Clouding Accountability: Canada's Government Secrecy and National Security Law "Complex"

CRAIG FORCESE*

Strong philosophical arguments, international legal precepts and the federal Access to Information Act *favour openness and transparency in government. Yet, national security interests may sometimes justify non-disclosure. Deciding when national security should trump access to information is a difficult undertaking, one regulated in Canada by law. Part 1 of this Article sets out the policy and legal basis for open government at the federal level in Canada. Part 2 juxtaposes this information disclosure regime with government secrecy law. Special attention is paid to the controversial* Security of Information Act, *the national security exemptions to the* Access to Information Act *and recent national security amendments to the* Canada Evidence Act. *The Article argues in Part 3 that these and other statutes comprise a labyrinth of imperfectly integrated national security secrecy law. The Article concludes with three "quick fixes" bringing government secrecy laws into better alignment with open government policies and international best practices, while at the same time permitting non-disclosure of legitimate national security secrets.*

Des arguments philosophiques convaincants, des principes de droit international et la Loi sur l'accès à l'information *fédérale militent en faveur de l'ouverture et de la transparence du gouvernement. Par contre, la sécurité nationale justifie parfois la non-communication de renseignements. Décider à quel moment la sécurité nationale doit primer sur l'accès à l'information est une tâche difficile, qui au Canada est régie par la loi. Cet article expose en première partie la politique et les fondements juridiques du gouvernement fédéral transparent au Canada. En deuxième partie, l'article examine ce régime de communication des renseignements contre la toile de fond de la loi relative au secret gouvernemental. Une attention particulière est accordée à la* Loi sur la protection de l'information *qui est controversée, aux exceptions à Loi sur l'accès à l'information pour des motifs de sécurité nationale ainsi qu'aux modifications récentes apportées à la* Loi sur la preuve au Canada *en matière de sécurité nationale. En troisième partie, l'argument est fait que ces lois et d'autres encore forment un labyrinthe législatif désordonné en matière du secret lié à la sécurité nationale. En conclusion, l'article propose trois solutions rapides pour que les lois relatives au secret gouvernemental soient plus en harmonie avec la politique de transparence du gouvernement et les pratiques exemplaires en droit international, tout en permettant la non-communication de secrets légitimement liés à la sécurité nationale.*

---

* Assistant Professor, Faculty of Law, University of Ottawa. B.A. (McGill), M.A. (Carleton), LL.B. (Ottawa), LL.M. (Yale), of the Bars of Ontario, New York and the District of Columbia. My thanks to Lise Rivet for her careful comments on drafts of this article and to the editors and staff of the *Ottawa Law Review* for their diligent editorial assistance.

Table of Contents

Clouding Accountability: Canada's Government Secrecy and National Security Law "Complex"

CRAIG FORCESE

Introduction

"SECRECY," SAID THE FRENCH Cardinal Richelieu in 1641, "is the first essential in affairs of the State."[1] Constraints on information may give governments a leg-up over their international rivals, preserve them from their enemies and insulate them from domestic opponents. Of course, what was virtue in Richelieu's day may be vice in today's modern democracies. One fierce opponent of government secrecy, Ralph Nader, has called information the "currency of democracy."[2] Only openness and transparency preserve citizens from the malfeasance, incompetence, corruption and self-serving behaviour of incumbent governments. Information is, as US Supreme Court Justice Louis Brandeis once quipped, "the best of disinfectants."[3]

Relative latecomers to the open government game, Canadians have shared this suspicion of government secrecy. Former Auditor General of Canada Denis Desautels has urged that "[i]nformation is the current that charges accountability in government."[4] Government accountability, in this view, requires timely and extensive access to government information. Absent a capacity to compel disclosure of information unfavourable to government, citizens—including elected members of Parliament—remain dependent on the potentially self-serving information government chooses to release.

Yet, while the case for citizen access to information is a strong one, few would disagree that the free flow of information should be constrained in certain circumstances, including in the interests of national security. Thus, as one expert in information policy has observed, "[i]t is difficult to

---

1. Duc De Richelieu, "Maxims" *Testament Politique* (1641), online: Bartleby <http://www.bartleby.com/66/34/46534.html>.
2. See *e.g.* "Ralph Nader interview" online: Academy of Achievement <http://www.achievement.org/autodoc/page/nad0int-4>.
3. Louis D. Brandeis, *Other People's Money and How the Bankers Use It* (New York: Frederick A. Stokes Company, 1914) at 92.
4. Canada, Office of the Information Commissioner of Canada, *Annual Report 2000–2001* (Ottawa: Minister of Public Works and Government Services) online: Office of the Information Commissioner of Canada <http://www.infocom.gc.ca/reports/2000-2001-e.asp>.

think of national security without also thinking about government secrecy."[5] Protection of the nation and its inhabitants may depend on keeping from enemies information about weapons systems, troop strengths, intelligence assets or physical vulnerabilities. As the famous World War II-era admonishment warned, "loose lips...sink ships."[6]

Still, secrecy, even when motivated by an objective as fundamental as national security, may sometimes create more perils than it forestalls. In 2003, the Standing Senate Committee on National Security and Defence released its report, *The Myth of Security at Canada's Airports*. The study documented deeply inadequate security at Canadian airports, even in the post-9/11 era, and concluded that "the front door of air security...[is] now being fairly well secured, with the side and back doors wide open."[7]

In the course of preparing its report, the Committee was "criticized for calling witnesses that have shared knowledge of these breaches with the Canadian public."[8] It rejected this criticism, observing:

> You can be sure that ships really will sink if they have a lot [*sic*] holes in them. And those holes aren't likely to get patched unless the public applies pressure to get the job done. They certainly aren't patched yet.
>
> The Committee recognizes the need to balance the public's right to know against the interests of national security. But unreasonable secrecy acts against national security. It shields incompetence and inaction, at a time that competence and action are both badly needed.[9]

National security, in other words, is not about insulating governments from embarrassment.

The dilemma of any government information regime lies in balancing the strong public interest in disclosure in all areas, including national security, against legitimate refusals to disclose. As the Senate Committee acknowledged, seeking assurances that secure doors at airports are actually locked is

---

5. Alasdair Roberts, "National Security and Open Government" (Spring 2004) 9:2 *The Georgetown Public Policy Review* at 69 [Roberts, "National Security and Open Government"].
6. The phrase was an allusion to the dangers to Atlantic convoys of German foreknowledge of sailing times and routes. See "Loose Lips Sink Ships," online: EyeWitness to History <http://www.eyewitnesstohistory.com/lslips.htm>.
7. Canada, Standing Senate Committee on National Security and Defence, *The Myth of Security at Canada's Airports* (January 2003) at 9, online: <http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.pdf>.
8. *Ibid.* at 11.
9. *Ibid.* at 12–13. Similar comments have been made by academic observers. See Sandra Coliver, "Commentary on The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" in Sandra Coliver *et al.*, eds., *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information* (The Hague: Martinus Nikhoff Publishers, 1999) 11 at 11–12 ("[F]reedom of expression and access to information, by enabling public scrutiny of government action, serve as safeguards against government abuse and thereby from a crucial component of genuine national security."); Paul H. Chevigny, "Information, the Executive and the Politics of Information" in Shimon Shetreet, ed., *Free Speech and National Security* (Boston: M. Nijhoff Publishers, 1991) 130 at 138 ("[t]he problem with the 'national security state' is not so much that it violates [fundamental] rights, although it sometimes does just that, but that it can lead to the repetition of irrational decisions").

a proper public concern. Demanding disclosure of the combination codes to those doors would not be.[10]

In Canada, how government balances disclosure with secrecy is ultimately a legal issue. At least eight federal statutes limit citizen access to government information on national security grounds. The most notable of these are the *Access to Information Act*,[11] the *Canada Evidence Act*[12] and the *Security of Information Act*.[13] However, several other, less information-specialized statutes also include controls on government information. Assessing the utility and propriety of this vast and poorly understood labyrinth of statutes is an important undertaking in a democratic system, especially in an era fixated on security concerns.

