as picketing at a labour dispute. Additionally, freedom of expression entails both the communicating and receiving of content. While freedom of speech in the American Constitution is not directly analogous to freedom of expression in the Canadian *Charter*, it may illustrate potential obstacles inherent in the protection of computer code as free expression.

The second part of this article addresses what is meant by computer code, highlighting the ubiquitous and prolific use of computer code in our daily lives. Emphasis will be placed on the importance of recognizing both object and source code as synonymous with language and, to take the metaphor one step further, recognizing computer software as a form of discourse: the use of language to produce a system of knowledge.

The third part examines the ways in which Canadian courts have approached freedom of expression in cases involving private property and economic rights. Given the important role of computer code as discourse and the flaws of a private property and economic rights approach, we argue that computer code should be a protected form of expression.

---

[1] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act, 1982* (U.K.), 1982, c. 11 [*Charter*].

[2] See Robert Martin, *Media Law* (Concord, Ont.: Irwin Law, 1997) at 2.

The fourth part of the article critically explores the Canadian approach to freedom of expression and compares it to the American approach using examples of the regulation of technology. We discuss three types of technologies: computer viruses, encryption, and technological protection measures. These examples have been selected to highlight the competing tensions in protecting computer code as expression. Case law from the United States and Canada are examined, focusing upon the arguments made for the protection of software and the courts' findings regarding software code. Starting from the platform that computer code is a protected form of expression, we consider "expression" from a Canadian perspective and suggest how Canadian courts might deal with analyses under the limitation provision of section 1 of the *Charter*.

I. Historical Underpinnings and Policy Objectives

A. Free Speech and the American Constitution

Freedom of speech is protected in the United States under the First Amendment, which states that "Congress shall make no law ... abridging the freedom of speech, or of the press ... ."[3] In analyzing this amendment, courts and academics have advanced two major theories to explain the rationale behind the protection of freedom of speech: the utilitarian theory and the libertarian theory.[4]

The utilitarian theory of free speech espouses the idea that speech is a tool to advance truth, democracy, and the exchange of ideas.[5] This theory was advanced by Justice Brennan of the United States Supreme Court in *Roth v. United States*,[6] where he stated that "[t]he protection given speech and press was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[7]

---

[3] U.S. Const. amend. I.

[4] The "utilitarian theory" is most readily associated with the works of John Stuart Mill. See J.S. Mill, "On Liberty" in R.B. McCallum, ed., *On Liberty and Considerations on Representative Government by J.S. Mill* (Oxford: Basil Blackwell, 1946). For a useful discussion of libertarianism, see Jan Narveson, *The Libertarian Idea* (Philadelphia: Temple University Press, 1988). See also Eric Barendt, *Freedom of Speech* (Oxford: Clarendon Press, 1987) at 8-23 for a brief discussion of three of the most prevalent arguments in favour of free speech.

[5] See Richard Moon, *The Constitutional Protection of Freedom of Expression* (Toronto: University of Toronto Press, 2000) at 8-31 [Moon, "Constitutional Protection"].

[6] 354 U.S. 476 at 484 (1957).

[7] *Ibid*. Justice Brennan attributed this idea to a letter written in 1774 by the Continental Congress to the inhabitants of Quebec. The section states:

> The last right we shall mention, regards the freedom of the press. The importance of this consists, besides the advancement of truth, science, morality, and arts in general, in its diffusion of liberal sentiments on the administration of Government, its ready communication of thoughts between subjects, and its consequential promotion of union

Libertarian theory, meanwhile, maintains that the protection of speech is an end in itself, which secures dignity by protecting an individual's right to develop intellectually and spiritually through expressive means.[8] In describing this idea, Justice Harlan of the United States Supreme Court wrote that

> [t]he constitutional right of free expression ... put[s] the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity and in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests.[9]

The libertarian model thus seeks to protect individual self-determination rather than any specific right.

The historical foundation of the First Amendment in the United States Constitution carries great weight in the interpretation that American courts have given to different forms of speech. Rhetoric surrounding the First Amendment often invokes sacrosanct sentiment.[10] America's revolutionary historical foundation has, in many ways, made the American treatment of free speech far more steadfast and absolute in its approach than its Canadian equivalent. The American free speech protection, furthermore, uses the word "speech," which is narrower than the Canadian term "expression."[11] Framed in absolute language,[12] the American Bill of Rights also does

---

> among them, whereby oppressive officers are shamed or intimidated, into more honourable and just modes of conducting affairs ("Letter to the Inhabitants of Quebec" (1774) 1 Journals of the Continental Congress 108, cited in *ibid.*).

[8] Barendt, *supra* note 4 at 14-20.

[9] *Cohen v. California*, 403 U.S. 15 at 24, 91 S. Ct. 1780, 29 L. Ed. 2d 284 (1971) [cited to U.S.].

[10] See *e.g.* Jonathan W. Emord, *Freedom, Technology and the First Amendment* (San Francisco: Pacific Research Institute for Public Policy, 1991). Emord writes:

> Comprehending the philosophical grounds that led our ancestors to risk incarceration and to sacrifice their lives in the fight to secure the freedom of speech and press is the essential first step in understanding the meaning of that freedom. To avoid the mistakes of past regimes whose transgressions of fundamental liberties fomented strife and revolution, we must understand our history. We must always bear in mind that the freedom we define is not ours individually to change. The freedom of speech and press is rightly regarded by the American people as theirs; we each share in this sovereign right, and not a single one of us possesses a legitimate power to fundamentally redefine it (*ibid.* at 18).

Similarly, Sableman suggests that "because this tumult [engendered by free speech] arises out of the underlying principle of liberty, our society for the most part accepts and even embraces it. It is, after all, part of the 'crowning glory of our country'" (Mark Sableman, *More Speech, Not Less: Communications Law in the Information Age* (Carbondale, Ill.: Southern Illinois University Press, 1997 at 5-6).

[11] Peter W. Hogg, *Constitutional Law of Canada*, student ed. (Scarborough, Ont.: Carswell, 1998).

[12] The absolutist interpretation of the language of free speech found in the United States Constitution is reviewed in Alexander Meiklejohn, "The First Amendment Is an Absolute" in Kent Middleton & Roy M. Mersky, eds., *Freedom of Expression: A Collection of Best Writings* (Buffalo, N.Y.: William S. Hein & Co., 1981) 63.

not contain a limitation clause equivalent to section 1 of the *Charter* allowing for the infringement of certain freedoms where demonstrably justified.[13] The absolute nature of the First Amendment has, thus, precluded any "principled justification for upholding laws that restrict speech."[14]

Ascertaining the applicable First Amendment test from American jurisprudence is difficult because several tests have emerged from the courts. The case of *Spence v. Washington*[15] determines whether the conduct in question is subject to First Amendment protection. If the conduct is deemed protected, the court must characterize the impending regulation. American courts have not adopted a contextual approach to free expression, but rather have opted for a categorical and analogous approach.[16] Legislation affecting the Internet has been analogized to media and communications regulation. In the area of media regulation, the court must ascertain whether the regulation is content-based or content-neutral. Each of these categories utilizes a different set of established doctrines to determine whether the restriction of free speech is valid. As Knutsen explains:

> A content-based restriction on expression involves regulating the expression because of the message it conveys. If the expression is distinguished from other expression based on whether or not it is considered "disfavored speech," such as harmful, indecent, or obscene expression, the regulation is content-based. ... Content-based restrictions on media invoke "the most exacting" judicial standard of strict scrutiny when courts evaluate the proposed regulation's [effect] on freedom of expression. The government regulation must serve a compelling, narrowly tailored state interest and must impinge freedom of expression in the least restrictive means possible.
>
> A content-neutral restriction on expression does not restrict on the basis of the ideas or views expressed in the expression. Media regulation which purports to control access to a medium of communication that is perceived to be in some scarcity is content-neutral regulation. ... Content-neutral regulation is subject to an intermediate standard of scrutiny if it can be proven that the aim of the regulation is not to burden expression based on the message contained in the expression. To pass this standard, a government must prove there exists a

---

[13] Hogg, *supra* note 11 at 831.

[14] *Ibid.*

[15] 418 U.S. 405, 94 S. Ct. 2727, 41 L. Ed. 2d (1974) [*Spence* cited to U.S.]. *Spence* involved a college student who was protesting the American invasion of Cambodia and the killing at Kent State. The student attached a peace symbol to an American flag and hung the flag outside of his apartment building contrary to a Washington statute that prohibited the "improper use" of a flag. To determine whether an action should be afforded free speech protection, the court reasoned that the "appellant did not choose to articulate his views through printed or spoken words. It is therefore necessary to determine whether his activity was sufficiently imbued with elements of communication to fall within the scope of the First and Fourteenth Amendments ... " (*ibid.* at 409). In the case at hand, the court found that the student's use of the flag did in fact fall within First Amendment coverage.

[16] See Erik S. Knutsen, "Techno-neutrality of Freedom of Expression in New Media Beyond the Internet: Solutions for the United States and Canada" (2001) 8 UCLA Ent. L. Rev. 87. The author expresses that the categorical and analogous approach in the U.S. has led to inconsistent precedents.

> substantial state interest that is demonstrated by government regulation that restricts freedom of expression only to an intermediate degree.[17]

The prevalent view of free speech in the United States is that the government is not the appropriate authority to act as a censor and has, therefore, adopted the most permissive free speech legal framework.[18] Censorship is less pervasive, self-perpetuated, or done through private citizens.[19]

B. Freedom of Expression in the Canadian Charter of Rights and Freedoms

Freedom of expression is a constitutional right under subsection 2(b) of the *Charter*.[20] To successfully raise a *Charter* claim, a litigant must characterize the impugned act as being an "action taken under statutory authority".[21] Subsection 2(b)

---

[17] Knutsen, *ibid.* at 93-95 [footnotes omitted]. For a discussion of the judicial standard of strict scrutiny, see *United States v. O'Brien*, 391 U.S. 367, 88 S. Ct. 1673, 20 L. Ed. 2d 672 (1968) [*O'Brien*], which established a standard for assessing content-based restrictions.

[18] See *e.g.* Sableman, *supra* note 10; The Georgetown Law Journal, *Media and the First Amendment in a Free Society* (Amherst, Mass.: The University of Massachusetts Press, 1973); Emord, *supra* note 10; William Ernest Hocking, *Freedom of the Press: A Framework of Principle* (New York: Da Capo Press, 1972); Franklyn S. Haiman, *Speech and Law in a Free Society* (Chicago: University of Chicago Press, 1981); Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge: Belknap Press of Harvard University Press, 1983); and Fred R. Berger, *Freedom, Rights and Pornography: A Collection of Papers by Fred R. Berger*, ed. by Bruce Russell (Dordrecht, Neth.: Kluwer Academic Publishers, 1991).

[19] Emord asserts that the government "poses the greatest, most pervasive threat to preserving liberty of speech and the press" and that the speech ban imposed by the Beijing government after the Tiananmen Square massacre is a far more serious threat to liberty of speech and the press than the decision by certain book vendors to abstain from selling Salman Rushdie's *The Satanic Verses* (*supra* note 10 at 7-8). Unfortunately, Emord misses what has become a truism of the Internet and digital technology in general: that it is not the government who regulates but it is, increasingly, private parties. The most famous quip is one of Lawrence Lessig's, namely that computer code is a form of law (Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 6). Emord's concern, therefore, is somewhat misplaced in the digital age. One must remember, however, that Emord's book was published in 1991, so a more charitable review should be given to his interpretation.

Other arguments supporting the claim that free speech concerns are lessened in the realm of the private market stem from resource allocation theory. An oversimplified version of this theory is that government by its nature is a monopoly, and, therefore, when it regulates, it is more likely to offend free speech principles. Private parties, in contrast, operate based on resource allocation, in relation to a given market. The net effect is the following proclamation: "distributed wisdom among the property holders is greater than that of a central planner" (de Sola Pool, *ibid.* at 236). The central planner in this situation is either a market monopoly or a government monopoly. The larger number of parties involved, therefore, help ensure that free speech will prevail. See *e.g.* de Sola Pool, *ibid.* at 234ff.

[20] *Supra* note 1.

[21] Hogg, *supra* note 11 at 34-12.1. For a thorough analysis of case law relating to freedom of expression see Claire Saint-Louis Marcouiller, *La Charte Canadienne des Droits et Libertés et le Domaine Constitutionnel de L'Expression Commerciale* (Ottawa: University of Ottawa, 1993).

of the *Charter* guarantees Canadians the "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."[22]

There are three main rationales for the protection of freedom of expression in Canada.[23] The first closely resembles the utilitarian theory of American jurisprudence. In *Switzman v. Elbling*, the Supreme Court of Canada found that "[t]he right of free expression of opinion and of criticism" is "essential to the working of a parliamentary democracy such as ours."[24] The persuasiveness of this rationale is evident in the protection of such democratic expression even before the advent of the *Charter*. "Canadian judges have always placed a high value on freedom of expression as an element of parliamentary democracy and have sought to protect it with the limited tools that were at their disposal before the adoption of the Charter of Rights."[25]

The second rationale conceives of protection of the freedom of expression "as an instrument of truth."[26] This includes the protection of "philosophy, history, the social sciences, the natural sciences, medicine and all the other branches of human knowledge."[27]

The third rationale for the protection of the freedom of expression recognizes expression as an "instrument of personal fulfilment."[28] Similar to the American libertarian rationale, this reason for protection recognizes the need to protect expression as an avenue for personal growth and self-realization.[29]

The Supreme Court of Canada accepted these three reasons in the case of *Irwin Toy v. Quebec*, finding that "(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-fulfilment and human flourishing ought to be cultivated."[30] The Court further established the parameters of subsection 2(b) of the *Charter* in this case. The Court adopted a broad reading of protected forms of expression and put forth a methodology for determining justifiable limits to this scope of protection. The full methodology, however, for subsection 2(b) evolved from four key decisions: *Irwin Toy*, *Edmonton Journal v. Alberta (A.G.)*,[31] *Rocket v. Royal College of Dental Surgeons of Ontario*,[32] and *R. v. Keegstra*.[33]

---

[22] *Supra* note 1, s. 2(b).
[23] Hogg , *supra* note 11 at 831-33. See also Moon, "Constitutional Protection", *supra* note 5 at 8-31.
[24] [1957] S.C.R. 285 at 326, 7 D.L.R. (2d) 337.
[25] Hogg, *supra* note 11 at 831.
[26] *Ibid.* at 832.
[27] *Ibid.*
[28] *Ibid.*
[29] *Ibid.* See also Moon, "Constitutional Protection", *supra* note 5 at 19-21.
[30] *Irwin Toy Ltd. v. Quebec (A.G.)*, [1989] 1 S.C.R. 927 at 976, 58 D.L.R. (4th) 577, [*Irwin Toy* cited to S.C.R.] (criteria established in *Ford v. Quebec (A.G.)* [1988] 2 S.C.R. 712, 54 D.L.R. (4th) 577).
[31] [1989] 2 S.C.R. 1326, 64 D.L.R. (4th) 577 [*Edmonton Journal* cited to S.C.R.].
[32] [1990] 2 S.C.R. 232, 71 D.L.R. (4th) 68 [*Rocket* cited to S.C.R.].
[33] [1990] 3 S.C.R. 697, [1991] 2 W.W.R. 1 [*Keegstra* cited to S.C.R.].

In *Irwin Toy*, the Court held in broad and abstract terms that any activity intending to convey meaning is prima facie protected expression. Under subsection 2(b) of the *Charter* "everyone can manifest their thoughts, opinions, beliefs, indeed all expressions of the heart and mind, however unpopular, distasteful or contrary to the mainstream."[34] Under *Irwin Toy,* once an activity falls within the scope of subsection 2(b) a court will consider whether either the purpose or the effect of the government action is to restrict the content of expression. If it is only the effect of the legislation that infringes a *Charter* right, the claimant must then demonstrate that his or her expressive activity conforms to the three principles underlying freedom of expression. More specifically, the activity must conform to the principles and values underlying the protection of free expression: an activity will not be protected simply because it has an expressive element. It is also necessary to demonstrate that the effect of the government's action was to restrict free expression and that the plaintiff's activity promotes at least one of the three stated principles.

If a court finds that the measure in question violates subsection 2(b) of the *Charter*, the court will then determine whether the measures are "reasonable limits prescribed by law ... demonstrably justified in a free and democratic society" within the meaning of section 1 of the *Charter*. The justification of a legislative provision under section 1 utilizes the test announced in the Supreme Court decision of *R. v. Oakes*:[35] once a court determines that legislation infringes upon a *Charter*-protected right, the government bears the burden of demonstrating that the infringement of the right is saved by section 1.

The *Oakes* test is two-pronged. The first step of the test determines whether there is a pressing and substantial purpose. The second step determines proportionality: the legislation must be proportional in its purpose and effect. The proportionality component of the test is, in turn, comprised of three sub-elements. First, there must be a rational connection to the objectives of the law. Second, the law must minimally impair the rights and freedoms. Third, the effects of the law and legislative objective must be proportionate to one another so as to find an appropriate balance between the deleterious and salutary effects.

The rational connection subcomponent stresses that "the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective."[36] The second prong of the proportionality test requires that the government action employ the least drastic means possible in infringing the protected right.[37] This subcomponent has received the most attention in the case law and is often the determinative element in the *Oakes* test. The third subcomponent considers the "proportionality between the deleterious and the salutary effects of the

[34] *Supra* note 30 at 968.
[35] [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200 [*Oakes* cited to S.C.R.].
[36] *Ibid.* at 139.
[37] *Ibid.*

measures"[38] or, put another way, that the burden on rights and freedoms does not outweigh the benefits of the law. This last branch has received the least amount of judicial consideration.

The Supreme Court, in *Irwin Toy*, expressly rejected the notion of hierarchical forms or categories of expression, opting instead for a broad interpretation. While all content is protected under the *Charter*, not all forms of expression are protected. In *Irwin Toy*, the Court specifically excluded violent forms of expression from protection, while leaving the category of excluded forms of expression open to further exceptions. The general reading of this decision is that a very broad interpretation is to be given to the scope of freedom of expression. The principle is that the content or value of expression is irrelevant; if expression conveys meaning, then it is protected under subsection 2(b). The limits on free expression, meanwhile, are delineated in the section 1 analysis. The nexus between the freedom of expression analysis in *Irwin Toy* and the limits set forth in the *Oakes* test is further developed in the subsequent judgments of *Edmonton Journal* and *Rocket*.

The Supreme Court, in *Edmonton Journal*, grappled with new methodologies for looking at the Court's section 1 analysis in *Irwin Toy*. A new, contextual approach was offered in dissent by Justice Wilson as an alternative to the approach taken in *Irwin Toy*. This contextual approach asserts that "the importance of the right or freedom must be assessed in context" under section 1. Although the Court did not adopt this contextual analysis in *Edmonton Journal*, it later endorsed it in *Rocket* and elaborated upon it in *Keegstra*. As one commentator noted:

> Under *Irwin Toy*, the standard of review depended on the government's rationale and in particular, whether the state had acted as the singular antagonist of the individual or in a capacity that advanced the traditional values of democratic governance. While those adjustments to *Oakes* retained section 1's focus on the question of justification, the contextual approach suggested, to the contrary, that the value of the expressive activity should determine the stringency of review.[39]

The Supreme Court, in *Keegstra*, modified the broad and abstract approach to protected speech so that it assigned a value to the expressive activity. Explaining the contextual approach, the Court found that "the expression *at stake in a particular case*" must be examined to determine whether the content reflects the values of subsection 2(b).[40] The Court distinguished content that is at the core of subsection 2(b) from content that is merely "tenuously connected" to the values of subsection 2(b).[41] The degree of connectivity between the content of expression and the values of

---

[38] *Dagenais v. Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835 at 889, 120 D.L.R. (4th) 12 [emphasis omitted].

[39] Jamie Cameron, "The Past, Present, and Future of Expressive Freedom under the *Charter*" (1997) 35 Osgoode Hall L.J. 1 at 15.

[40] *Keegstra*, *supra* note 33 at 760 [emphasis in original].

[41] *Ibid.* at 761.

subsection 2(b) determines the stringency of review under section 1 of the *Charter*. In the case at hand, the Court ruled that hate propaganda was of "limited importance when measured against free expression values,"[42] and held that such speech did not conform to the principles underlying freedom of expression: truth, participation in political and social decision making, and individual self-fulfillment.

While Canada has accepted a very broad and abstract definition of expression, the scope of protection is restricted where notions of "public order" compete with the values that underpin free expression. Protecting society from harmful, hateful, obscene, or violent speech is understood as contributing towards public order or, as it is often referred to, the public interest. Likewise, courts have been reticent to afford protection to modes of expression that interfere with private property or economic rights.[43] Canadian courts, in a somewhat complicated maze of free expression doctrine, have outlined an approach that requires balancing: between public interest and an individual's private interest (e.g., the effects of racist speech on society versus an individual's right to espouse such beliefs);[44] between competing rights and *Charter* freedoms (e.g., property rights versus freedom of expression); and between potentially conflicting *Charter* rights (e.g., freedom of religion versus freedom of expression).

As previously stated, American constitutional protection of free speech is written in language that is narrower and more absolute than its Canadian counterpart. American courts have nonetheless fashioned a framework not dissimilar to that found in the Canadian context. On a theoretical basis, the *Spence* test works somewhat like the test for expression under *Irwin Toy* considering the scope of protection. The strict scrutiny test established in *United States v. O'Brien* parallels many of the ideas of *Oakes*.[45] The notion of "sufficiently important government interest," however, does not extend to the Canadian equivalent of "public interest" or "public order" limitation, and is, in turn, dependent on the type of speech in question. As we have seen, content-based speech is not subject to the same evaluation as content-neutral speech.[46] Another example often employed to illustrate the notional interpretations of free expression is the protection of hate speech. In the United States, such forms of

---

[42] *Ibid.* at 762.

[43] See *e.g. Compagnie Générale des Établissements Michelin-Michelin & Cie v. National Automobile, Aerospace, Transportation and General Workers Union of Canada* (1996), [1997] 2 F.C. 306, 124 F.T.R. 192, 71 C.P.R. (3d) [*Michelin* cited to F.C.].

[44] *R. v. Zundel*, [1992] 2 S.C.R. 731, 95 D.L.R. (4th) 202 [*Zundel* cited to S.C.R.].

[45] *O'Brien*, *supra* note 17.

[46] See *e.g. American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473, 14 Comm. Reg. (P & F) 1145, 27 Media L. Rep. (BNA) 1449 at 493ff (E.D. Pa. 1999) [*ACLU v. Reno* cited to F. Supp. 2d], aff'd sub nom. *Ashcroft v. American Civil Liberties Union*, 52 U.S. 656, 124 S. Ct. 2783, 159 L.Ed.2d 690 (2004), where the Pennsylvania District Court highlighted different approaches to free speech under the law of the United States of America.

propaganda enjoy full protection and are not subject to limitations.[47] Canada, by contrast, has set limits on the protection afforded to hate speech.[48]

II. Computer Code as a Protected Form of Expression

The term "computer code" refers to "instructions meant to direct the execution of a computer."[49] This definition includes operating software such as Microsoft Windows, application software such as Adobe Photoshop, and even embedded instructions in pocket calculators.[50] "Code" can be divided into two categories: "source code" and "object code".[51]

A. Source Code

A piece of software is typically first written in source code.[52] Source code is the actual text of the program that is written in a high-level programming language by the human programmers.[53] Programming languages are similar to conventional languages in that they contain grammatical rules to ensure that programs are comprehensible to others trained in the language.[54] In writing source code, computer programmers must follow the syntax, punctuation, and format of the chosen programming language.[55] Source code resembles English instructions, making it easier for computer programmers versed in the programming language to read, write, and modify the programs.[56] A source code program usually consists of "English words and mathematical symbols that demonstrate the exact steps the computer should be performing."[57] A computer, however, cannot make use of the source code until it is first translated into machine-readable language, known as "object code."[58]

---

[47] Sableman discusses a 1977 case in the United States where a small group of Nazis marched in Skokie, Illinois, a community with a large Jewish population—many of whom had survived the Holocaust. The courts upheld the right of the Nazis to march (Sableman, *supra* note 10 at 4).

[48] See *Zundel*, *supra* note 44. While the promulgation of anti-Semitic rhetoric was a form of protected expression, regulations against such hate speech were held to be justifiable under section 1 of the *Charter*.

[49] Ryan Christopher Fox, "Old Law and New Technology: The Problem of Computer Code and the First Amendment" (2002) 49 UCLA L. Rev. 871 at 876.

[50] *Ibid.*

[51] *Ibid.*

[52] Casey P. August & Derek K.W. Smith, "Software Expression (SSO), Interfaces, and Reverse Assembly" (1994) 10 C.I.P.R. 679 at 680.

[53] *Bernstein v. United States (Department of Justice)*, 176 F. 3d 1132 (9th Cir. 1999) [*Bernstein*].

[54] Steven E. Halpern, "Harmonizing the Convergence of Medium, Expression, and Functionality: A Study of the Speech Interest in Computer Software" (2000) 14 Harv. J.L. & Tech. 139 at 143.

[55] *Ibid.*

[56] *Bernstein*, *supra* note 53 at 1140.

[57] Fox, *supra* note 49 at 877.

[58] *Bernstein*, *supra* note 53 at 1140.

B. Object Code

Object code consists of "the pure instructional data that is created to run directly on a computer's processor."[59] It is often referred to as assembly code. Object code is produced by converting source code into strings of ones and zeros that the computer can understand.[60] The conversion is accomplished by employing a "compiler", a computer program designed to translate source code into the binary format necessary for the computer to understand the instructions, while creating a program that still "performs a function equivalent to that expressed in the source code."[61]

C. Software as Discourse

It can be argued that computer software is more than merely source or object code. Characterizing computer code simply as source or object code is to limit its description to its functional nature. Computer code occupies a field much larger than its mere function; it consists of languages that contribute to produce a system of knowledge—in short, discourse. Drawing from post-structuralist writings and theories of identity politics, Brian Fitzgerald, in the Seventh Annual Herbert Tenzer Distinguished Lecture in Intellectual Property Law in 1999 at the Cardozo School of Law, addressed the importance of software as a medium for communication and the pivotal role it plays in our social structure.[62] Professor Fitzgerald concluded that software must be seen as a form of discourse and not merely as a functional technology.[63] For the purpose of examining the legal implications of this argument, the relevant test becomes whether computer code is sufficiently expressive so as to fall under the protection of the *Charter*.

The expressiveness of computer code can be seen in the creativity employed to create software. Source code contains the "original selection and arrangement of lines of code and of groupings or subroutines of code lines."[64] A computer function can be performed in alternative computer languages and with a different selection and arrangement of lines of code.[65] This selection of lines of code is also important academically. Computer science is a field where professors, academics, and

---

[59] Fox, *supra* note 49 at 880.

[60] August & Smith, *supra* note 52 at 680.

[61] Fox, *supra* note 49 at 880.

[62] For an adaptation of the lecture, see Brian F. Fitzgerald, "Software as Discourse: The Power of Intellectual Property in Digital Architecture" (2000) 18 Cardozo Arts & Ent. L.J. 337. To name but a few, the author uses the works of philosophers Foucault, Derrida, Baudrillard, and Heidegger to define the contours of discourse, and to illustrate how software impacts on such discursive formation to form a powerful communication tool.

[63] Similar arguments have been made by Jack M. Balkin. Balkin wrote of how digital technologies change the social conditions of communication, in particular how technology democratizes speech (Jack M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society" (2004) 79 N.Y.U.L. Rev. 1).

[64] August & Smith, *supra* note 52 at 680.

[65] *Ibid.*

programmers "write hundreds of volumes of text every year describing algorithms, methods, and data structures."[66] "Good software design has become a sort of *cause célèbre* among computer programmers in the last decade ... [w]hat is important is to understand that the structure of source code can be modified not just for purposes of efficiency or history, but also to further its use in intellectual discussion, or even to follow or buck trends."[67]

There is no doubt that computer programs are highly individualistic in nature and contain a form of expression personal to the individual programmer. No two programmers would ever write a program in exactly the same way (except perhaps in the case of the simplest program). Even the same programmer, after writing a program and leaving it for some time, would not write the program the same way on a second occasion; the sequence of instructions would certainly be different. The possibility of two programmers creating identical programs without copying has been compared by the Federal Court to the likelihood of a monkey sitting at a typewriter producing Shakespeare.[68] The same holds true of the likelihood of two individuals producing the same book chapter or music score.

Canadian courts must also recognize the importance of software to communication between those who use it. Software developers use code like "mathematicians use equations[,] ... economists use graphs", and musicians use musical scores.[69] Computer software also pervades many facets of our lives, so much so that it is almost taken for granted: the world wide web protocol (www) we systematically use to navigate websites; the search engine software employed to find the website we seek; the swipe of the debit card to make an instant purchase; the computer chip embedded in our driver's licence; the operating systems of cars and appliances; and the thousands of programs that facilitate communication in wireless, satellite, and Internet technologies. Viewed in this light, it is clear that the creation and dissemination of software code satisfy the principles of seeking truth, attaining individual self-fulfillment, and allowing for human-flourishing, all of which govern the freedom of expression guarantees in the *Charter*.