This article takes up this challenge in three parts. Part 1 sets out the policy and legal basis for open government at the federal level in Canada, examining philosophical arguments favouring information access, highlighting the international legal context and then focusing in particular on the federal *Access to Information Act*.

Part 2 juxtaposes this information disclosure regime with Canadian government secrecy law. Special attention is paid to the controversial *Security of Information Act*, the national security exemptions to the *Access to Information Act* and recent national security amendments to the *Canada Evidence Act*.

The article argues in Part 3 that these and other statutes comprise a vast "complex" of imperfectly integrated national security secrecy law. The uncertainty created by these laws—and their overbreadth—risks gravely undermining open government far more than is necessary for legitimate national security purposes. The article concludes with three "quick fixes" for government secrecy laws in Canada.

1. Access to Information and Open Government

A. ACCESS TO INFORMATION AS THE CURRENCY OF DEMOCRACY

It has become trite to argue that access to information is an essential attribute of democracy. As one of the founders of the United States, James Madison noted, "[a] popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy, or perhaps both. Knowledge will forever govern ignorance; and the people who mean

10. *Supra* note 7 at 12.
11. R.S. 1985, c. A-1 [*Access Act*].
12. R.S.C. 1985, c. C-5, s. 38.
13. R.S.C. 1985, c. O-5.

to be their own Governors, must arm themselves with the power which knowledge gives."[14]

Madison's sentiments were echoed repeatedly in discussions of what would become the United States *Freedom of Information Act (FOIA)*,[15] introduced in 1966. There, it was argued that "[f]ree people are, of necessity, informed; uninformed people can never be free."[16] In signing the *FOIA*, President Johnson noted that "[t]his legislation springs from one of our most essential principles: A democracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest."[17] In a 1978 decision under the *FOIA*, the US Supreme Court echoed this comment, noting that "[t]he basic purpose of *FOIA* is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[18]

Similar views were expressed in Canada during discussions of federal information access laws. Prime Minister Pierre Trudeau noted in 1975 that "[d]emocratic progress requires the ready availability of true and complete information. In this way people can objectively evaluate the government's policies. To act otherwise is to give way to despotic secrecy."[19] President of the Privy Council Walter Baker underscored this point in 1979, urging that "[i]f this Parliament is to function, if groups in society are to function, if the people of the country are to judge in a knowledgeable way what their government is doing, then some of the tools of power must be shared with the people, and that is the purpose of freedom of information legislation."[20]

The legislative history of what became the *Access to Information Act* contains similar statements of principle. For example, when introducing the *Access* bill for second reading in the House of Commons, Minister of Communications Francis Fox urged that "[t]his legislation will, over time,

---

14. Letter from James Madison to W.T. Barry (4 August 1822) in S. Padover, ed., *The Complete Madison*, 337 (1953), cited in T. Murray Rankin, *Freedom of Information in Canada: Will the doors stay shut?* (Canadian Bar Association, 1979) at 1.
15. *Freedom of Information Act* of July 4, 1966, Pub. L. No. 89-487, 80 Stat. 250 (5 U.S.C. § 552).
16. Freedom of Information: Hearings on S. 1666 and S. 1663 Before the Subcomm. on Admin. Practice and Procedure of the Senate Comm. on the Judiciary, 88th Cong. 3 (1964) (statement of Sen. Edward Long), cited in Charles J. Wichmann III, "Ridding FOIA of those 'Unanticipated Consequences': Repaving a Necessary Road to Freedom" (1998) 47 Duke L.J. 1213 at 1217.
17. Statement by the President Upon Signing Bill Revising Public Information Provisions of the Administrative Procedure Act, Weekly Comp. Pres. Doc. 895 (July 4, 1966).
18. *NLRB v. Robbins Tire and Rubber Company*, 437 U.S. 214 at 242 (1978), 57 L Ed 2d 159 at 178.
19. Pierre Elliot Trudeau, quoted by G. Baldwin, M.P., in *Minutes of Proceedings and Evidence of the Standing Joint Committee on Regulations and other Statutory Instruments*, 30th Parl., 1st Sess. (1974-75), 22:7, cited in Rankin, *supra* note 11.
20. *House of Commons Debates*, (29 November 1979) at 1858, cited in Canada, The Standing Committee on Justice and the Solicitor General on the Review of the Access to Information Act and the Privacy Act, *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (March 1987) at 4 [Standing Committee on Justice and the Solicitor General].

become one of the cornerstones of Canadian democracy. The access legislation will be an important tool of accountability to Parliament and the electorate."[21] In the debates on third reading, Fox argued that because of the law, "Canadians will be better informed of their government's decisions and actions. They will be better equipped to inquire into the reasons for a given course of government action. This bill—imperfect as some may find it—will make for better government in Canada."[22]

In submissions made during the review of the Act undertaken in the mid-1980s by the Standing Committee on Justice and the Solicitor-General, the Canadian Bar Association argued that "[i]n a society that is committed to democratic values, the best government is one that is responsive and responsible to the public it serves...The free flow of information is essential to an accountable government in a free society."[23] In its report, the Standing Committee cited with approval the sentiments expressed in some of the statements reproduced above and noted that the *Access Act*, along with the *Charter of Rights and Freedoms*[24] and the *Privacy Act*,[25] "represent significant limits on bureaucracy and have provided a firm anchor to individual rights."[26]

These views continue to be expressed by the Information Commissioners appointed pursuant to the Act. Then-Information Commissioner John Grace used colourful language to describe this perspective in his 1998 annual report:

> Any society aspiring to be free, just and civil must depend upon and nurture a wide array of methods for exposing, and imposing sanctions on, ethical failures. ...In one way or another, all the checks and balances designed to limit abuses of government power are dependent upon there being access by outsiders to governments' insider information.
>
> Yes, webs of intrigue are more easily woven in the dark; greed, misdeeds and honest mistakes are more easily hidden. A public service which holds tight to a culture of secrecy is a public service ripe for abuse.[27]

The courts have also recognized the importance of free access to information in a democracy. In his reasons in *Dagg v. Canada*, LaForest J. urged that "[t]he overarching purpose of access to information legislation...is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate mean-

---

21. *House of Commons Debates* (29 January 1981) at 6689.
22. *House of Commons Debates* (28 June 1982) at 18851.
23. Canadian Bar Association Task Force on the Access to Information Act/Privacy Act, "The Access to Information Act and the Privacy Act" (Submitted to the Standing Committee on Justice and Legal Affairs, April 1986) at 6.
24. *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.
25. R.S. 1985, c. P-21.
26. Standing Committee on Justice and the Solicitor General, *supra* note 20 at 1.
27. Canada, Information Commissioner, *Annual Report 1997–1998* (Ottawa: Minister of Public Works and Government Services) at 4, online: <http://www.infocom.gc.ca/reports/pdf/OIC97_8E.PDF>.

ingfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry."[28] While LaForest J. was writing in dissent, his approach to interpreting the *Access Act* was endorsed by the majority in that case and has since been followed by the lower courts.[29]

More recently, the Supreme Court has noted that the federal *Access to Information Act* makes information "equally available to each member of the public because it is thought that the availability of such information, as a general matter, is necessary to ensure the accountability of the state and to promote the capacity of the citizenry to participate in decision-making processes."[30]

B. ACCESS TO INFORMATION AS AN INTERNATIONAL RIGHT

Notably, free and ready disclosure of government information is justified by more than simply pious pronouncements on the prerequisites of democracy. Often overlooked in discussions of information law are the international legal principles favouring a large measure of openness. Thus, Article 19 of the *Universal Declaration of Human Rights* (*UDHR*) provides that "[e]veryone has the right to freedom of opinion and expression; this right includes [the right to]...*seek...and impart information* and ideas through any media and regardless of frontiers."[31] As the UN Special Rapporteur on freedom of expression has noted, this provision creates a right to disclosure of information.[32] Notably, the *Universal Declaration of Human Rights* arguably has legal force as customary international law.[33] If so, then the *UDHR* is likely part of

---

28. [1997] 2 S.C.R. 403 at para. 61, 148 D.L.R. (4th) 385 [*Dagg* cited to S.C.R.].
29. See *e.g. Canada (Attorney General) v. Canada (Information Commissioner)*, 2004 FC 431 at para. 22 (F.C.T.D.); *Yeager v. Canada (Correctional Service)*, [2003] 3 F.C. 107 at para. 29, 2003 FCA 30; *Rubin v. Canada (Minister of Transport)*, [1998] 2 F.C. 430 at para. 36, 154 D.L.R. (4th) 414 (F.C.A.) [*Rubin*].
30. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66 at para. 32, 224 D.L.R. (4th) 1.
31. *Universal Declaration of Human Rights*, GA Res. 217 A (III), 3d sess., supp. No. 13, UN Doc. A/810 (1948) [emphasis added].
32. Commission of Human Rights, Civil and Political Rights Including the Question of: Freedom of Expression, UN ESC, 56th Sess., UN Doc. E/CN.4/2000/63 (18 January 2000) at para. 42-44 ("...the Special Rapporteur wishes to state again that the right to seek, receive and impart information is not merely a corollary of freedom of opinion and expression; it is a right in and of itself. As such, it is one of the rights upon which free and democratic societies depend. It is also a right that gives meaning to the right to participate which has been acknowledged as fundamental to, for example, the realization of the right to development" and noting "...[p]ublic bodies have an obligation to disclose information and every member of the public has a corresponding right to receive information; 'information' includes all records held by a public body, regardless of the form in which it is stored...").
33. See *Statement 95/1 Notes For An Address By The Honourable Christine Stewart, Secretary Of State (Latin America And Africa), At The 10th Annual Consultation Between Non-Governmental Organizations And The Department Of Foreign Affairs And International Trade*, Ottawa, Ontario, January 17, 1995 ("...Canada regards the principles of the Universal Declaration of Human Rights as entrenched in customary international law binding on all governments"); *Alvarez-Machain v. United States*, 331 F.3d 604, 618 (9th Cir. 2003) ("We have recognized that the Universal Declaration, although not binding on states, constitutes 'a powerful and authoritative statement of the customary international law of human rights'"), citing *Siderman de Blake v. Republic of Argentina*, 965 F.2d 699 (9th Cir. 1992).

the common law of Canada.[34]

Meanwhile, Article 19 of the *International Covenant on Civil and Political Rights*[35] ratified by (and thus directly binding on) Canada, also provides that "[e]veryone shall have the right to freedom of expression; this right shall include freedom to *seek, receive and impart information and ideas of all kinds*, regardless of frontiers; either orally, in writing or in print, in the form of art, or through any other media of his choice."[36] Pursuant to Article 19(3), this right is subject *only* to such restrictions "as are provided by law and are necessary, (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."[37]

None of these exceptions is defined in the Covenant itself, a matter of concern.[38] For this reason, a group of experts convened by the International Commission of Jurists in 1984 proposed the *Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights*.[39] Though of no legal force, the Principles provide a helpful interpretive tool, defining several of the passages found in Article 19. Taken together, the *Siracusa Principles* impose sensible constraints, designed to

---

34. See *Jose Pereira E Hijos S. A. v. Canada (Attorney General)*, [1997] 2 F.C. 84 at para. 20, [1996] F.C.J. No. 1669 (F.C.T.D.). ("The principles concerning the application of international law in our courts are well settled.... One may sum those up in the following terms: accepted principles of customary international law are recognized and are applied in Canadian courts, as part of the domestic law unless, of course, they are in conflict with domestic law. In construing domestic law, whether statutory or common law, the courts will seek to avoid construction or application that would conflict with the accepted principles of international law.").
35. *International Covenant on Civil and Political Rights*, 19 December 1966, 999 U.N.T.S. 172 (entered into force on 23 March 1976) [*ICCPR*].
36. *Ibid.*
37. *Ibid.*
38. Erica-Irene A. Daes, *A Study on the Individual's Duties to the Community and the Limitations on Human Rights and Freedoms under Article 29 of the Universal Declaration of Human Rights* U.N. Sales No. E.89.XIV.5 (1990). ("[T]he terms 'public safety' and 'national security' are not sufficiently precise to be used as the basis for limitation or restriction of the exercise of certain rights and freedoms of the individual. On the contrary, they are terms with a very broad meaning and application. Therefore they can be used by certain States to justify unreasonable limitations or restrictions.").
39. UNESCOR, 41 Sess., UN Doc. E/CN.4/1985/4 (1985) [*Siracusa Principles*].

guard against governments invoking the Article 19(3) exceptions to stave off legitimate critiques or mask improper motivations.[40]

Additional guidance on the scope of Article 19(3) may be extracted from views enunciated by the UN Human Rights Committee in response to individual complaints brought under the First Optional Protocol to the *ICCPR*. Thus, the Committee has held that a justification under Article 19(3) "must be provided by law, it must address one of the aims set out in paragraph 3 (a) and (b) (respect of the rights and reputation of others; protection of national security or of public order, or of public health or morals), and it must be necessary to achieve a legitimate purpose."[41] Thus, the Committee has rejected invocations of national security or public order to justify infringements of Article 19 where governments have failed to explain precisely how exercise of the Article 19 right threatens these interests.[42]