The creation of object code, meanwhile, requires that a computer programmer first express creativity by creating the source code. While the eventual object code may simply be a string of ones and zeros, the object code is still a manifestation of the creativity and expression of the computer programmer.

The expressiveness of software is not without support in Canada. In *Apple Computer v. Mackintosh Computers Ltd.*,[70] Justice Reed of the Federal Court made several references to the literary and expressive qualities of both the source and object

---

[66] Fox, *supra* note 49 at 879.

[67] *Ibid.* at 878-79 [footnotes omitted].

[68] *Apple Computer v. Mackintosh Computers Ltd.* (1986), [1987] 1 F.C. 173, 28 D.L.R. (4th) 178 at 184, 10 C.P.R. (3d) 1 [*Apple* cited to D.L.R.].

[69] *Bernstein*, *supra* note 53 at 1141.

[70] *Supra* note 68.

code utilized in computer programs. Referring to the definition of translation from the traditional literary perspective, Justice Reed wrote that "the conversion of a work into a code, or the conversion of a work originally written in one code into another code constitutes a translation ... ."[71] She added that "[t]he computer program when written is clearly a literary work. What is more, its embodiment in a silicon chip retains the form of expression of the original work."[72]

As mentioned above, the Supreme Court in *Irwin Toy* expressly rejected the notion of hierarchical forms of expression, opting instead for a broad interpretation. It said that an "[a]ctivity is expressive if it attempts to convey meaning."[73] All content is protected under the *Charter*, although not all forms of expression are protected. Arguably, the path from idea to human language to source code to object code is a continuum. Computer code, whether source or object, is a means of expressing ideas. It can be said that computer code, used both to encrypt and decrypt, conveys meaning so that it falls within the purview of subsection 2(b) of the *Charter*. There have been many court decisions, however, that have either failed altogether to apply the Supreme Court test in *Irwin Toy* or have misapplied its principles, as will be examined in the next section.

III. Computer Code as Private Property/Economic Rights

Where private property and economic rights are concerned, the courts have readily excluded forms of expression from the scope of subsection 2(b). By doing so, the courts have frequently halted free expression analysis at the first step of the *Irwin Toy* test. This narrow analysis precludes the court from addressing the remaining steps: first, whether the purpose or effects of a legislative provision impede freedom of expression; and second, in the event that the right to freedom of expression has been violated, whether this impediment is justified.

What is perhaps most curious is the stark dichotomy in the protection afforded to modes of expression that affect public interest and those that interfere with private property and economic rights. By way of example, when the Supreme Court dealt with child pornography,[74] hate speech,[75] and homosexual pornography,[76] a broad approach resulted in finding that such expressions were protected forms of expression. On the contrary, where private property and economic rights were involved, courts have adopted a different approach. In the latter context—as will be shown in the remainder of this section—the form of expression in question was not

---

[71] *Apple*, *ibid.* at 198.
[72] *Ibid.* at 201.
[73] *Irwin Toy*, *supra* note 30 at 968.
[74] *R. v. Sharpe*, [2001] 1 S.C.R. 45, 194 D.L.R. (4th) 1, 2001 SCC 2 [*Sharpe* cited to S.C.R.].
[75] *Zundel*, *supra* note 44.
[76] *Little Sisters Book and Art Emporium v. Canada (Minister of Justice)*, [2000] 2 S.C.R. 1120, 193 D.L.R. (4th) 193, 2000 SCC 69. "Homosexual pornography" is somewhat of a misnomer, as one of the issues in this case was whether the said works in question should be classified as pornographic.

seen as a protected one. Private property and economic rights issues are often manifest in situations involving copyright protection.

The Canadian *Copyright Act*,[77] grants various protections to "every original literary, dramatic, musical and artistic work ... ."[78] A "computer program," defined as "a set of instructions or statements, expressed, fixed, embodied or stored in any manner, that is to be used directly or indirectly in a computer in order to bring about a specific result," is considered a "literary work" for the purposes of the *Copyright Act*.[79] The *Copyright Act* encourages the creation of original works by, among other things, prohibiting the copying or distribution of copyrighted works without the author's consent, except under limited circumstances.[80] Such a regime induces authors to create by prohibiting others from profiting from the author's work. As will be demonstrated by the cases below, striking a balance between the private property rights created by the *Copyright Act* and the constitutional right to freedom of expression is a difficult and sometimes controversial proposition.

In *Michelin*, the Federal Court considered whether the use of the defendant's trade name in a labour union dispute was a form of protected expression.[81] The Federal Court held that the labour union's depiction of the Michelin logo constituted copyright infringement. Parody was not considered a form of "criticism" and, therefore, was not an exception to copyright infringement. Ultimately, the court held that this was a prohibited form of expression and did not fall within the scope of protected expression; the *Charter* does not confer the right to the use of private property in the name of freedom of expression. The court highlighted that "[w]e should guard against our instincts ... to undervalue the nature of the plaintiff's copyright and overestimate the breadth of the defendants' freedom of expression."[82] This strong language demonstrates the court's reluctance to advance the right of free expression over competing rights such as the right of the individual to the enjoyment of property. The court did not find it necessary to move to the second branch of the *Irwin Toy* test, nor to determine whether the provisions of the *Copyright Act* could be justified under section 1 of the *Charter*.

In the case of *New Brunswick Broadcasting Co. Ltd. v. Canada (Radio-television and Telecommunications Commission)*, the court asserted that property rights in encrypted data may take priority over the right of expression.[83] The court held that the refusal of a licence under the *Broadcasting Act*[84] did not constitute a restriction on

---

[77] R.S.C. 1985, c. C-42.

[78] *Ibid.*, s. 5(1).

[79] *Ibid.*, ss. 2§5.5 and 2§5.0, respectively.

[80] *Ibid.*, s. 27. See also the "Fair Dealing" section, s. 29, for a circumstance where it is lawful to copy or distribute copyright material.

[81] *Supra* note 43.

[82] *Ibid.* at 376.

[83] [1984] 2 F.C. 410, 13 D.L.R. (4th) 77, 2 C.P.R. (3d) 433. The court held that the refusal of a license under the *Broadcasting Act* did not constitute a restriction on freedom of expression.

[84] R.S.C. 1991, c. 11.

freedom of expression. Similarly, in *R. v. Drainville*,[85] it was held that the freedom of expression did not protect a right to use another's property.

In *Productions Avanti Ciné-Vidéo v. Favreau*,[86] the Quebec Court of Appeal noted that the appropriation of a work of another for criticism or comment had to be distinguished from doing so for commercial purposes. Moreover, the court emphasized the need "to make the proper distinctions in each case having regard to copyright protection as well as freedom of expression."[87] In its analysis the court acknowledged that parody was a form of "criticism" within the *Copyright Act* and could, therefore, be a form of protected expression.[88] No reference was made to the test articulated in *Irwin Toy.*

Meanwhile, there is debate as to whether sections 9 and 10 of the *Radiocommunication Act*[89] violate freedom of expression. Although there has not been a decision by the Supreme Court directly addressing this issue, the courts have indicated that freedom of expression in this context is subject to limitations. Reference has been made to the fact that although freedom of expression extends to recipients, it also applies to the originators of a communication.[90] Recently, a number of *Charter* challenges have been launched contesting the constitutionality of sections 9 and 10 of the *Radiocommunication Act.*[91] For example, paragraph 9(1)(c) of the *Radiocommunication Act* provides that:

> [n]o person shall decode an encrypted subscription programming signal or encrypted network feed otherwise than under and in accordance with an authorization from the lawful distributor of the signal or feed.[92]

This section was challenged in *Bell ExpressVu Limited Partnership v. Rex*, a case considering the legality of Canadian access to American satellite signals.[93] While finally bringing certainty to the proper interpretation of paragraph 9(1)(c) of the *Radiocommunication Act*, the Supreme Court left open the possibility of a *Charter*

---

[85] (1991), 5 C.R. (4th) 38, [1992] 3 C.N.L.R. 44.

[86] *Productions Avanti Ciné-Vidéo inc. v. Favreau*, [1999] R.J.Q. 1939, 177 D.L.R. (4th) 568, 1 C.P.R. (4th) 129 (C.A.) [cited to D.L.R.], leave to appeal to S.C.C. refused, [2000] 1 S.C.R. xi.

[87] *Ibid.* at 575.

[88] As the defendant's actions did not constitute parody, the court concluded that the actions were not a form of protected expression.

[89] R.S.C. 1985, c. R-2.

[90] See Tarnopolsky J.A.'s support of a broad interpretation of the freedom of expression in *R. v. Videoflicks* (1984), 48 O.R. (2d) 395, 14 D.L.R. (4th) 10, 15 C.C.C. (3d) 353 (C.A.).

[91] See *e.g.* the ongoing litigation involving Jacques D'Argy and Richard Thériault, *infra* notes 94, 101, and 102 as well as *WIC Premium Television Ltd. v. General Instrument Corp*. (1999), 253 A.R. 153 (Q.B.) [*WIC*]. In an application to strike certain portions of the statement of claim in *WIC*, the judge commented that an argument based on s. 2(b) of the *Charter* is really an attempt to protect commercial interests. The defendants will likely argue this issue more fully at trial.

[92] *Supra* note 89, s. 9(1)(c).

[93] [2002] 2 S.C.R. 559, 212 D.L.R. 4th 1, 2002 SCC 42.

challenge to the provision based on freedom of expression, as it found that the material submitted for the case was insufficient for it to properly consider the issue.[94]

Recently, the Court of Quebec considered a case involving Jacques D'Argy and Richard Thériault,[95] and found paragraphs 9(1)(c) and 10(1)(b) of the *Radiocommunication Act* unconstitutional as they infringed the right to freedom of expression. This case is important because it marks the first time that a Canadian court issued a lengthy and detailed analysis of freedom of expression in the context of private property and economic rights and, albeit somewhat indirectly, computer code. The case involved the use of smart card technology (computer code) to decrypt the protection of satellite programs. At issue was the reception of an American satellite service known as DIRECTV.[96]

In order to access DIRECTV, Canadians can use two methods: using a false mailing address or, circumventing the encryption technology of the satellite decoder. In the case of a false mailing address, a Canadian purchaser of American satellite equipment acquires an American mailing address and submit payments using that address. Under this method, American satellite broadcasters treat the Canadian receiver of signals as a legal American purchaser, and remotely activate the customer's smart card thus allowing for the decryption of the satellite broadcast. In such cases, the Canadian resident pays an identical amount for the programming package as does an American resident.[97] The court referred to this situation as "grey market".

In the case of encryption circumvention, viewers download decryption software available on the Internet and transfer the software code directly onto the smart card. In other words, programmers "hack" the satellite smart card rather than paying an American satellite provider for authorization to unscramble the satellite signals. These "pirate" cards can be purchased in Canada from satellite dealers and reprogrammed periodically to stay ahead of broadcaster changes to the encryption codes.[98] This is known colloquially as "black market", as viewers access DIRECTV broadcasts without the consent of the broadcaster and have not paid any subscription fees.

---

[94] For a consideration of this decision and a *Charter* analysis of the freedom of expression argument, see Alex Colangelo, "Satellite Wars: Culture vs. Expression" (2003) 5:2 Vand. J. Ent. L. & Prac. 105 [Colangelo, "Satellite Wars"].

[95] *R. c. Thériault* (2004), [2005] R.J.Q. 857 (C.A. (Crim. & Pen. Div.)) [*Thériault* cited to R.J.Q.].

[96] For a discussion of satellite broadcasting and related cases in Canada see Colangelo, "Satellite Wars", *supra* note 94. At the time, Bell ExpressVu and StarChoice were the only two satellite broadcasters licensed and authorized by the Canadian Radio-television and Telecommunications Commission ("CRTC") to offer satellite programming in Canada.

[97] *Ibid.*

[98] *Ibid.*

Justice Côté, on behalf of the majority in *Thériault*, discussed subsection 2(b) of the *Charter* at length, along with a detailed analysis of *Irwin Toy* and the *Oakes* test.[99] In previous judgments relating to the *Radiocommunication Act*, freedom of expression arguments were either not heard, dismissed straight away, or the analysis was very brief, keeping in line with the reluctance of Canadian courts to discuss freedom of expression when private property is involved.[100] In this case, however, the court broke the freedom of expression analysis into two branches based on the different modes of reception of signals.

The court first considered the case of "black market" decryption of satellite signals received without the consent of DIRECTV and without the user paying a subscription fee. The court found that this activity is not a protected form of expression under subsection 2(b) of the *Charter*. Thus, the activity failed even to meet the low threshold under *Irwin Toy*. This part of the decision follows previous decisions dealing with private property rights.

With regards to the "grey market" reception of satellite signals, the court found that paragraphs 9(1)(c) and 10(1)(b) violate subsection 2(b) of the *Charter*. With respect to a viewer who uses a false mailing address to pay for and receive DIRECTV services, the court held that such false declarations and illegal activities are due to the prohibitions imposed by the government. The court took public interest arguments into account, noting that users would want to access programs offered in various languages as well as those offering specific cultural and religious content, many of which are only available through American satellite services. The court also noted the willingness of DIRECTV to offer services to Canadian customers using false mailing addresses. The latter sentiment indirectly characterizes the programming content of such satellite services as private property. The court found that the activity in question was a protected form of expression, which satisfied the rationales from *Irwin Toy*.[101]

The court then shifted its analysis to section 1 of the *Charter*. The court determined that the legislation in question was pressing and substantial, and rationally connected to its purpose, but it did not minimally impair the right. Thus, paragraphs 9(1)(c) and 10(1)(b) of the *Radiocommunication Act* failed to meet the *Oakes* standard for the reasonable limitation of rights, and were struck down.

The court in *Thériault*, therefore, found that while the "grey market" reception of American satellite broadcasts meets the threshold of expression under *Irwin Toy*, the reception of the same signals by using a "black market" satellite card does not. This decision was subsequently overturned by the Quebec Superior Court.[102] Justice Décarie, on behalf of the court, held that the judge at first instance erred in pursuing a

---

[99] *Thériault*, *supra* note 95. The one exception was a lack of discussion on possible deleterious effects of the proportionality component of the *Oakes* test.

[100] For discussion of the individual cases see Colangelo, "Satellite Wars", *supra* note 94.

[101] See Part I.B., above.

[102] *R. v. D'Argy*, [2005] R.J.Q. 1520 (Sup. Ct.) [*D'Argy*].

constitutional analysis of the "grey market" scenario as no evidence was presented at trial on point; rather, the evidence presented related to the "black market" scenario. As such, there was no need to debate the constitutional validity of the activity under a "grey market" scenario. Even so, the court was of the view that regulations prohibiting the "grey market" would not violate freedom of expression given that the defendants would have had to fraudulently present themselves as having American addresses to subscribe to DIRECTV. Justice Décarie noted that DIRECTV would not have authorized subscriptions to its services were it not for the fraudulent representation. Moreover, the court highlighted that the giving of a false American address was not only a fraudulent representation to DIRECTV but that such actions were equally fraudulent towards Canadian distributors of programs who pay copyright holders to obtain the rights to broadcast or transmit within Canada. The judge sent the case back to the lower court for reconsideration. One may infer from this decision that neither the "black market" nor "grey market" scenarios would attract *Charter* protection under the first limb of *Irwin Toy*. In fact, the court did not engage in any *Charter* analysis, echoing previous decisions where private property and economic rights trumped freedom of expression. The defendants were granted leave to appeal to the Quebec Court of Appeal on 20 April 2005.[103]

While the Court of Quebec provided an analysis of freedom of expression otherwise unseen in Canada, the court's findings with respect to the freedom of expression are flawed. The *Thériault* and *D'Argy* decisions have taken too narrow an approach to subsection 2(b) of the *Charter*. It should, at a minimum, protect expression in both the "black market" and "grey market" scenarios. The threshold of whether activity constitutes expression should not be determined by the method of decryption, and the court should have recognized that even decrypting satellite broadcasts by using a "pirate" satellite card constitutes expression under the *Charter*. The narrowness of the *Thériault* and *D'Argy* decisions is unfortunately consistent with the approach Canadian courts have taken when balancing freedom of expression with copyright protection: courts have favoured the protection of property rights over rights to free expression. It is an inconsistent application of the freedom of expression guarantee to find that child pornography[104] and hate speech[105] are protected forms of expression under the *Charter*, while the use of the copyright-protected Michelin man logo in a labour dispute,[106] and the use of a decryption technology to access satellite television content[107] are not protected.[108] When applied to computer code, this

---

[103] *R. v. D'Argy*, 2005 QCCA 604.

[104] *Sharpe*, *supra* note 74.

[105] *Zundel*, *supra* note 44.

[106] *Michelin*, *supra* note 43.

[107] *Thériault*, *supra* note 95.

[108] See *e.g.* Richard Moon, "Justified Limits on Free Expression: The Collapse of the General Approach to Limits on *Charter* Rights" (2002) 40 Osgoode Hall L.J. 337 [Moon, "Justified Limits"]. The author writes that "in most of the Canadian freedom of expression cases, the section 2(b) analysis seems to be a little more than a formal step that must be taken before the Court moves on to the more substantial issue of limits under section 1" (*ibid.* at 339).

disparity could lead to undesirable consequences in the cases of computer viruses, encryption, and technological protection measures, as will be illustrated in the following section.

Where technology is concerned, subsection 2(b) should protect the activity, whatever the method, while section 1 should limit certain uses. Such an approach would provide stability in freedom of expression jurisprudence, recognizing the consistency and breadth of subsection 2(b) while allowing section 1 limitations based on underlying values. To do otherwise would be to import the analyses of underlying values into what should be a much more straightforward consideration of "expression".

Some commentators have criticized the use of section 1 to justify the limits of freedom of expression. They argue that this approach "increasingly appears vague and malleable"[109] and has "reduce[d] adjudication to a highly subjective exercise with little predictability."[110] This criticism, however, does not strike at the mere use of section 1 to justify the limits, but rather at how the courts have actually used section 1.[111] Our approach does not advocate a specific approach to section 1; we simply wish to argue that computer code should be a protected form of expression and to offer some insight and reflection on the balancing of legislative objectives and effects under section 1. An approach that does not recognize computer code as expression runs the risk of legislating "technological specificity"[112] into the *Charter* and limiting a person's expression to non-proscribed mediums.[113]

There is a growing discourse on freedom of expression within Canadian jurisprudence that, arguably, will expand the scope of what some critics have called an underdeveloped and inadequate treatment of this area of the law.[114] In *Haig v. Canada (Chief Electoral Officer*),[115] the Supreme Court of Canada left open the possibility that freedom of expression may include a positive obligation even where rights are cast in negative terms. In *United Food and Commercial Workers, Local 1518 v. KMart Canada Ltd.*,[116] the Supreme Court held that the restriction on leafleting activity was too broad, striking down legislation because the infringement of freedom of expression could not be justified under section 1 of the *Charter.* These

---

[109] *Ibid.* at 338.

[110] Christopher D. Bredt & Adam M. Dodek, "The Increasing Irrelevance of Section 1 of the *Charter*" (2001) 14 Sup. Ct. L. Rev. 175 at 185.

[111] See Moon, "Justified Limits", *supra* note 108 and Bredt & Dodek, *ibid.*

[112] "Technological neutrality" as opposed to "technological specificity" is the aim of most international and Canadian legislation concerning technology.

[113] Two specific examples illustrating a more appropriate approach to computer code will be discussed in Parts IV and VI, below.

[114] See David Fewer, "Constitutionalizing Copyright: Freedom of Expression and the Limits of Copyright in Canada" (1997) 55 U.T. Fac. L. Rev. 175.

[115] [1993] 2 S.C.R. 995 at 1039, 105 D.L.R. (4th) 577 [*Haig* cited to S.C.R.].

[116] [1999] 2 S.C.R. 1083, 176 D.L.R. (4th) 607.

examples suggest an emerging trend towards an expanded view of freedom of expression.

Considering the breadth of the interpretation of subsection 2(b) of the *Charter* under *Irwin Toy*, the recognition that software contains the creative expression of computer programmers, and the fact that software facilitates the values underlying freedom of expression, software code must be found by Canadian courts to be a protected form of expression under the *Charter*. Canadian courts should not consider the functionality of code nor property rights inherent in computer software in determining whether it is worthy of protection. Rather, they should recognize software as a form of expression worthy of protection under the *Charter* as a way of insulating Canadian courts from the type of legal uncertainty currently prevalent in the United States, as well as allowing section 1 of the *Charter* to be the arbiter of whether the circumstances warrant specific legislation. A full discussion of these points will be explored through three examples: computer viruses, encryption software, and technological protection measures.

IV. Computer Viruses

A. Background

A computer "virus" is a computer program "capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission."[117] While some viruses attach themselves to files so that they are executed when the infected file is executed, others hide surreptitiously in the memory of the computer and infect computer files as they are opened, modified, or as new files are created.[118] Once a virus has infected a computer file it can implement the symptoms planned by the programmer of the virus, which could include damaging or erasing files on the computer.[119]

In *United States v. Mendelsohn*,[120] the Ninth Circuit Court of Appeal for California considered the First Amendment defence to charges of "aiding and abetting the interstate transportation of wagering paraphernalia."[121] The defendants mailed a computer floppy disk containing a sports wagering program from Nevada to an undercover police officer posing as a bookmaker in California.[122] The computer program contained on the disk could be used to record and analyze bets. It also

---

[117] McAfee, Inc., "Virus Glossary," online: McAfee, Inc. <http://us.mcafee.com/virusInfo/default.asp?id=glossary>.

[118] *Ibid.*

[119] *Ibid.*

[120] 896 F.2d 1183 (9th Cir. 1990) [*Mendelsohn*].

[121] 18 U.S.C. §§ 371, 1953.

[122] *Mendelsohn*, *supra* note 120 at 1184.

allowed the user to record and review information concerning game schedules and other information relevant to placing bets on those games.[123]

The defendants relied on the First Amendment, arguing that the computer program was protected speech and, as such, immune from the legislation.[124] The District Court of Appeal found that

> [t]here was no evidence that the defendants thought Felix [the undercover officer] was going to use SOAP [the computer program] for anything other than illegal bookmaking. On the contrary, the defendants knew that SOAP was to be used as an integral part of a bookmaker's illegal activity, helping the bookmaker record, calculate, analyze, and quickly erase illegal bets.[125]

The court did not allow the defence, relying on *United States v. Freeman* to find that "where speech becomes an integral part of the crime, a First Amendment defense is foreclosed even if the prosecution rests on words alone."[126] This opinion left open the possibility that a computer program that could be used to commit a crime would be protected where the author or distributor provided access to the program for legal purposes: "Although a computer program under other circumstances *might warrant first amendment protection*, SOAP does not."[127] This was also the case in *Freeman*, where the Ninth Circuit for Oregon found that "[w]here there is some evidence, however, that the purpose of the speaker or the tendency of his words are directed to ideas or consequences remote from the commission of the criminal act, a defense based on the First Amendment is a legitimate matter for the jury's consideration."[128]

Applying these principles to a hypothetical case involving the dissemination of virus software, it seems that an American court would analyze the use of the software when determining whether First Amendment protection is available. If the virus software were distributed maliciously, with the intent to damage computer systems, it is likely that courts would apply the decision in *Mendelsohn* and refuse to extend the protection of the First Amendment. Where a computer science professor places the code to virus software on a course website for the purpose of instruction, courts may find that the First Amendment would protect such acts.

With respect to code written for illegal purposes, the Supreme Court of Canada has held that subsection 2(b) protection should not be withheld because the expression is the subject of a criminal offence:[129] "[T]he content of a statement cannot

---

[123] *Ibid.* at 1184.
[124] *Ibid.* at 1185.
[125] *Ibid.*
[126] 761 F.2d 549 at 552 (9th Cir. 1985) [*Freeman*].
[127] *Mendelsohn*, *supra* note 119 at 1186 [emphasis added].
[128] *Freeman*, *supra* note 126 at 551.
[129] See *Reference Re ss. 193 and 195.1(1)(c) of the Criminal Code*, [1990] 1 S.C.R. 1123 at 1183, 109 N.R. 81 where Lamer J. concurred with the majority opinion and stated that "it would be unwise and overly restrictive to *a priori* exclude from the protection of s. 2(b) of the *Charter* activities solely

deprive it of the protection accorded by s. 2(*b*), no matter how offensive it may be."[130] Thus, the content of software code should not determine whether the protection of subsection 2(b) should be extended to the code. Canadian courts cannot follow the lead of *Freeman* and *Mendelsohn*, which found that there can be no protection of speech where the communication becomes an integral part of a crime. The creation or dissemination of a computer virus that cripples computer systems by deleting files, the publishing of encryption code that infringes upon export regulations, and the publishing of computer code that bypasses technological protection measures should all be extended the same protection under the *Charter*. While the restrictions upon such activity may serve purposes that do not infringe the *Charter*, the effects of such restrictions would undermine the principles underlying the protection. The creation of software, even malicious software, is a manifestation of creativity and expression, and encourages the cultivation of individual self-fulfillment. Meanwhile, the use of software, even for malevolent purposes such as distributing a virus or circumventing copyright, falls within the ambit of social and political action. As considered above, the existence of section 1 of the *Charter* allows for a more consistent analysis than the American approach in determining whether communication is protected under subsection 2(b), without having to carve out unwanted categories of protected expression.

Example: Criminal Code section 430(1.1)

When "Mafiaboy", a teenage computer hacker from Montreal, was apprehended after his attacks on computer websites, he was charged under the *Criminal Code* provision of "mischief in relation to data."[131] Subsection 430(1.1) makes it a crime to destroy or alter data; render data meaningless, useless or ineffective; obstruct, interrupt or interfere with the lawful use of data; or obstruct, interrupt or interfere with any person in the lawful use of data or to deny access to any person who is entitled such access.[132] While Mafiaboy did not use a computer virus to attack the websites in question, it is likely that a person who disseminated a computer virus would be charged under this provision. We will now examine whether this provision stands under the *Oakes* test.

B. The Oakes *Test*

The objective of subsection 430(1.1) of the *Criminal Code* is the protection of data from malicious activity. As society becomes more reliant on the Internet and computer technology, the importance of protecting such systems from malicious activity becomes increasingly apparent. This fact, combined with the deference that courts have given legislatures with respect to the first step in the *Oakes* analysis

---

because they have been made the subject of criminal offences" (*ibid.*). See also *Keegstra*, *supra* note 33 and *Zundel*, *supra* note 44.

[130] *Keegstra*, *ibid.* at 828.

[131] R.S.C. 1985, c. C-46, s. 430(1.1) [*Criminal Code*].

[132] *Ibid.*

strongly suggests that protecting data from malicious activity is a sufficiently important objective.

The rational connection between a law and its objective need not be proven by the evidence; "a causal connection based on 'reason' or 'logic' would suffice."[133] A *Criminal Code* provision that criminalizes the destruction and interference of data is logically connected to the objective of protecting data from such destruction and interference. Thus, the first component of the proportionality test of *Oakes* is satisfied.

The second part of the proportionality test of *Oakes* considers whether the *Criminal Code* provision in question restricts the freedom of expression under the *Charter* "as little as is reasonably possible".[134] The *Criminal Code* provision for "mischief in relation to data" requires that the actor wilfully destroy, alter, or obstruct data. There are two important features of this provision that limit its application and satisfy the second tenet of the proportionality test. First, the *Criminal Code* provision for mischief to data does not prohibit the publication of software code for academic, scientific, or even recreational purposes. A person who publishes the code for a virus onto the Internet, therefore, would not be susceptible to liability under this section. Second, the provision requires wilful intent. If a person were to disseminate a virus unknowingly onto the Internet, that person would also be protected from prosecution. Unknowing dissemination could occur if a person's computer became infected with a virus, and the user subsequently did something that facilitated the spread of the virus. The section of the *Criminal Code* that prohibits the destruction or obstruction of data has been narrowly tailored to exclude those who simply publish computer code and those who facilitate the spread of a computer virus unknowingly. The provision, then, only infringes upon the freedom of expression of those who wilfully facilitate the destruction and interruption of data. Thus, the *Criminal Code* section dealing with "mischief in relation to data" infringes the freedom of expression "as little as is reasonably possible" and passes the second part of the proportionality test. A hypothetical *Criminal Code* provision that lowered the requirements necessary to be charged under this section, however, might not pass constitutional muster.

The third element of the proportionality test requires balancing the effects and objective of the provision. As has been demonstrated, the objective of the *Criminal Code* provision prohibiting the destruction and obstruction of data is sufficiently important to warrant the abridgment of the freedom of expression. Furthermore, the provision has been constructed narrowly so as not to hamper legitimate expression, and requires wilful intent. The effects of the provision are proportional to the objective, and do not severely trench on the freedom of expression.