---

40. Thus, the Principles urge that the phrase "rights and reputation" in the Covenant does not mean a limitation "to protect the State and its officials from public opinion or criticism." *Ibid.* at para. 37. "Public order" is defined "as the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded. Respect for human rights is part of public order. *Ibid.* at para. 22. "Public health" should include only "measures dealing with a serious threat to the health of the population or individual members of the population. These measures must be specifically aimed at preventing disease or injury or providing care for the sick and injured." *Ibid.* at para. 25. "Public morals" may only be invoked to limit rights where the "limitation in question is essential to the maintenance of respect for fundamental values of the community." *Ibid.* at para. 27. "National security" is given the most comprehensive definition. Under the Principles, "[n]ational security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force." *Ibid.* at paras. 29–30. It is not an appropriate response to "merely local or relatively isolated threats to law and order." In relation to national security, the *Siracusa Principles* have now been superseded by the more detailed–and arguably more authoritative–*Johannesburg Principles*, discussed below.
41. *Malcolm Ross v. Canada*, UNICCPROR, 70th Sess., UN Doc. CCPR/C/70/D/736/1997 (2000) at para. 11.2.
42. See *e.g. Jong-Kyu Sohn v. Republic of Korea*, UNICCPROR, 54th Sess., UN Doc. CCPR/C/54/D/518/1992 (1995) (rejecting invocation of national security and public order to restrain speech allegedly directed at inciting a national strike). Further, the Committee has rejected the national security or public order justification where Article 19 rights are violated "to safeguard an alleged vulnerable state of national unity". *Albert Womah Mukong v. Cameroon*, UNICCPROR, 51th Sess., UN Doc. CCPR/C/51/D/458/1991 (1994). (The Committee "considers that the legitimate objective of safeguarding and indeed strengthening national unity under difficult political circumstances cannot be achieved by attempting to muzzle advocacy of multi-party democracy, democratic tenets and human rights") at 9.7. However, in a case brought against Canada concerning restricted access to the Parliamentary press gallery, it has agreed that "the protection of Parliamentary procedure can be seen as a legitimate goal of public order" at para. 9.7. That said, the restriction in the case was not "a necessary and proportionate restriction of rights within the meaning of Article 19, paragraph 3, of the Covenant, in order to ensure the effective operation of Parliament and the safety of its members". *Robert W. Gauthier v. Canada*, UNICCPROR, *65th Sess.*, UN Doc. CCPR/C/65/D/633/1995 (1999) at para. 13.6. In relation to the reference in Article 19(3)(b) to "rights and reputation," the Committee has noted in another case brought against Canada that the "rights or reputations of others for the protection of which restrictions may be permitted under Article 19, may relate to other persons or to a community as a whole." *Malcolm Ross, ibid.* at para. 11.5. That case concerned the removal from the classroom of a school teacher for anti-Semitic comments. When this decision was challenged as a violation of Article 19, the Committee concluded that the restrictions imposed on the complainant "were for the purpose of protecting the 'rights or reputations' of persons of Jewish faith, including the right to have an education in the public school system free from bias, prejudice and intolerance." Further, given the role of a teacher in educating the young, the restrictions imposed on the complainant were necessary. *Ibid.* at para. 11.6.

C. INTERNATIONAL "BEST PRACTICES" FOR INFORMATION ACCESS

There is also a body of comparative law influential in understanding information law and policy. Indeed, as of May 2004, over 50 countries had introduced freedom of information laws.[43] Building on this rich experience, the international free-expression non-governmental organization "Article 19" proposes nine "best practice" principles that should guide government access to information policies.[44] These principles "are based on international and regional law and standards, evolving state practice (as reflected, *inter alia*, in national laws and judgments of national courts) and the general principles of law recognised by the community of nations."[45]

Several of these standards are worth flagging in this article. First, access to information law should favour maximum disclosure. This principle obliges the government body refusing disclosure to bear the onus of demonstrating the legitimacy of this course of action.[46]

Further, exemptions from access "should be clearly and narrowly drawn and subject to strict 'harm' and 'public interest' tests."[47] The legitimacy of an exception should be measured via a three-part analysis. First, "the information must relate to a legitimate aim listed in the law." Second, "disclosure must threaten to cause substantial harm to that aim." Third, "the harm to the aim must be greater than the public interest in having the information."[48] Legitimate exceptions include, *inter alia*, the protection of national security, defence and international relations,[49] at least where there is a real prospect of harm to these interests. Indeed, most freedom of information laws include national security exemptions.[50]

In addition, laws inconsistent with the notion of maximum disclosure should be amended or repealed. Laws on government secrecy inconsistent with access laws should be subordinated to these access laws, since the latter already include carefully demarcated exceptions capturing any legitimate secrecy objectives governments might have.[51]

---

43. David Banisar, *Freedom of Information and Access to Government Record Laws Around the World* (2004), online: Freedom of Information <http://www.freedominfo.org/survey/global_survey 2004.pdf>.
44. Toby Mendel, *Freedom of Information: A Comparative Legal Survey* (2003), online: Article 19 <http://www.article19.org/docimages/1707.pdf>.
45. *Ibid.* at 23.
46. *Ibid.* at 26.
47. *Ibid.* at 28.
48. *Ibid.* at 28–29.
49. *Ibid.* at 29.
50. Banisar, *supra* note 43 at 5.
51. *Ibid.*

D. CANADA'S FEDERAL GOVERNMENT INFORMATION LAWS

An assessment of whether Canada's information laws reflect these international benchmarks requires close scrutiny of the *Access to Information Act*.[52]

1) The Right to Access

The *Access Act* creates a broad principle of access in its first dozen or so sections and then spends a sizeable portion of its remaining sections creating exceptions and caveats to this principle. It articulates a purpose consistent with the information law prerequisites as in Article 19; specifically, the express purpose of the Act is "to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government."[53]

The key provision of the Act, section 4, provides that every Canadian citizen and permanent resident "has a right to and shall, on request, be given access to any record under the control of a government institution," subject to other sections in the Act. Notably, the Federal Court has referred to this right as "quasi-constitutional" in nature.[54] In part, this status reflects the language in subsection 4(1) providing the right in section 4 applies notwithstanding any other statute.[55]

Nevertheless, it remains unclear whether the right to access articulated in section 4 also has a truly constitutional counterpart. Lower courts have refused to find a right to information disclosure in subsection 2(b) of the *Charter of Rights and Freedoms*, the constitutional free expression provision,[56]

---

52. Note should also be made of the *Privacy Act*, *supra* note 25. Among other things, this Act is supposed to provide individuals with a right of access to the information about themselves held by the government. See *Privacy Act*, s. 2. Because the *Privacy Act* disclosure regime is confined to personal information, and is not a full access to information law, a discussion of the *Privacy Act* does not figure in this article. Nevertheless, the discussion of national security exemptions under the *Access Act* found *infra* generally applies equally to the *Privacy Act*. See *e.g. Privacy Act*, s. 21.

53. *Supra* note 11 at s. 2.

54. *Canada (Attorney General) v. Canada (Information Commissioner)*, [2002] 3 F.C. 630, at para. 20, 2002 FCT 128.

55. *Canada Post Corporation v. Canada (Minister of Public Works)*, [1995] 2 F.C. 110 at 129, F.C.J. No. 241 (F.C.A.) ("subsection 4(1) contains a 'notwithstanding clause' which gives the Act an overriding status with respect to any other Act of Parliament").