---

[133] Hogg, *supra* note 11 at 724.
[134] *Ibid.*

C. Hypothetical: Mobile Phone Cabir Virus

"29A" is an international "hacker" group that specializes in the writing and development of innovative viruses. 29A recently wrote the world's first mobile phone virus known as Cabir.[135] 29A does not actually spread viruses like Cabir. Other hackers obtain the computer code of the virus and spread it themselves. 29A sees itself as a pioneer in innovative computer programming and as a group dedicated to exposing security risks. In the words of one of its founders:

> The purpose of 29A has always been technical progress, invention and innovation of new and technically mature and interesting viruses. 29A distances itself from virus-spreading, since 29A always tried to act as a security group, not any cybergang, as has been portrayed in the media. 29A just wants to share ideas with others, and source code is a way of expression ...
>
> Coming up with new ideas advances the Internet, since it becomes more prepared against real attacks ...
>
> ... almost all ex-members and current members of 29A are employed in the antivirus and information technology security industry.[136]

Let us now assume that members of 29A had written the Cabir virus to expose security flaws and to write cutting edge computer code. Other hackers outside of the group study the virus and initiate its spread through the system, sometimes in its original form and sometimes as a new and improved variety (Cabir2, Cabir3, etc.). Suppose thousands of Nokia customers' phones are affected. Another hacker (Hacker G), intrigued by the innovativeness and sophistication of the virus, decides to write a computer program to counter Cabir: an antivirus (A-Cabir1). Hacker G, without the permission of Nokia or its customers, spreads A-Cabir1 to correct the damage caused by the various Cabir viruses. Meanwhile, an antivirus company has also written an antivirus program to counter Cabir and has made it available to the public (A-Cabir2). Company O studies the source code for the Cabir viruses and their antiviruses, and uses part of the code to develop a derivative software program (Kabeer) which is later used to transmit data more rapidly through the Nokia model. Kabeer revolutionizes the cellular telephone industry (at least for a few months).

One immediately wonders which of the above-mentioned activities falls within the construction of the hacking provisions in the *Criminal Code*. Which computer programs would be subject to *Charter* protection? Cabir? Cabir1? Cabir2? A-Cabir1? A-Cabir2? Kabeer? The private property and economic rights approach taken by the courts (in particular, in *Thériault*) is problematic and difficult to use with

---

[135] The virus only potentially affects Nokia's Series 60 operating system where transmitted over a Bluetooth connection. See "Cabir Virus Spreads to France, Japan" *Telecom Asia Daily* (7 March 2005), online: Telecom Asia <http://www.telecomasia.net/telecomasia/article/articleDetail.jsp?id=150104>.

[136] Robert Lemos, "He's got the virus-writing bug" *CNET News* (14 January 2005), online: CNET News.com <http://news.com.com/Hes+got+the+virus-writing+bug/2008-1025_3-5520278.html>.

technology.[137] Technology, and computer programs in particular, may be created for a specific purpose, but will inevitably be used for many other purposes both predictable and unforeseeable. Categorizing one computer program as within the scope of subsection 2(b) and another as falling outside its scope could have significant ramifications to a business or government's ability to effectively prevent and respond to issues such as cyber-terrorism and the promotion of multiculturalism through software. It could also stifle the development and expression of computer code in general.[138] It may hamper the development of beneficial software. Courts should extend subsection 2(b) protection to such code and use section 1 to limit malevolent uses that are inconsistent with core values. To do otherwise would be to invite a court to decide whether a piece of software is expressive enough to qualify for subsection 2(b) protection without the benefit of considering the effects of the software.

V. Encryption Software

A. Background

"Cryptography is the science of secret writing, a science that has roots stretching back hundreds, and perhaps thousands, of years."[139] Traditionally, cryptography has been the exclusive domain of government and the military. The advent of commercial computer technology has brought cryptography into the civilian sphere and transformed it into an academic discipline.[140]

A cryptographic program has two basic functions: encryption and decryption. The process of encryption involves converting a readable message into unintelligible data. Decryption is the reverse procedure, taking the unintelligible data and constructing the original message. These procedures are made possible by employing "keys", which act as passwords. Each user employs his or her key in order to encrypt or decrypt a message and keeps his or her key private.[141]

In response to the perceived threat of foreign powers using computer encryption to conceal communication, the United States, under the Clinton administration, passed regulations controlling the export of encryption technology.[142] The restriction

---

[137] Recall the approach taken in *Thériault*, *supra* note 95: illegal "black market" (decryption device without permission or paying subscription fees) activity did not fall within the purview of protection afforded under s. 2(b), while so-called illegal "grey market" (false mailing address coupled with the use of a decryption device but subscription fees paid) activity was worthy of protection.

[138] Many experts warn that software and telecommunications companies are vulnerable to terrorist attacks because they do not take security seriously enough. See *e.g.* Dr. Himanshu Pant's comments in "Movements" *TelecomAsia* 15:7 (July 2004) 15.

[139] *Bernstein*, *supra* note 53 at 1136.

[140] *Ibid.* at 1136-37.

[141] Yvonne C. Ocrant, "A Constitutional Challenge to Encryption Export Regulations: Software is Speechless" (1998) 48 DePaul L. Rev. 503 at 508-509.

[142] Fox, *supra* note 49 at 886-87.

of encryption technologies by the United States proved to be the impetus for a trilogy of encryption export cases that tested the constitutionality of the regulations.

In *Karn v. United States (Department of State)*,[143] the court dealt with an entrepreneur who was interested in exporting material authored by Bruce Schneier. Schneier wrote a book on cryptography that referred to two diskettes containing encryption source code, both of which were available from the author. The defendant, Philip Karn, wanted to export these items and wanted to know whether he would need an export license under the relevant regulations. Pursuant to Karn's petition, the Department of State's Office of Defence Trade Controls found that the book was not subject to the export restriction but that the computer disk was.[144] After appealing the finding to the Deputy Assistant Secretary of State and the Assistant Secretary of State for Political-Military Affairs, Karn brought an appeal to the District Court for the district of Columbia, claiming that the regulation of the disk violated the First Amendment.

In addressing Karn's free speech claim, the District Court simply assumed that the source code on the disk was "within the arena" of the speech protected by the First Amendment.[145] While the court did not specifically consider the *Spence* test or provide an analysis for such a determination, the court upheld the constitutionality of the regulations, using the *O'Brien* test.[146] In considering the *O'Brien* test, the court found that the regulations were content-neutral, were within the constitutional powers of the government, and were narrowly tailored to an important and substantial government interest.[147] Thus, the court allowed the export regulation and threw out Karn's complaint.

The decision of the Ninth Circuit in *Berstein* has been withdrawn for an *en banc* hearing.[148] This decision nonetheless provides an example of American jurisprudence in this area. Daniel Bernstein was a professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago. When he was a doctoral candidate, Professor Bernstein developed an encryption method that he called "Snuffle".[149] Professor Bernstein authored a paper containing an analysis and mathematical equations describing his method, as well as two computer programs. He also translated the source code into a set of English instructions. Like Karn, Professor Bernstein inquired as to whether he would require a license to publish his code in the various forms. The State Department informed him that he would need a license to export the paper, the source code, and the instructions.

---

[143] 925 F. Supp. 1 (D.D.C. 1996) [*Karn*].
[144] *Ibid.*
[145] *Ibid.* at 9ff.
[146] *Ibid.* at 9-13. See *O'Brien*, *supra* note 17.
[147] *Ibid.*
[148] *Bernstein*, *supra* note 53.
[149] *Ibid.*

In considering the application of the First Amendment to encryption source code, the court found that "the chief task for cryptographers is the development of secure methods of encryption."[150] The court recognized that cryptographers use source code to express ideas and to facilitate peer review:

> [B]y compiling the source code, a cryptographer can create a working model subject to rigorous security tests. The need for precisely articulated hypotheses and formal empirical testing, of course, is not unique to the science of cryptography; it appears, however, that in this field, source code is the preferred means to these ends.[151]

The court compared the fact that cryptographers use source code to express ideas by drawing an analogy to the way mathematicians use equations and economists use graphs. While the court recognized that mathematical equations and graphs are not always used to express ideas, "mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas."[152] The court found that cryptographers utilize source code in the same way.

In considering the government's arguments that source code was inherently functional and should be limited in its use, the court made two key findings. First, the court distinguished between source code, which is meant to be read and understood by computer programmers and cannot be directly used to control a computer, and object code, which is meant to direct the functions of the computer. Second, the court rejected the notion that "even one drop of 'direct functionality' overwhelms any constitutional protections that expression might otherwise enjoy."[153] The court also considered the growing dependence on technology and the use of speech in controlling technology, stating that

> [t]he fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the government the unfettered power to impose prior restraints on speech in an effort to control its "functional" aspects. The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution.[154]

The court found that the encryption source code was expressive and protected by the First Amendment. In considering whether the regulations were allowable limits on speech, the court found that the licensing scheme vested too much discretion in government officials and lacked adequate safeguards. The licensing scheme was therefore an unconstitutional prior restraint on Professor Bernstein's speech.

---

[150] *Ibid.* at 1141.
[151] *Ibid.*
[152] *Ibid.* [footnotes omitted].
[153] *Ibid.* at 1142.
[154] *Ibid.*

The appellant in *Junger v. Daley*, meanwhile, was a professor at Case Western Reserve University Law School.[155] Professor Junger maintained websites on the Internet that included information about courses he taught. One of his courses dealt with computers and the law. Professor Junger wanted to post encryption source code onto his website in order to demonstrate how such code worked. Under the *Export Administration Regulations*,[156] such a posting was considered an export and was covered by the regulations.[157] Professor Junger submitted three applications to the Commerce Department in June 1997, requesting the determination of commodity classifications for encryption software programs. Within a month, the Export Administration ruled that while Professor Junger's textbook was an allowable unlicensed export, he would require an export licence in order to post the encryption software program to his website. Professor Junger appealed the ruling.

In its decision, the District Court set up a standard that distinguished between expressive and functional activity.[158] The court found that

> [c]ertain software is inherently expressive. Such expressive software contains an "exposition of ideas." ... In contrast, other software is inherently functional. With such software, users look to the performance of tasks with scant concern for the methods employed or the software language used to control such methods.[159]

In describing encryption code, the court found that encryption software is "especially functional rather than expressive"[160] because it simply carries out the function of encryption, expressing few ideas and providing little information about how software functions.

> In the overwhelming majority of circumstances, encryption source code is exported to transfer functions, not to communicate ideas. In exporting functioning capability, encryption source code is like other encryption devices. For the broad majority of persons receiving such source code, the value comes from the function the source code does.[161]

Even though the court found that the most important issue was "whether the export of encryption software source code is sufficiently expressive to merit First Amendment protection,"[162] it failed to clearly define what was necessary to qualify as

---

[155] 8 F. Supp. 2d 708 (N.D. Ohio 1998) [*Junger 1*], rev'd 209 F.3d 481 (6th Cir. 2000) [*Junger 2*].

[156] 15 C.F.R. § 734.2(b)(9).

[157] *Junger 1*, *supra* note 155 at 714.

[158] *Ibid.* at 715-17. See also Seth Hanson, "*Bernstein v. United States Department of Justice:* A Cryptic Interpretation of Speech" (2000) B.Y.U.L. Rev. 663. See also *Bernstein*, *supra* note 53.

[159] *Junger 1*, *supra* note 155 at 716.

[160] *Ibid.*

[161] *Ibid.*

[162] *Ibid.* at 715.

"sufficiently expressive."[163] The court did, however, recognize that encryption source code could have expressive elements:

> While finding that encryption source code is rarely expressive, in limited circumstances it may communicate ideas. Although it is all but unintelligible to most people, trained computer programmers can read and write in source code. Moreover, people such as Plaintiff Junger can reveal source code to exchange information and ideas about cryptography.[164]

While encryption code "can occasionally have communicative elements,"[165] encryption source code was found to be inherently functional. Accordingly, the First Amendment did not require that Professor Junger be allowed to export the software.

The decision of the trial court was overturned, however, by the Court of Appeals, Sixth Circuit.[166] The District Court found that the functional aspects of the encryption code surpassed the expressiveness of the code, but the Court of Appeals found that the functionality of code should not preclude constitutional protection. The Court of Appeals drew an analogy to musical notation, stating that "a musical score cannot be read by the majority of the public but can be used as a means of communication among musicians. Likewise, computer source code, though unintelligible to many, is the preferred method of communication among computer programmers."[167] The court considered source code to be an expressive medium for the "exchange of information and ideas about computer programming"[168] and as such found that source code is protected by the First Amendment. While the court determined that source code is protected by the First Amendment under the *Spence* test, it declined to determine whether the export regulations passed the scrutiny of the *O'Brien* test in light of the revisions made to the regulations during the course of the proceedings. As such, the Court of Appeals ordered the District Court's decision be reversed and remanded for new consideration in light of the amended regulations.

In Canada, export controls are administered under the *Export and Import Permits Act*[169] and its regulations. Section 3 of the *EIPA* authorizes the Governor in Council to establish an "Export Control List" in order to set controls and procedures for the export of certain goods.[170] Under section 7 of the *EIPA*, permits may be issued to those wishing to export an item on the Export Control List.[171] Group 1151(a) of the Export Control List includes "[s]ystems, equipment, application specific 'electronic assemblies', modules or integrated circuits for 'information security', as follows, ... [d]esigned or modified to use 'cryptography' employing digital techniques to ensure

---

[163] Hanson, *supra* note 158 at 672.
[164] *Junger 1*, *supra* note 155 at 717.
[165] *Ibid.* at 717.
[166] *Junger 2*, *supra* note 155.
[167] *Ibid.* at 484.
[168] *Ibid.* at 485.
[169] R.S.C. 1985, c. E-19 [*EIPA*].
[170] *Ibid.* s. 3.
[171] *Ibid.* s. 7.

'information security'"[172] while group 1154(3)(a) includes "'[s]oftware having the characteristics, or performing or simulating the functions of the equipment controlled by 1151. or 1152. [test, inspection and production equipment of information security]."[173]

According to these regulations, the export of cryptographic software requires a permit. While a permit may be granted for the export to certain countries, it is conceivable that if the government were to consider the publication of cryptographic software code online to be an "export" as was found in *Bernstein* and *Junger*, permission to publish such code may be withheld for fear that rogue nations would gain access. There is currently no Canadian jurisprudence on the issue. A consideration of the constitutionality of such export regulations will follow.

B. The Oakes *Test*

The introduction to the Export Control List outlines the objectives of export controls:

> Canada's export controls are not intended to hamper business. Rather, the regulations are designed to ensure that exports and transfers of certain goods and technology are in keeping with the strategic interests of Canada or its allies and are consistent with Canada's bilateral or multilateral commitments. Considering the volatility of the international political environment—and the speed with which new technology is being developed—it is clear that these controls are necessary to safeguard Canadian security, political and international interests.[174]

The importance of regulating the encryption software was recognized in the United States in *Karn*, which upheld the export regulations.[175] This objective is further supported by the fact that thirty-three countries have supported such initiatives by supporting the *Wassenaar* agreement limiting the export of such technologies.[176] Considering the importance of national security and the deference given to legislators in this regard, the objective behind controlling exports would likely be considered sufficiently important to justify the limitation on the freedom of expression.

The *EIPA* limits the export of cryptography by requiring a permit to export such software. In so doing, the *EIPA* attempts to limit the availability of strong encryption

---

[172] *Export Control List*, Category 1151: Systems, Equipment and Components, online: International Trade Canada <http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1f-en.asp#1151>.

[173] *Export Control List*, Category 1154: Software, online: International Trade Canada <http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1f-en.asp#1154>.

[174] *Export Control List Introduction*, online: International Trade Canada <http://www.dfait-maeci.gc.ca/trade/eicb/military/intro-en.asp?#introduction>.

[175] The other two export cases did not make a determination on this facet of the *O'Brien* test. *Karn* is the only decision specifically considering the government objective in regulation encryption.

[176] U.S. Department of Commerce, "The Wassenaar Arrangement: Frequently Asked Questions", online: U.S. Department of Commerce <http://www.bxa.doc.gov/Wassenaar/WASSFAQs.html#7>.

solutions to those in rogue countries that may use the software to protect their correspondence from interception and analysis. It can thus be said that there is a reasonable connection between this objective and the law requiring permits before exporting such software.

While the *EIPA* allows for the granting of permits for the exportation of encryption software, it is silent as to whether the posting of material onto the Internet is considered an export. If this were found to be the case, the export would conceivably be to every country in the world. It is likely that permits would not be granted in cases where, like in the United States, a professor wanted to post encryption code onto a website. Such an "export" would be considered to include rogue nations that Canada would not want to have access to such software, and permits could be withheld. The legislation is vague as to whether technological protection measures would make a difference in such a determination. For example, a professor could protect the source code from access beyond his or her class by placing it in a password-protected directory. Thus, the software would be inaccessible to anyone not in the professor's class. The legislation, however, is not clear in this respect.

The legislation also does not provide for an appeal from the Minister's decision. The *Bernstein* court found this to be a major deficiency in the American export regulations, finding that too much discretion had been left to government officials without adequate safeguards. The situation is similar in Canada, where the Minister has full discretion to decide whether to grant a permit. It is difficult to predict how a court in Canada would decide on this issue. The *Bernstein* decision suggests that the vagueness of the application of the export limits with respect to the Internet and the amount of discretion awarded to government officials restrict freedom of expression more than is reasonably necessary. The legislation would, therefore, fail the second step of the proportionality test under *Oakes*.

If the law and regulations limiting the export of cryptography were found to infringe unreasonably upon freedom of expression, the effect of the law would likely also be found to be disproportionate to the stated objective. The lack of clarity in the law regarding posting content on the Internet, and a lack of appeal procedures, limit expression so far as to outweigh the salutary effects of the legislative scheme. The last criteria of the proportionality test under *Oakes* would likely fail.

VI. Technological Protection Measures

A. Background

A technological protection measure ("M") consists of a technological method, usually in the form of computer software code, that controls authorized access to digitized content. In a sense, such technologies are like a virtual fence (with a gate)

around digitized content.[177] This virtual fence allows control of access, as well as other uses such as copying, distributing, printing, saving, and display. Some examples of Ms include cryptography, passwords, digital tickets, and digital management systems such as Extensible Rights Mark-up Language ("XrML").[178]

Many nations, including the United States, members of the European Union, China, Australia, and Japan have enacted what are known as anticircumvention legal measures in order to comply with the obligations set forth in the World Intellectual Property Organization ("WIPO") treaties.[179] Anticircumvention measures are legal provisions that make the circumvention of an M illegal. They fall generally into four types: (1) general access control measures, (2) limited access control measures, (3) use / copy control measures, and (4) anti-device measures. Each of these concepts are briefly explained below.

A general access control measure prohibits *any* act that circumvents an access control M, irrespective of whether the circumvented M functions to control a work subject to copyright and irrespective of whether the act of circumvention actually infringes copyright.[180]

A limited access control measure prohibits only some acts that circumvent an access control M. It will protect an access control M only *if* the M functions to prevent access to a work subject to copyright. So long as the M prevents access to copyright protected works, a limited access protection measure would operate even if the act of circumvention does not ultimately infringe copyright.[181]

An use/copy control measure is a prohibition against the circumvention of Ms meant to control unauthorized copies of a work. Many current Ms display both access control and use control characteristics.[182]

An anti-device measure proscribes the manufacturing, distribution, or sale of devices that are used to circumvent technologies employed to protect copyright. Such measures are meant to deter copyright infringement by stopping it at its source. Anti-

---

[177] Dr. Ian R. Kerr, Alana Maurushat & Christian S. Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill" (2002-2003) 34 Ottawa L. Rev. 7 at 13 [Kerr, Maurushat & Tacit, "TPM Copyright's Windmill"].

[178] For a detailed explanation of these technologies see *ibid.* at 14-28.

[179] *World Intellectual Property Organization: Copyright Treaty*, 20 December 1996, 36 I.L.M. 65 (entered into force 2 March 2002) [*WIPO Copyright Treaty*]; *World Intellectual Property Organization: Performances and Phonograms Treaty*, 20 December 1996, 36 I.L.M. 76 (entered into force 20 May 2004).

[180] Ian Kerr, Alana Maurushat & Christian S. Tacit, "Technical Protection Measures: Part II—The Legal Protection of TPMs" (2002) at 3.1, online: Department of Canadian Heritage <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/index_e.cfm> [Kerr, Maurushat & Tacit, "TPM Part II"].

[181] *Ibid.*

[182] *Ibid.*

device measures operate on the premise that sanctioning acts of circumvention on a case-by-case basis is costly and ineffective.[183]

Although Canada is a signatory to the WIPO treaties, it has yet to ratify them. Canada tabled legislation in June 2005 that would have implemented the provisions of the WIPO treaties in Bill C-60, *An Act to amend the Copyright Act*.[184] With the election of a new government in January 2006, however, Bill C-60 died on the order table. The Bill however, provides a useful framework to assess the potential *Charter* issues. The section on Ms reads as follows:

> (1) An owner of copyright in a work, a performer's performance fixed in a sound recording or a sound recording and a holder of moral rights in respect of a work or such a performer's performance are, *subject to this Act*, entitled to all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right against a person who, *without the consent of the copyright owner or moral rights holder, circumvents, removes or in any way renders ineffective a technological measure* protecting any material form of the work, the performer's performance or the sound recording for the purpose of an act that is an *infringement of the copyright in it or the moral rights in respect of it or for the purpose of making a copy* referred to in subsection 80(1).
>
> (2) An owner of copyright or a holder of moral rights referred to in subsection (1) has the same remedies against a person who *offers or provides a service* to circumvent, remove or render ineffective a technological measure protecting a material form of the work, the performer's performance or the sound recording and *knows or ought to know* that providing the service will result in an infringement of the copyright or moral rights.
>
> (3) If a technological measure protecting a material form of a work, a performer's performance or a sound recording referred to in subsection (1) is removed or rendered ineffective in a manner that does not give rise to the remedies under that subsection, the owner of copyright or holder of moral rights nevertheless has those remedies against a person who knows or ought to know that the measure has been removed or rendered ineffective and, without the owner's or holder's consent, does any of the following acts with respect to the material form in question:
>
> (a) sells it or rents it out;

---

[183] *Ibid.*

[184] Bill C-60, *An Act to Amend the Copyright Act*, 1st Sess., 38th Parl., 2005, (first reading 20 June 2005) [Bill C-60].

> (b) *distributes it to such an extent as to prejudicially affect the owner of the copyright*;
>
> (c) by way of trade, distributes it, exposes or offers it for sale or rental or exhibits it in public; or
>
> (d) imports it into Canada for the purpose of doing anything referred to in any of paragraphs (a) to (c).[185]

It appears that the previously proposed legislation could be characterized as a use/copy control measure and potentially as a limited access control measure. The provisions would only have applied to works subject to copyright in conjunction with the purpose of infringing copyright or, in the case of moral rights, to make a copy of a work without consent. In other words, there would have been no requirement that copyright be infringed; mere circumvention, with the purpose to infringe would have satisfied the provision.

It is important to reiterate that Ms do not often easily fall within any given category; in fact, many Ms display multiple characteristics such as access and copy/use control measures. Furthermore, as Bill C-60 is no longer before Parliament, it is possible that a new proposal may contain an access measure and an anti-device measure (certainly the entertainment industry will lobby hard on this point). The following analysis, therefore, will include the possible effects of Bill C-60, had it passed, as well as potential ramifications of the adoption of a general access measure and anti-device measure.

While there are no Canadian decisions regarding Ms, there are a host of interesting American decisions and situations that highlight some of the difficulties with anticircumvention measures. *Universal City Studios, Inc. v. Reimerdes*[186] best illustrates the competing tensions of anticircumvention measures in the *Digital Millennium Copyright Act* (*DMCA*).[187] The *DMCA* has been viewed by many commentators as an inappropriate extension of copyright with potential First Amendment ramifications, while others have heralded it as a necessary instrument to protect copyrighted materials in the digital age.

In 1999, a Norwegian teenager by the name of Jon Johansen, along with two other individuals, developed the software, "DeCSS", that enables users to break the software known as Content Scrambling System ("CSS"). CSS is a type of M developed by the Motion Picture Association of America ("MPAA"). CSS is a copy protection system allowing authorized distribution and viewing of DVD movies on CSS-compliant playing devices over the Internet, namely the Microsoft operating system. DeCSS is a software program designed to decrypt CSS to allow DVDs to be played on the Linux operating system. DeCSS was quickly disseminated on the

---

[185] *Ibid.* ss. 34.02(1-3) [emphasis added].
[186] 82 F. Supp. 2d 211 (S.D.N.Y.) 2000 [*Reimerdes*].
[187] *Digital Millennium Copyright Act*, 17 U.S.C. § 1201 [*DMCA*].

Internet, in many computer magazines as well as on personal websites. While DeCSS would allow users that had legitimately purchased a DVD to play the content on a Linux system, the program also allowed computer users to make copies of DVD movies, which could then be distributed and downloaded for free via file-sharing programs over the Internet. The MPAA was concerned that this program would allow widespread pirating of copyrighted movies and feared a situation similar to that of the dissemination of MP3s.[188]

The MPAA, under the *DMCA*, demanded that Internet service providers remove DeCSS from their servers, and that individuals refrain from posting DeCSS. They met with relative success, as a considerable number of DeCSS postings were removed. Members of the hacker community, however, initiated a mass effort to distribute DeCSS via the Internet in an attempt to preclude effective judicial relief.

The major motion picture studios brought an action for injunctive relief against the defendant, Shawn Reimerdes, the owner of the online computer publication Magazine 2600. Magazine 2600 routinely publishes novel and innovative computer code. The MPAA claimed the defendant was responsible for proliferating a software device (DeCSS) that unlawfully defeated the DVD copy protection and access control system (CSS) so that individuals could make, distribute, and electronically transmit unauthorized copies of copyrighted motion pictures and other audiovisual works. The plaintiffs alleged that the actions of the defendants violated the provisions of the *Copyright Act of 1976*[189] governing circumvention of copyright protection systems.

The *Reimerdes* case was the first to challenge the *DMCA* on the grounds of freedom of speech. The court, in a decision written by Justice Kaplan, determined that executable computer code was sufficiently expressive to be protected speech, but that the *DMCA*'s prohibition of dissemination of DeCSS did not violate the defendant's First Amendment rights.

Justice Kaplan began the constitutional analysis by emphasizing that it was not clear from either the jurisprudence or the statutes that DeCSS constituted speech.[190] Courts have, in the past, been divided on whether computer program code is constitutionally protected expression. Justice Kaplan stated that the First Amendment does not shield copyright infringement, and that a detailed First Amendment analysis is imperative because the *DMCA* prohibits production and dissemination of technology more broadly than the *United States Copyright Act*.[191]

With respect to Congress' jurisdiction to legislate in this area, the court stressed that the Necessary and Proper Clause was to be interpreted to give substantial deference to Congress in order to determine how best to protect copyright in an age of

---

[188] See *e.g.* Alex Colangelo, "Copyright Infringement in the Internet Era: The Challenge of MP3s" (2002) 39 Alta. L. Rev. 891.

[189] Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended at 17 U.S.C. § 1-1332).

[190] *Reimerdes*, *supra* note 186 at 219-20.

[191] *Ibid.* at 220.

rapid technological change.[192] The court outlined the thrust behind Congress' enactment of the *DMCA*: to afford sufficient copyright protection to new medias such as the Internet, and to bring United States law in line with the requirements of WIPO treaties that mandate participating nations to take legislative steps towards banning "access control circumvention" devices.[193] Paragraph 1201(a)(2) of the *DMCA* was, therefore, determined to be a proper exercise of Congress' power under the Necessary and Proper Clause.[194]

Justice Kaplan then shifted his analysis to one of balancing the public interest in regulation against freedom of speech.[195] The court said that DeCSS may have some expressive content but that this expressive aspect was minimal when compared to its functional component. Without limits on new technologies such as DeCSS, the goals of copyright would be undermined while artistic progress would be curtailed. Justice Kaplan concluded decisively that executable computer code does little to further traditional First Amendment interests. The balance of public interest fell on the side of regulation.[196]

Application of the *DMCA* was postulated as constitutional on another ground. The distribution of DeCSS was done as part of a course of conduct in violation of the law. DeCSS was disseminated to permit widespread copying and distribution of unauthorized copies of copyrighted works without the permission of the copyright holder. The fact that DeCSS was expressive to some degree does not alter the reality that its dissemination was in violation of the law.[197]

The decision was appealed. The United States Court of Appeals dismissed the appeal and had several noteworthy points regarding freedom of speech. The court held that computer code was a protected form of speech stating, "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."[198] Further, computer programs are not exempted from the category of speech protected by the US Constitution simply because their instructions require the use of a computer. The court referred to the functional quality of DeCSS and not its content. In other words, DeCSS served the function of instructing a computer to circumvent a technological protection measure. The anticircumvention measures were content-neutral and passed constitutional scrutiny.

---

[192] *Ibid.* at 221.