56. *Criminal Lawyers' Assn. v. Ontario (Ministry of Public Safety and Security)* (2004), 184 O.A.C. 223 at para. 42, [2004] C.R.D.J. 1644 (Ont. Div. Ct.) (declining to find s. 2(b) applied where access had been denied under the Ontario law)[*Criminal Lawyers' Assn.*]; *Ontario (Attorney General) v. Fineberg* (1994), 19 O.R. (3d) 197 at 204, [1994] O.J. no. 1419 (Ont. Div. Ct.) ("it is not possible to proclaim that s. 2(b) entails a general constitutional right of access to all information under the control of government"); *Yeager v. Canada (Correctional Service)*, 3 F.C. 107 at para. 65, 2003 FCA 30 (citing and then stating: "Without endorsing all the reasons for decision given in that case, I am in respectful agreement with the conclusion of the Motions Judge that the respondent's Charter right was not contravened here.").

or in the unwritten principles of the Constitution.[57]

Yet, in a different context, the Supreme Court apparently agrees that "freedom of expression in section 2(b) protects both listeners and readers."[58] It therefore supports "open courts": "[o]penness permits public access to information about the courts, which in turn permits the public to discuss and put forward opinions and criticisms of court practices and proceedings."[59] It is not a tremendous leap to apply similar reasoning to openness of government generally. Whether the courts will eventually do so or not remains to be seen.

2) Exemptions to Access

To temper the potent section 4, the Act includes a large number of reasonably well-delimitated exemptions limiting access to information. These exemptions can be classed in two ways, as noted in the chart in the Appendix (see p. 91). First, some of the exemptions are "injury-based" while others are merely "class-based." In keeping with the group Article 19's view of best practices, injury-based exemptions may only be employed where the government concludes that disclosure will produce the harm enumerated by the Act.[60]

By comparison, class-based exemptions are triggered as soon as the requested information is found to fall within a certain class of information, as defined by the Act. There need not be any subsequent assessment of whether injury would result from disclosure, creating a substantial number of exceptions that do not meet Article 19's best practice standards.

Second, exemptions to access under the Act are of two sorts: mandatory and discretionary. With mandatory exemptions, the government is obliged to decline disclosure, subject in a few instances to a public interest override. This override allows disclosure where the public interest in disclosure outweighs the interest in non-disclosure.

In fact, the majority of exceptions in the Act are not mandatory, but rather discretionary. Thus, the government may choose to decline disclosure of a document captured by the exemption. While these discretionary

---

57. *Criminal Lawyers' Assn.*, *ibid.*, (holding that the unwritten "[democratic] principle" "is more concerned with matters relating to the proper functioning of responsible government, and with the proper election of legislative representatives and the recognition and protection of minority and cultural identities, than it is with promoting access to information in order to facilitate the expressive rights of individuals.").

58. *Ruby v. Canada (Solicitor General)*, [2002] 4 S.C.R. 3 at para. 52, 2002 SCC 75 [*Ruby* cited to S.C.R.].

59. *Ibid.* at para. 53, citing *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480 at para. 23, 139 D.L.R. (4th) 385.

60. See *e.g. Rubin, supra* note 29, at para. 30, citing *Canada Packers Inc. v. Canada (Minister of Agriculture)*, [1989] 1 F.C. 47 at 60 (F.C.A.), F.C.J. No. 615. ("Subsection 2(1) provides a clear statement that the Act should be interpreted in the light of the principle that government information should be available to the public and that exceptions to the public's right of access should be 'limited and specific'. With such a mandate, I believe one must interpret the exceptions to access in paragraphs [20(1)] (c) and (d) to require a *reasonable expectation of probable harm*") (emphasis added).

exemptions do not include a public interest override, the recent government Access to Information Review Task Force concluded that such an override "is not necessary" as discretionary exemptions "already imply a balancing of the public interest in protecting the information, and the public interest in disclosure."[61]

In fiscal year 2002–03, the most common exceptions invoked by government were the section 19 personal information exemption (32.6%), the section 20 third party information exemption (18.8%) and the section 21 operations of government exemption (16.4%).[62] This pattern has remained more or less constant throughout the life of the Act, although the relative importance of the government operations and personal information provisions as against the third party information exemption has increased in the last several years.[63]

3) Exclusions from the Act

As well as exemptions, the *Access Act* also includes three exclusions. First, the Act does not apply to published materials, or to library or museum materials preserved solely for public reference or exhibition purpose, nor to material placed in the National Archives or other cultural institutions by or on behalf of persons other than government bodies.[64] Second, and more controversially, the Act does not apply to confidences of the Queen's Privy Council for Canada—essentially Cabinet documents.[65] Further, in the wake of the government's 2001 anti-terrorism amendments, the Act does not apply to infor-

---

61. Access to Information Review Task Force, *Report: Access to Information: Making it Work for Canadians* (2002) at 43, online: Government of Canada <http://www.atirtf-geai.gc.ca/report2002-e.html> [Access to Information Review Task Force]. Authority supporting this conclusion exists in the caselaw. See *e.g. Rubin v. Canada (Minister of Transport)*, [1995] 105 F.T.R. 81 at para. 34, F.C.J. No. 1731 (F.C.T.D.) ("[w]hile not every exemption has a subsection 20(6) public interest override clause, each exemption is subject to section 2. Thus, all exemptions must meet an implicit injury test that by its very nature means balancing the harm of release against the injury that comes with non-release. Paragraph 16(1)(c) has a public interest emphasis because it stipulates an explicit injury test"), *rev'd*, but *aff'd* on this ground, *Rubin*, *supra* note 29, at para. 40 ("[a]s for the third issue, of whether or not to consider the public interest as an independent step under the test for reasonable expectation of probable injury.... Suffice it to say that I am in general agreement with the method adopted by the Trial Judge"). See also *Dagg v. Canada (Minister of Finance)*, *supra* note 28 at 16, 148 D.L.R. 385 (discussing paragraph 8(2)(m)(i) of the *Privacy Act* and commenting "the Minister is not obliged to consider whether it is in the public interest to disclose personal information. However in the face of a demand for disclosure, he is required to exercise that discretion by at least considering the matter. If he refuses or neglects to do so, the Minister is declining jurisdiction which is granted to him alone").

62. *InfoSource Bulletin*, No. 26 (2003), online: <http://infosource.gc.ca/bulletin/2003/bulletin00_e.asp>.

63. In the period 1983–91, 40% of the exemptions used involved third party information, 21.3% involved personal information and 12.1% involved the operations of government, Treasury Board, *InfoSource Bulletin* (1991). In the period 1993–1998, 28.4% of the exemptions used by government institutions invoked the third party exception, while 26.8% relied on the personal information exception and 15% cited the government operations provision. Figures calculated from Treasury Board, *InfoSource Bulletins* 1993–1998.

64. *Supra* note 11 at 68.

65. *Ibid.* s. 69.

mation certified by the government as national security information under the *Canada Evidence Act*.[66] This exclusion is discussed in greater detail below.

4) Enforcement

The Act creates a mechanism for policing government decisions on disclosure and its use of exemptions. Thus, an Office of the Information Commissioner is created, and is charged with investigating access complaints brought by requesters.[67] The Commissioner has extensive powers to conduct investigations, but has no power to compel the release of the information if he or she feels that such release is warranted. Instead, to compel disclosure, the Information Commissioner, or any requester dissatisfied with the outcome of the Commissioner's investigation, must bring an application before the Federal Court.[68]

5) Government Performance

The Information Commissioner also reports on—and critiques—government performance in Annual Reports. The Commissioner's assessment of government responsiveness to the Act has often been scathing. Thus, Information Commissioner John Grace had this evaluation in his 1998 annual report:

> A culture of secrecy still flourishes in too many high places even after 15 years of life under the *Access to Information Act*. Too many public officials cling to the old proprietorial notion that they, and not the *Access to Information Act*, should determine what and when information should be dispensed to the unwashed public...The commitment, by word and deed, to the principle of accountability through transparency has been too often, faltering and weak-kneed.[69]

Other observers have echoed the Commissioner's conclusions. In a review of the Act issued in the late 1990s, Professor Alasdair Roberts concluded that

> [t]here is now significant evidence that the administration of the [Act] has deteriorated significantly over the last five years. The time taken to process requests has lengthened; disclosure practices appear to be more restrictive; and the probability that a request will result in a substantiated complaint to the Information Commissioner has almost doubled.[70]

More specifically, Roberts found that the number of complaints upheld by the Information Commissioner had tripled between 1991 and

---

66. *Ibid.* s. 69.1.
67. *Ibid.* s. 30.
68. *Ibid.* ss. 41, 42.
69. *Supra* note 27 at 3.
70. Alasdair Roberts, Working Paper: "Monitoring Performance by Federal Agencies: A Tool for Enforcement of the Access to Information Act" (Kingston: Queen's University School of Policy Studies, 1999) at 12, online: <http://faculty.maxwell.syr.edu/asroberts/documents/papers/atia99.pdf> [Roberts Report].

1998, a pace of increase far exceeding that in the number of requests. In fiscal year 1997–98, 7.9% of all requests resulted in meritorious (*i.e.* resolved) complaints, as opposed to 2.9% in 1991–92. It was felt that these figures understated the extent of non-compliance with the Act, as many requesters abandon unfilled requests early in the process. In addition, whereas in 1993–94, 79% of requests were filled within 60 days, that figure had dropped to 68.1% in 1997–98. The number of exemptions invoked in the context of requests had also increased, from an average of 2.2 in 1993–94 to 2.44 in 1997–98.[71]

Since the Roberts Report, some performance indicators have improved. By 2002–03, requests received a response within 60 days in 82% of cases.[72] Further, the number of meritorious complaints as a proportion of total requests had fallen to 2.6%.[73] Other indicators are, however, more mixed. The proportion of access requests resulting in full disclosure stood at about one-third from 1983 to 1998, spiked at 40.6% in the late 1990s and now has dropped to below the historical average, standing at 29.6% in 2002–03.[74]

The government's Access to Information Review Task Force found in 2002 that many requestors continue to feel that the Act is applied "inconsistently and in such a way as to contradict the principles of openness, transparency and accountability that underlie it."[75] In deciding to employ discretionary exemptions, "heads of government institutions (or their delegates) do not always consider all relevant factors in exercising their discretion, nor do they articulate clear reasons for withholding information."[76] Roberts has also flagged this problem, noting that government departments and agencies "may try to stretch and test the law in an effort to protect bureaucratic or governmental interests."[77] Officials are said to be adopting broad interpretations of exemptions.[78]

Given these complaints about government as a whole, one might expect commitment to open government where national security concerns are engaged to be even more lacklustre, a matter to which this article now turns.

---

71. *Ibid.* at 2–6.
72. *Supra* note 62 at 13.
73. Calculated from *ibid.* at 12, statistical tables (total requests) and Information Commissioner, Annual Report 2002–2003, *supra* note 4, statistical tables ("resolved" column, in "Complaints Finding" table).
74. Calculated from Treasury Board, *InfoSource Bulletin*, for the period 1998–2003, online: <http://infosource.gc.ca/bulletin/bulletin_e.asp>.
75. Access to Information Review Task Force, *supra* note 61 at 3.
76. *Ibid.* at 43.
77. Roberts Report, *supra* note 70 at 2.
78. Alasdair Roberts, "Limited Access: Assessing the Health of Canada's Freedom of Information Laws" (Kingston: School of Policy Studies, Queen's University, 1998) 12, online: <http://faculty.maxwell.syr.edu/asroberts/documents/papers/limitedaccess.pdf>.

II. The National Security Challenge to Open Government

A. LEGITIMATE NATIONAL SECURITY CONSTRAINTS ON ACCESS TO INFORMATION

Few credible observers would deny that there are secrets states must keep in safeguarding the security of their citizens. On the other hand, national security should not be used to cloak governments from criticism or accountability. As one critic has noted, national security is an imprecise concept. As a consequence, it is often used "to suppress precisely the kinds of speech that provide protection against government abuse," including damage to the environment, corruption, wasting of public assets and other forms of wrongdoing by government officials.[79] There is merit, in other words, in openness, even on national security matters.

Indeed, some observers have even argued that transparency *enhances*, rather than prejudices, national security by increasing a flow of information essential in the coordination of national security efforts. Alasdair Roberts has argued that:

> [a]n informed public can help policymakers to formulate better policy, monitor the readiness of national security bureaucracies and act independently to preserve security. An information-rich environment is one in which citizens and frontline government employees are better able to make sense of unfolding events and respond appropriately to them.... In the jargon of the American military, a policy of transparency can be a powerful "force multiplier," which helps to build a state that is resilient as well as respectful of citizen rights.[80]

From this perspective, national security matters should not be excluded, *prima facie*, from open government laws. Instead, boundaries need to be drawn between information whose disclosure truly prejudices national security, and other, less problematic information. Deciding where to draw this line, and how best to define "national security" is tremendously difficult.

In partial response to this problem, experts on the topic proposed, in 1995, the *Johannesburg Principles: National Security, Freedom of Expression and Access to Information*,[81] an enhancement of the *Siracusa Principles* discussed above and a tool for interpreting Article 19(3) of the *International Covenant on Civil and Political Rights*. The UN Special Rapporteur on Freedom of

---

79. Coliver, *supra* note 9 at 12–13.
80. Roberts, "National Security and Open Government," *supra* note 5 at 82.
81. *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, UN Doc. E/CN.4/1996/39 (1996) [*Johannesburg Principles*].

Opinion and Expression has since endorsed the *Johannesburg Principles*.[82] They have also been invoked by the UN Human Rights Commission in the preamble of many of its resolutions, each time during years in which Canada was a member.[83] Further, the definition of "legitimate" national security contained in the *Johannesburg Principles* has also been cited –arguably with approval–by the House of Lords in *Secretary of State for the Home Department v. Rehman*.[84]

In their material parts, the *Johannesburg Principles* underscore that "[e]veryone has the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas of all kinds". They acknowledge that these rights "may be subject to restrictions on specific grounds, as established in international law, including for the protection of national security." However, any restriction must be "prescribed by law and...necessary in a democratic society to protect a legitimate national security interest." In practice, this requirement obliges a government to show that "the expression or information at issue poses a serious threat to a legitimate national security interest;...the restriction imposed is the least restrictive means possible for protecting that interest; and...the restriction is compatible with democratic principles."[85]

---

82. See Special Rapporteur, *Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN ESCOR, 1996, UN Doc. E/CN.4/1996/39 at para. 154 ("the Special Rapporteur recommends that the Commission on Human Rights endorse the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, which are contained in the annex to the present report and which the Special Rapporteur considers give useful guidance for protecting adequately the right to freedom of opinion, expression and information"), online: <http://www.unhchr.ch/Huridocda/Huridoca.nsf/0/7011edbe0ec2be5b802 566b1004fd129?OpenDocument>.