[193] *WIPO Copyright Treaty*, *supra* note 179, article 11 stipulates that:

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

[194] *Reimerdes*, *supra* note 186 at 221.

[195] *Ibid.* at 221.

[196] *Ibid.* at 222.

[197] *Ibid.* at 222-23.

[198] *Universal City Studios, Inc. v. Corley*, 273 F. 3d 429 at 445.

In Canada, the majority of copyright infringement cases address piracy (unauthorized copying and distribution) issues where the interests of the infringing party are primarily economic or functional. These interests fall far from the core of values enshrined in subsection 2(b) of the *Charter*. Anticircumvention provisions, as applied in the DeCSS case, could be characterized as constraining economics to prevent piracy. Economic piracy threatens to undermine investment in informational goods while simultaneously encouraging proprietors to raise barriers to access. These kinds of developments do little to further the objectives of freedom of expression. In the case of DeCSS, the United States Court found the fact that the code was developed in part to run on the open source Linux system to be marginal in comparison with its broader application: the ability to view movies online for free through Microsoft Windows. The modification of a program to make it operable using a different operating system—namely open source operating systems—is a fair use right in the United States. Even if the infringer is motivated partly by legitimate expressive values, the expressive interests of infringers would likely be seen as marginal when compared to DeCSS's function: the enablement of circumventing technological measures to gain free access to a work which they would otherwise not have access to without having purchased the product. Such an analysis, however, woefully neglects many potentially negative effects of such a limited approach.

For example, after the dissemination of the source code of DeCSS over the Internet, many new computer applications were developed, building on this innovative open source code. DivX was one of these technologies. DivX is a piece of compression software allowing DVDs to be downloaded and viewed online in a shorter manner, using less space on a computer's hard-drive. It is now widely used in many legitimate application features such as game consoles and video streaming. Many companies, including Sony and Universal Studios (the same companies involved in the law suits against the developers and publishers of DeCSS), use this technology to stream video online. This example demonstrates that even software code that is thought to have only malicious uses can provide a foundation for future legitimate use. The development and deployment of technology is rarely foreseeable as new, unanticipated applications of technologies are constantly evolving. A narrow approach to software as a protected form of expression could have unintended negative effects on the future development and functions of technology.

B. The Oakes *Test*

Bill C-60, as it was drafted, may have violated subsection 2(b) of the *Charter*. Assuming that the anticircumvention measures proposed in Bill C-60 would have violated subsection 2(b) of the *Charter*, whether a measure would have been saved under section 1 of the *Charter* would have largely depended on whether the traditional balance of copyright law was preserved.

The purpose of anticircumvention measures are considered to be pressing and substantial by the copyright industry. Anticircumvention provisions are promulgated to suppress copyright piracy and infringement, and to promote the availability of copyright works in digital form. The Canadian Government further recognized the benefits derived from a strong network-based economy, the relationship among democracy, electronic commerce, and Government-On-Line,[199] and that the success of a network-based economy is dependent on the availability of creative content.[200] Without adequate protection, the goals of copyright could be undermined, and lack of protection could discourage artistic progress. Copyright and anticircumvention measures serve goals of social value. Additionally, the pressing and substantial nature of anticircumvention measures is buttressed by Canada's international obligations as a signatory to the *WIPO Copyright Treaty*.[201]

The more important question is whether anticircumvention measures would actually achieve the goals sought or if they would, in fact, hinder them. Concerned with the possible ramifications of anticircumvention legislation, the Copyright Policy group at the Department of Canadian Heritage commissioned two studies on this topic[202] concluding that the market for digital content and the extent of M development are unknown and, until the M market matures, the Canadian Government should refrain from adopting legislative measures.[203]

Within a freedom of expression analysis a key question surfaces: Is the implementation of anticircumvention measures, whether access control mechanisms or anti-device measures, justified when compared to potential drawbacks of implementation—one being its impact on free expression—at such an early stage of the development of circumvention and anticircumvention technologies? Surely the values of free expression, that is, what society seeks to recognize as deserving of protection, will vary depending on the context and, perhaps, mode of communication. The core underpinnings of freedom of expression within the context of journalism

---

[199] See Government On-Line, online: Government On-line <http://www.gol-ged.gc.ca>.

[200] See Intellectual Property Policy Directorate (Industry Canada) and Copyright Policy Branch (Canadian Heritage), "Consultation Paper on Digital Copyright Issues" (2001), online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwapj/digital.pdf/$FILE/digital.pdf>.

[201] In *Michelin*, *supra* note 43 at 380-81, the court acknowledged that international obligations are a factor when addressing the pressing and substantial element of a statutory provision.

[202] Ian Kerr, Alana Maurushat & Christian S. Tacit, "Technical Protection Measures: Part I—Trends in Technical Protection Measures and Circumvention Technologies" (2002), online: Department of Canadian Heritage <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/index_e.cfm> [Kerr, Maurushat & Tacit, "TPM Part I"]; Kerr, Maurushat & Tacit, "TPM Part II," *supra* note 180.

[203] An example may be drawn from the recent purchase of ContentGuard, a company specializing in Digital Rights Management, by Time Warner and Microsoft. ContentGuard has a patent on the popular XrML (eXtensible rights Markup Language). As noted by Michael Miron, CEO of ContentGuard, "Together with Microsoft's, Time Warner's input into our company's direction will accelerate the pace of development for the new standards and technologies that we champion." See Preston Gralla, "Time Warner, Microsoft Make DRM Move" *CRN* (8 April 2004), online: CRN <http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=18841418&_req>.

may be different than what elements of free expression are valued in a labour dispute or in the context of pornography.

We are at an early stage in the digital era where we are only starting to see the value of expression as conveyed through technology. The specific measures on circumvention that are adopted will be influential in carving out what subsection 2(b) of the *Charter* means in the digital age. Will information sharing be facilitated and fostered in this new environment, will information be retained in an enclosed domain where it is subject to an owner's exclusive control, or will a median be negotiated between these two competing values? A freedom of expression analysis will be contingent on the extent and scope of the provisions adopted and on the future design of such technologies. The actual technologies and programs that individuals and corporations employ will dictate the political philosophy of this new medium.

While Bill C-60 was not passed, its legislative objectives stated in the opening summary offer some useful insight into these questions:

> This enactment amends the *Copyright Act* to implement the provisions of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, to clarify the liability of network service providers, to facilitate technology-enhanced learning and interlibrary loans, and to update certain other provisions of the Act.[204]

Unlike the *Copyright Act*, which strives to balance the interests of both copyright holders and users, Bill C-60 did not purport to do so. The anticircumvention measures proposed in Bill C-60, however, are grounded in persuasive arguments. First, in the absence of adequate protection, producers will not make content available in a digital form capable of networked distribution. Second, the copyright industries are an important and prosperous sector of the economy. Finally, legislation must introduce anti-device measures and general access control measures because relying solely on a limited access control measure renders the legal enforcement of copyright cumbersome and ineffective. A blanket prohibition proscribing all circumvention per se raises significantly different freedom of expression challenges than would a provision that only prohibited circumvention for the purpose of infringement of copyright. In the second situation, fair dealings and a number of other exemptions would apply. At a minimum, a general access prohibition would raise questions of whether freedom of expression had been minimally impaired. A limited access control measure would likely be less of an impediment.

It is important to recognize from a policy perspective that the prohibition of circumvention devices may discourage capital flow to innovative technology, thereby impeding one of the goals that copyright legislation sought to secure: the encouragement of innovative works. These same provisions may also act as a deterrent to open-source programming in Canada by exposing individuals to liability. Although these issues may not be entirely pertinent to a freedom of expression

---

[204] *Supra* note 184, Summary.

analysis, they do demonstrate potential weaknesses in what anticircumvention measures purport to achieve and what they *actually* achieve.

Bill C-60 did not contain a general access measure nor did it contain an anti-device measure. This does not mean that the test of rational connection would not have been met. It merely means that it is more likely that the test would have been met. If the rational connection test is met, it does not mean that freedom of expression would have been minimally impaired with the absence of such measures.

Whether or not there is a minimal impairment of the freedom of expression largely depends on the wording of the provision and whether or not there were exemptions. It would also be contingent upon whether circumvention per se was prohibited rather than only prohibiting circumvention for the purpose of copyright infringement. For example, if the measures were to read: "prohibit the circumvention, for infringing purposes, of technological measures, where such measures are designed to restrict acts not permitted by the *Copyright Act*," it is more likely that the provision would be found to minimally impair the right to freedom of expression (providing that fair dealings of works currently allowed under the *Copyright Act* remained in effect as well as any other relevant exemptions).

If, however, an approach were taken along the lines of the United States or the European Union (i.e., that of prohibiting circumvention regardless of whether there is copyright infringement), it becomes more doubtful that freedom of expression would be minimally impaired. Such a prohibition on circumvention could allow an organization or company to control the legitimate use of a work by utilizing encryption code to limit access to the work. This type of prohibition could have the effect of denying access to works that are in the public domain, or works that would normally fall under an exemption such as fair dealing. The prohibition could preclude valid activity that conforms to the principles underlying freedom of expression: the attainment of truth, participation in social and political decision making, and the fostering of a tolerant and diverse society. For example, while the *Copyright Act* has a fair dealing exemption for educational institutions, a technical prohibition coupled with a statute outlawing all cases of decryption of technical protections would deprive the educational institution of the ability to exercise its rights under the *Copyright Act*. A prohibition of circumvention could have the effect of significantly curtailing freedom of expression, as it would provide an effective censorship tool for private and public organizations.

Bill C-60 was limited to works subject to copyright and to those situations where the purpose of circumvention is to infringe copyright (and moral rights where copying takes place without consent). Although not explicitly stated in Bill C-60, one can reason that fair dealing exemptions would have applied in the context of circumvention. Such fair dealing exemptions might include educational use, criticism, reverse engineering of computer code, and interoperability (e.g., open source operating system). At first blush, the circumvention measures in Bill C-60 seem to minimally impair the right to free expression. Unlike the American context, however, fair dealings are defences to copyright infringement; they are not rights conferred on

the users of copyright. Businesses and governments may include contractual provisions that impair, if not eliminate, a user or consumer's ability to deal fairly with the copyright works. In fact, during previous rounds of copyright reform in Canada there was a recommendation to adopt a fair use doctrine rather than the British legacy of fair dealings.[205] Australia is also considering such a switch. Fair dealings could be viewed as an empty concept in Canada, especially in the context of computer software; most proprietary software is distributed with a contractual limitation forbidding any manipulation of the computer code, rendering the fair dealing defence of reverse engineering and interoperability non-existent.[206]

Another potential problem with the implementation of access measures, as illustrated by Jane Ginsburg, is the allowance for what she calls a "fair access exception for purposes of making a transformative use."[207] Ginsburg suggests that a more suitable circumvention measure in the United States would be to continue to provide protection against unauthorized initial access to a protected work, but to allow for circumvention in order to engage in the fair uses where a copy has been lawfully acquired. The same analogy could be made in the Canadian context with respect to the fair dealings of a work. In order to ensure that freedom of expression is minimally impaired, the legislator may wish to adopt a measure similar to Ginsburg's suggestion.

Of course, this becomes a circular argument; the protection of the initial unauthorized access, and the allowance of circumvention in order to engage in fair dealings would likely be rendered ineffective if circumvention devices and services were prohibited. Indeed, Bill C-60 would have made it illegal to offer circumvention services. While there may be some individuals capable of circumventing access controls without relying on the products or services of others, the vast majority of users will have to rely on circumvention devices or services. The problem is that the same devices are used for infringing and non-infringing purposes, making it impossible to restrict or permit devices based on their use. Furthermore, if circumvention were allowed or privileged as a matter of free expression, it would be difficult to sustain a prohibition on the creation and trade in products necessary to enable users to engage in circumvention. The right to freedom of expression in this circumstance would likely be impaired if the use of devices and services necessary to engage in effective speech are prohibited.

---

[205] See Barry Torno, *Fair Dealing: The Need for Conceptual Clarity on the Road to Copyright Revision* (Ottawa: Copyright Revision Studies, Research and International Affairs Branch, Bureau of Corporate Affairs, Consumer and Corporate Affairs Canada, 1981).

[206] See generally Lucie M.C.R. Guibault, "Contracts and Copyright Exemptions" in P. Bernt Hugenholtz, ed., *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (The Hague: Kluwer Law International, 2000) 125.

[207] J. Ginsburg, "From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law," (2003) 50 J. Copyright Soc'y U.S.A. 113 at 130. The author argues that problems arise, not only when users cannot make use of a work under a fair use right, but also in the context where a user cannot obtain access to a work under reasonable terms.

The wording of Bill C-60 indicated that fair dealings would have applied to circumvention. Are fair dealings an adequate manner of redressing the unbalanced shift that Bill C-60 potentially presented?[208] The reality is that fair dealing is merely a defence to copyright infringement, and not a right. Further to this articulation, fair dealings may be significantly impaired or become non-existent through contractual provisions such as those usually found in consumer contracts for products where the contract is unilateral and non-negotiable. Most important, even if users legitimately circumvent a technological measure, they may still have been in contravention of the Bill where the use of a work would prejudice the owner of the copyright.[209] Therefore, as drafted, Bill C-60 may not have met the test under the "minimal impairment" part of *Oakes*.

In order to ensure that future legislation meets the threshold under the minimal impairment test enunciated in *Oakes*, the government may consider various options. One potential solution to preserve a more balanced scheme and to reduce the risk of the violation of free expression would be to place rights holders under a positive obligation to provide access to a person or institution falling under an exception or limitation as set out in the *Copyright Act*.[210] Such an obligation may include the positive obligation to allow access to works in the public domain, or to provide unfettered access to works to educational institutions and other organizations that are currently exempted from many of the provisions in the *Copyright Act*. It is important to note that the Supreme Court in *Haig*, recognized the possible public property right of access. The Court stated that

> a situation might arise in which, in order to make a fundamental freedom meaningful, a posture of restraint would not be enough, and positive governmental action might be required. This might, for example, take the form of legislative intervention aimed at preventing certain conditions which muzzle expression, or ensuring public access to certain kinds of information.[211]

---

[208] New rights conferred to copyright owners and holders would have included, but were not limited to the following examples: copyright infringement for personal use would no longer have been permissible; rights management and technological measures were introduced; introduction of the protection of a new type of work—"lesson"—though nowhere defined in the Bill with a host of new obligations; copyright holders (not just copyright authors) would have been able to seek remedy for the infringement of moral rights in limited contexts; educational institutions that had entered into agreements with collective societies would have been able to make authorized digital reproductions; and both the uploading and downloading of peer-to-peer files would have been considered copyright infringement.