83. See United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 2003/42, UN ESCOR, 2003, Supp. No. 3, UN Doc. E/2003/23-E/CN.4/2003/135, 157, ("Recalling the Johannesburg Principles on National Security, Freedom of Expression and Access to Information adopted by a group of experts meeting in South Africa on 1 October 1995 (E/CN.4/1996/39, annex)"); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 2002/48, UN ESCOR, 2002, Supp. No. 3, UN Doc. E/2002/23-E/CN.4/2002/200, 206 (same); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 2001/47, UN ESCOR, 2001, Supp. No. 3, UN Doc. E/2001/23-E/CN.4/2001/167, 209 (same); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 2000/38, UN ESCOR, 2000, Supp. No. 3, UN Doc. E/2000/23-E/CN.4/2000/167, 180 (same); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 1999/36, UN ESCOR, 1999, Supp. No. 3, UN Doc. E/CN.4/1999/167-E/1999/23, (same); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 1998/42, UN ESCOR, 1998, Supp. No. 3, UN Doc. E/CN.4/1998/177-E/1998/23, ("Taking note of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information adopted by a group of experts meeting in South Africa on 1 October 1995 (E/CN.4/1996/39, annex)"); United Nations Human Rights Commission, *The Right to Freedom of Opinion and Expression*, ESC Res. 1997/27, UN ESCOR, 1997, Supp. No. 3, UN Doc. E/CN.4/1997/150-E/1997/23, (same), online: <http://www.unhchr.ch/huridocda/huridoca.nsf/Documents?OpenFrameset>.

84. [2003] 1 AC 153, [2001] 3 W.L.R. 877 at 181 per Slynn L.J. (referring to the *Johannesburg Principles* and then indicating that "[i]t seems to me that the appellant is entitled to say that 'the interests of national security' cannot be used to justify any reason the Secretary of State has for wishing to deport an individual from the United Kingdom. There must be some possibility of risk or danger to the security or well-being of the nation which the Secretary of State considers makes it desirable for the public good that the individual should be deported"). [*Rehman* cited to AC].

85. *Johannesburg Principles*, *supra* note 81.

The *Principles* carefully circumscribe what is meant by a "legitimate" national security interest. Thus, Principle 2 provides that a restriction justified on the ground of national security "is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government." Principle 2 further specifies that

> a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Thus, the *Principles* set a high threshold of national security legitimacy, with a clear focus on actual or threatened use of physical force. National security would not, therefore, apply where the secret related to some question of economic advantage or policy, say for example an anticipated Bank of Canada interest rate change. Nor would it attach to simple diplomatic correspondence, or information about Canada's negotiating position in a trade agreement. Other justifications may exist for restraining access to this information, but these justifications must flow from rationales other than national security—perhaps public order.

The *Principles* also contain standards curbing government responses to unauthorized disclosure of secrets. Thus, Principle 15 precludes punishment of a person on national security grounds "for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure." Likewise, Principle 16 condemns subjecting a person "to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure."

B. CANADIAN GOVERNMENT SECRECY LAWS

The natural question arising from the discussion above is how well Canada's government secrecy laws measure up both against its commitment to open government articulated in the *Access Act* and the hortatory standards set out in the *Johannesburg Principles*.

1) Security of Information Act

i. Background

The cornerstone of Canada's secrecy law is the *Security of Information Act*.[86] Originally enacted in 1939 as the *Official Secrets Act*,[87] the statute was amended substantially and renamed in December 2001, as part of the government's anti-terrorism omnibus law.[88] The 1939 Act, for its part, was a variant on the 1889 UK *Official Secrets Act*, and had two main foci. First, in section 3, it created an offence of espionage or spying and second, in section 4 it criminalized wrongful dissemination of information, sometimes called "leakage."[89]

This statute was roundly condemned, beginning at least in the 1960s, for its breadth and ambiguity. Thus, the Royal Commission on Security (the Mackenzie Commission) called it "an unwieldy statute, couched in very broad and ambiguous language."[90] In 1986, the Law Reform Commission condemned the statute "as one of the poorest examples of legislative drafting in the statute books."[91] It called the Act and other laws criminalizing "crimes against the state" as "out of date, complex, repetitive, vague, inconsistent, lacking in principle and over-inclusive," as well as potentially unconstitutional under the *Charter of Rights and Freedoms*.[92]

In particular, the Commission took issue with then section 3 of the Act, relating to spying, which could be interpreted as imposing an onus of proving innocence on the accused. This reversed onus, the Commission speculated, was inconsistent with subsection 11(d) of the *Charter*, which guarantees the presumption of innocence until proven guilty.[93] Criticism of the statute was voiced by the government itself in 1998, when the then-Solicitor General called the Act "badly outdated and overbroad."[94]

Perhaps for these reasons, the Act has rarely been invoked. The Canadian Security Intelligence Service reports that since 1939 there have been two dozen prosecutions under the Act, but only six in the last 40 years.[95] In one of these cases, Stephen Ratkai pleaded guilty in 1989 to

---

86. *Supra* note 13.
87. R.S.C. 1970, c. O-3. This Act, in turn, is an "adoption of the English statutes as enacted in Great Britain (1911 (U.K.) c.28, and 1920 (U.K.), c.75)"; *R. v. Toronto Sun Publishing Limited*, (1979) 24 O.R. (2d) 621 at 623, 98 D.L.R. (3d) 534 (Ont. Prov. Ct.) [*Toronto Sun*].
88. Bill C-36, *An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism*, 1st Sess., 37th Parl., 2001.
89. See Canada, Canadian Security Intelligence Service (CSIS), *Security of Information Act* (April 2004), online: <http://www.csis-scrs.gc.ca/eng/backgrnd/back12_e.html>.
90. Canada, Mackenzie Commission, *Report of the Royal Commission on Security* (Ottawa: The Queen's Printer, 1969) at para. 204.
91. Canada, Law Reform Commission, *Crimes Against the State* (Ottawa: 1986) at 30.
92. *Ibid.* at 38–39.
93. *Ibid.* at 39.
94. *House of Commons Debates*, 096 (30 April 1998) at 1010 (Hon. Andy Scott).
95. *Supra* note 89.

charges under the espionage provisions of the statute of spying for the USSR. In sentencing Ratkai to two concurrent terms of nine years, the court commented that the object of the *Official Secrets Act* "is to protect the safety and interests of the state. Every country has an obligation to protect its citizens and its territory and countries must depend and rely upon its citizens to ensure its safety and security. What is disturbing and despicable about offences of this nature is that a citizen betrays his country which he has a duty to protect and defend."[96]

However, in *R. v. Toronto Sun*—probably the leading case on the *Official Secrets Act*—the court was moved much less by the Act's objectives than by its awkward structure. At issue in this pre-*Charter* case was whether a newspaper and its editors had violated the Act by printing excerpts of a top secret document concerning Soviet intelligence activities in Canada. The court concluded that they had not, as the allegedly secret information had been previously invoked in the public domain. However, the court was also critical of the Act itself. In the court's words,

> [s]ince the *Official Secrets Act* is a *restricting* statute, and seeks to curb basic freedoms, such as freedom of speech and the press, it should be given strict interpretation.... The statute must, in clear and unambiguous language, articulate the restriction it intends to impose upon a citizen. A reading of ss. 3 and 4 of the *Official Secrets Act* amply demonstrates its failure to do so; the provisions are ambiguous and unwieldy.... A complete redrafting of the Canadian *Official Secrets Act* seems appropriate and necessary.[97]

ii. Post-9/11 Amendments

In fact, the *Official Secrets Act* was substantially amended—and renamed—by Bill C-36, the government's 2001 anti-terrorism law. The Bill C-36 changes are notable both for what they did and what they failed to do.