[209] See Bill C-60, *supra* note 184, s. 34.02(3)(b).

[210] Many academics have made similar arguments. Lessig predicts that future debate will centre on the issue of "copy-duty" while Foley argues for a "Digital Lending Right" and Hugenholtz calls for a new access right to public information law. Lessig, *supra* note 19 at 127; Joshua H. Foley, "Enter the Library: Creating a Digital Lending Right", Comment (2001) 16 Conn. J. Int'l L. 369; P. Bernt Hugenholtz, "Copyright, Contract and Code: What Will Remain of the Public Domain?" (2000) 26 Brook. J. Int'l L. 77.

[211] *Haig*, *supra* note 115.

One may infer from this judgment that, even if Parliament chooses not to include a positive obligation provision (there was no such contemplation in Bill C-60), it is possible that a court could mandate governmental action in order to render freedom of expression meaningful.

The Supreme Court of Canada, in the recent decision of *Théberge v. Galerie d'Art du Petit Champlain*,[212] further emphasized the need for a balanced approach to copyright law. It paid attention to the importance of the public domain in fostering creative innovation:

> The proper balance among these and other public policy objectives lies not only in recognizing the creator's rights but in giving due weight to their limited nature. In crassly economic terms it would be as inefficient to overcompensate artists and authors for the right of reproduction as it would be self-defeating to undercompensate them. Once an authorized copy of a work is sold to a member of the public, it is generally for the purchaser, not the author, to determine what happens to it.
>
> Excessive control by holders of copyrights and other forms of intellectual property may unduly limit the ability of the public domain to incorporate and embellish creative innovation in the long-term interests of society as a whole, or create practical obstacles to proper utilization. This is reflected in the exceptions to copyright infringement enumerated in ss. 29 to 32.2, which seek to protect the public domain in traditional ways such as fair dealing for the purpose of criticism or review and to add new protections to reflect new technology, such as limited computer program reproduction and "ephemeral recordings" in connection with live performances.[213]

While it is true that the legislature may not have an affirmative duty to prevent the control of information through encryption codes, it seems counterintuitive to ignore the potential ramifications and widespread abuse that may result from such a system. The important question to ask is what is at stake if such provisions act as a catalyst for the widespread abuse and control of information that may, or may not be, the subject of copyright protection. Add to this that actual copyright infringement need not occur to trigger the circumvention measure; it is sufficient that the purpose be copyright infringement. Freedom of expression rhetoric has traditionally rested on the premise that it is government power, rather than private power, that is the main threat to free expression. Anticircumvention provisions could reverse this paradigm, as they create the potential over-concentration of the marketplace of ideas, and more important, limit access to content to a small group of commercial organizations. Without the application of fair dealings and a positive access right to information, such provisions would potentially allow an organization to take action against someone who has circumvented a technological measure before copyright

---

[212] *Théberge v. Galerie d'Art du Petit Champlain*, [2002] 2 S.C.R. 336 at 355-56, 210 D.L.R. (4th) 385, 2002 SCC 34.

[213] *Ibid.* at 355-56.

infringement is proven. This power is a form of private censorship that strikes at the very heart of the right to freedom of expression.

Undoubtedly, the wide dissemination of information and the existence of diverse and antagonistic sources of rhetoric are goals worth pursuing if freedom of expression is to have any meaning. The notion that the government itself should not purposefully impede the free flow of ideas does not afford non-governmental combinations or organizations a refuge if they impose restraints on free expression. To say so would undermine the very thing that is at stake—the assurance that freedom of expression actually means something in the digital age. It would seem that any analysis of freedom of expression that is process-oriented and not goal-oriented may undermine the appropriate scope of the right to free expression.

The effects of anticircumvention provisions could be severe enough to outweigh the government's pressing and substantial objective of providing protection to copyrighted works in the digital age. As the M market is not fully developed, an analysis of deleterious effects in the Canadian context is based on speculation. There are, however, important lessons to be learned from other jurisdictions that have adopted anticircumvention measures, most notably the United States and Europe.

Some serious problems arising from the application of anticircumvention measures concern: (1) the impairment of the fair use and fair dealing doctrine; (2) the violation of free expression; (3) the enclosure of the public domain through digital lock-up; (4) a skewing of the balance that copyright policy has traditionally aimed to achieve between private rights and the public interest; (5) the inadequate privacy protection afforded to individuals whose private information may be tracked through the use of Ms;[214] (6) the chilling effect on scientific research; and (7) the extent to which such a complex maze of prohibitions and exemptions is workable. Although some of these concerns may be culture specific, others are readily applicable to most nation states. As evident from the discussion above, Bill C-60 as drafted would have created an environment where deleterious effects may outweigh any salutary effects.

The three following examples further illustrate the potential deleterious effects of anticircumvention measures and freedom of expression.[215] Our first example involves a declaratory judgment against the *DMCA* sought by Professor Edward Felten, his research team, and Usenix (a technical conference). The recording industry issued a challenge (the "Hack SDMI Challenge") to the computer community to test the security of their digital watermark (copy protection) technology known as SDMI. Professor Felten's team circumvented a number of the SDMI protection mechanisms, but declined to accept the prize for successfully breaking these codes as doing so would require signing a non-disclosure agreement. Instead, Professor Felten and his

---

[214] Graham Greenleaf, "IP, Phone Home: The Uneasy Relationship Between Copyright and Privacy, Illustrated in the Laws of Hong Kong and Australia" (2002) 32 Hong Kong L.J. 35.

[215] These examples are drawn from Kerr, Maurushat & Tacit, "TPM Copyright's Windmill", *supra* note 177.

team wished to present and publish their findings at an academic conference. The SDMI member companies sent Felten's team a letter threatening action under the provisions of the *DMCA*. The Usenix group became concerned that they could be subject to civil and criminal liability if they allowed the paper to be presented at its security conference. After receiving severely negative publicity, the recording industry withdrew its opposition allowing Professor Felten and his team to present their paper.[216]

Our second example involves the impact the *DMCA* is having in the scientific community. The case involves a professional cryptographer, Niels Ferguson, who found a fatal flaw in a cryptographic system known as High-Bandwidth Digital Content Protection ("HDCP"). HDCP is a device that allows interconnection between DVD players and digital cameras with other digital devices such as television. Ferguson found that the flaw in HDCP could result in the decryption of movies, impersonation of any HDCP device, and even the creation of new HDCP devices that would work with legitimate ones.[217] Ferguson wrote a paper containing the results of his research which, under normal circumstances, he would have published. After the Felten debacle, however, Ferguson became afraid to publish his paper for fear of prosecution under the *DMCA* (even though he lives in the Netherlands). His concerns stemmed from the fact that he often traveled to the United States. Fergusen has voiced additional concerns regarding the *DMCA*: it protects flawed software instead of encouraging the repair of such flaws prior to their mass adoption in the manufacture of electronic products, and it interferes with free speech.[218]

Our last example, illustrating the extent to which the *DMCA* has had a chilling effect on freedom of expression in the science community, is a contractual clause found in the standard copyright form of the Institute for Electrical and Electronic Engineers ("IEEE").[219] The IEEE is a non-profit, technical professional association with 375,000 members in approximately 150 countries. According to its website, it is a leading authority in a wide range of areas including aerospace, computers and telecommunications, biomedicine, electric power, and consumer electronics.[220] The organization further claims to produce thirty per cent of the world's published literature in these areas producing over one hundred journals, and holding more than three hundred technical conferences each year. Participants in IEEE publications and conferences were required to sign the IEEE copyright form where they warranted that the publication or dissemination of the work did not violate any proprietary right or

---

[216] A summary of this case and other related information is found on the website of the Electronic Frontier Foundation, online: Electronic Frontier Foundation <http://www.eff.org/IP/DMCA/Felten_v_RIAA/>.

[217] Kerr, Maurushat & Tacit, "TPM Copyright's Windmill", *supra* note 177 at 70.

[218] This dilemma is described in Niels Ferguson, "Censorship in Action: Why I Don't Publish My HDCP Results," online: <http://www.macfergus.com/niels/dmca/cia.html>.

[219] "IEEE Copyright Form", online: Institute for Electrical and Electronic Engineers <http://www.ieee.org/about/documentation/copyright/cfrmlink.htm>.

[220] IEEE online: IEEE <http://www.ieee.org/about/>.

the *DMCA*.[221] As a result of extreme pressure both internal and external to the organization, the IEEE decided to remove the contractual warrant in the summer of 2002.[222]

These examples illustrate the potential deleterious effects that an anticircumvention provision could have on the values that underpin freedom of expression. Any provision adopted would have to balance competing economic and proprietary rights with the public interest in the dissemination of knowledge. It is plausible that in a particular factual situation, freedom of expression concerns may outweigh the concerns iterated by the protection copyright via anticircumvention measures. If, for example, no heed is paid to fair dealings, the promulgation of anticircumvention measures could have a very serious deleterious effects.[223] A positive access right may be necessary to minimize the negative impact of such legislative measures.[224] Even when fair dealings would apply to circumvention, as was the case in Bill C-60, there is still the potential to allow a distortion of the balance that copyright has traditionally respected. The following example illustrates that potential.

C. Hypothetical: Inuktitut Educational Video Game

Company X creates an educational video game program, Spacia. Company X sells the video game to a larger computer and games company, Sintendo. Spacia will only play on Sintendo game consoles. Additionally, Sintendo game consoles are fitted with a computerized v-chip to prevent the playing of pirated and non-regional games. X sells the video game Spacia with licensing restrictions that prohibit any reverse engineering of the computer code.

Daniel Ducheneaux runs a cultural and educational centre in the Nunavut territory. On a recent trip to Europe, he purchases Spacia. When he returns to Nunavut, he is unable to play Spacia on his Sintendo game console as the v-chip contained inside only allows for games with "regional access code" to play on the North American Sintendo game console. Annoyed with this, he searches the Internet and purchases a mod-chip that circumvents the v-chip. With the mod-chip, Daniel is able to play Spacia on his Sintendo game console. After playing Spacia, Daniel is greatly impressed with the video game and its ability to amuse and educate at the same time. He wishes that similar video games could be developed using Inuktitut as

---

[221] Ironically, the text of the actual copyright form refers to it as the "*Digital Copyright Millennium Act* (the 'DCMA')."

[222] Lisa M. Bowman, "IEEE Backs Off on Copyright Law" *ZDNet News* (16 April 2002), online: ZDNET <http://zdnet.com.com/2100-1106-884288.html>.

[223] In *Michelin*, *supra* note 43 at 381, the court highlighted that the list of exceptions in the *Copyright Act* implied that the defendant's right of free expression had been minimally impaired.

[224] A positive access right would provide the public with a legally protected right to access digital information. See *e.g.* Julie E. Cohen, "Intellectual Privacy and Censorship of the Internet" (1998) 8 Seton Hall Const. L.J. 693 at 700-701.

this would help him to educate the children at the education and cultural centre in the ways of their culture as well as in their language development.

One student at the education and culture centre is a young computer science whiz, aged fifteen, named Suzanne Hudon. Daniel tells Suzanne about Spacia and gives her the game to play. Intrigued by the game, Suzanne spends the next few months reverse engineering the computer code in Spacia. During these few months, Suzanne adapts the computer code in Spacia so that it will run on her Linux operating system at home. She then spends an additional six months developing a computer code that would enable students at the education and cultural centre to play the video game in Inuktitut. In doing so, she has invented the first computer code to translate from English to Inuktitut, which she calls Tranab. Suzanne takes the modified Spacia game and gives it to Daniel. Spacia is an absolute hit at the centre with the children. Daniel asks Suzanne to make some extra copies to distribute to some of the other education and cultural institutes in Nunavut, as well as to some of the students so that they can play the games at home.

Is there a protected form of expression in the above example? Do all derivatives of Spacia qualify as a protected form of expression? How does one measure the "core of the value of expression" found in Spacia, the derivative of Spacia, and Tranab? Would the circumvention have been lawful under Bill C-60? Does such circumvention negatively affect the sales and distribution of Spacia? Would Bill C-60 in application to this situation have violated subsection 2(b) of the *Charter*?

The proposal in Bill C-60 would not have covered the circumvention of an access measure used to prevent the playing of pirated and non-regional video games on the Sintendo game console nor would it necessarily have to do so. An effective mod-chip would have to include identical computer code in parts as the v-chip. The unauthorized copying of this computer code would already constitute direct copyright infringement under the *Copyright Act*.

The sale of the mod-chip may have contravened the circumvention provisions in Bill C-60 if it could be said that the seller was providing a circumvention service. It is plausible that Suzanne's actions may also fall within the context of circumvention service.

Suzanne would furthermore not be able to rely on the fair dealing defence of reverse engineering to make the computer code operable with the Linux operating systems because she has not herself purchased the product (licence to use Spacia). Even if she had purchased her own copy of Spacia, the contractual provisions would prohibit her from relying on the fair dealing defence.

To go one step further, the eventual distribution of the revised Spacia to other educational and cultural institutions in Nunavut could have potentially violated the circumvention measures in Bill C-60 were they to prejudicially affect the copyright owner.

Imagine that the translation program Tranab became used in many applications to translate from the English to Inuktitut. As has been demonstrated, the line between property and economic rights, and freedom of expression are not easily reconciled.

The approach taken in *Thériault*,[225] applied to the above example could yield problematic results. To protect Spacia as expression, and not the derivative of Spacia nor Tranab because access to the code was achieved through circumvention of a measure, coupled with contravention of a contractual provision (a controversial contractual provision at that) is disturbing. At a minimum, subsection 2(b) of the *Charter* should protect the activity, whatever the method, while section 1 should be employed to limit certain uses. The impact of the legislative provisions would have to be considered under the *Oakes* test with the hope of greater reducing any adverse and negative effects of the circumvention measures.

Conclusion

While the absolute language of the First Amendment and the lack of a limiting clause in the American Constitution have caused academic and jurisprudential confusion in the United States, Canadian courts should embrace the unique features of the *Charter* to simplify the analysis. Subsection 2(b) of the *Charter* has been given a broad interpretation by the Supreme Court and the limitation clause of section 1 supports the liberal approach. Canadian courts should avoid being drawn into a debate regarding the functionality of software and should instead recognize the expressiveness of code and its necessity in supporting the principles underlying freedom of expression. The argument that software and computer code are signaled as having a particular function is a slippery slope; there are always unanticipated uses of technology and its underlying computer code. The communication of ideas through computer code should be recognized as a protected form of expression under subsection 2(b) of the *Charter*. Canadian courts should, consequently, allow section 1 of the *Charter* to act as the arbiter in the determination of whether specific legislation limiting the use of software is constitutional.

---

[225] *Supra* note 95.