1. NEW WINE IN A NEW BOTTLE: NEW SECRECY LAWS IN THE *SECURITY OF INFORMATION ACT*

(a) Persons Permanently Bound By Secrecy

First, Bill C-36 created a new series of provisions under the heading "Special Operational Information and Persons Permanently Bound to Secrecy". Thus, under the new Act, persons employed at a number of security and intelligence government agencies are deemed permanently bound to secrecy.[98]

---

96. *R v. Ratkai*, [1989] N.J. No. 334 (Nfld. S.C. (T.D.)) (QL).
97. *Toronto Sun*, *supra* note 87 at 632.
98. S. 8 and accompanying schedule. Further, under s. 10, other persons may be designated "a person permanently bound to secrecy" if certain senior government officials believe that "by reason of the person's office, position, duties, contract or arrangement,...the person had, has or will have authorized access to special operational information; and...it is in the interest of national security to designate the person".

Under section 13 of the *Security of Information Act*, "[e]very person permanently bound to secrecy commits an offence who, intentionally and without authority, communicates or confirms information that, if it were true, would be special operational information." "Special operational information" is a defined term and basically means military and intelligence-related information that the government seeks to "safeguard,"[99] an undefined expression. Section 13 appears intended to allow prosecution for the communication of false secrets. Thus, under section 13, it is irrelevant whether or not the information is true. The penalty under section 13 is imprisonment for no more than five years.

Section 14 contains a second offence, permitting imprisonment of up to 14 years for a person permanently bound by secrecy who "intentionally and without authority, communicates or confirms special operational information." No caveat exists indicating that this information need not be true. Thus, section 14 seemingly penalizes only communication of true secrets. If so, then, in practice, a decision to prosecute under section 14 would create real dilemmas for the government. The mere fact of selecting section 14 over section 13 would seemingly have the effect of confirming the truth of the information communicated, something the government would likely be loathe to do. In practice, it seems likely the government would opt for a section 13 proceeding, unless no security issue is raised by admitting the truth of the information leaked.

Notably, both sections 13 and 14 are subject to a carefully defined "public interest defence". Thus, pursuant to section 15, "[n]o person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest." A person "acts in the public interest" if his or her purpose is to disclose "an offence under an Act of Parliament that he or she reasonably believes has been, is being or is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada" in circumstances where "the public interest in the disclosure outweighs the public interest in non-disclosure."[100]

---

99. S. 8.

100. In weighing the relative public interests of disclosure versus non-disclosure, s. 15(4) instructs a court to consider whether the disclosure is narrowly confined to that required to forestall the alleged offence, the seriousness of this alleged offence, whether the whistleblower resorted to other reasonable alternatives prior to disclosure, whether the whistleblower had reasonable grounds to believe that disclosure was in the public interest, the nature of that public interest, the harm or risk created by disclosure and any exigent circumstances justifying disclosure. Except where necessary to avoid grievous bodily harm, s. 15(5) makes it clear that the public interest defence only exists where two prerequisites are met: first, prior to disclosure, the whistleblower must have provided all relevant information to his or her deputy head or the deputy Attorney General of Canada and have received no response within a reasonable time. Subsequently, the whistleblower must have also provided the information to the Security Intelligence Review Committee or, where the alleged offence concerns the Communications Security Establishment, the Communications Security Establishment Commissioner, and not received a response within a reasonable time. The Act leaves open the question of what would constitute a "reasonable time". Likewise, it does not address whether the public interest defence would apply if the responses received from these bodies was inadequate.

(b) Other Anti-Espionage Provisions

The new *Security of Information Act* also includes a number of anti-espionage provisions. Thus, included under the heading "Communications with Foreign Entities or Terrorist Groups," subsection 16(1) makes it a crime for a person to communicate information the government is trying to "safeguard" to a foreign entity or terrorist group while believing (or reckless as to whether) that information is safeguarded and for the purpose of increasing the capacity of that foreign entity or terrorist group to do harm to "Canadian interests". Subsection 16(2) creates a mirror offence for circumstances where the information actually causes harm to "Canadian interests". Notably, the expression "safeguarded" is not defined. Nor are the Canadian "interests" that might be harmed by disclosure.

Section 17 criminalizes intentional and unauthorized communication of special operational information to a foreign entity or to a terrorist group if the person believes, or is reckless as to whether, the information is special operational information.

Section 18 criminalizes communication, or an agreement to communicate information, by a person with security clearance to a foreign entity or a terrorist group of "a type" the government is taking steps to safeguard.

Finally, under the head "economic espionage", section 19 of the Act makes it an offence for a person to, "at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right", communicate a trade secret to another person, group or organization or obtain, retain, alter or destroy a trade secret "to the detriment of" Canada's economic interests, international relations, national defence or national security.[101] None of these expressions are defined.

2. OLD WINE IN A NEW BOTTLE: CRIMINALIZING LEAKAGE IN THE *SECURITY OF INFORMATION ACT*

While the Bill C-36 amendments to the Act introduced in 2001 eliminated the antiquated spying provision in section 3 in favour of the new espionage provisions discussed above, they left intact section 4, criminalizing leakage. As past criticisms cited above suggest, the precise scope of section 4 of the *Security of Information Act* is difficult to discern from the wording of the section itself. In *Keable v. Canada (Attorney-General)*, the Supreme Court held that "Section 4 of the *Official Secrets Act* makes it clear that it is the duty of every person who has in his possession information entrusted in confidence by a government official and subject to the Act, to refrain from communi-

101. The economic espionage offence in s. 19 is constrained in s. 19(3) by certain defences protecting independent development of trade secrets or reverse engineering.

cating it to any unauthorized person."[102] However, the section is much broader in its scope than this interpretation suggests. Appreciating fully the section's breadth—and its ambiguity—requires a full analysis of its content.

(a) Overview

With a few exceptions noted below, section 4 protects "any secret official code word, password, sketch, plan, model, article, note, document or information that relates to or is used in a prohibited place or anything in a prohibited place."[103] An initial interpretation question is whether the adjectives "secret" and "official" extend to all the nouns that follow, or simply to code words and possibly pass words.[104] If the adjectives apply to the full string of nouns in section 4, then the government must prove that the information is both secret and official, and will not secure a conviction where the impugned information is in the public domain or is not classified by the government as secret.[105] While the old English law was apparently interpreted differently, Canadian courts addressing this issue have limited the scope of the Act, holding that the terms "secret" and "official" apply to all the listed sorts of information.[106] Thus, in *Toronto Sun*, the courts took the view that an accused could not be convicted under the *Official Secrets Act* unless the information at issue was "secret."[107]

The actual offences created by section 4 can be divided into four broad classes: first, offences that criminalize inadequate care of secret information; second, provisions that criminalize communication or malicious use of secret information; third, sections that criminalize receipt and retention of secret information; and, fourth, provisions that depart from the secrecy thrust of the section and apparently criminalize disclosure of even non-secret information.

(b) Inadequate Care of Secret Information

Under the first category, subsection 4(1) criminalizes poor supervision of secret information by persons possessing it. Thus, it is an offence for a per-

---

102. [1979] 1 S.C.R. 218 at 250-51, 90 D.L.R. (3d) 161 [*Keable* cited to S.C.R.].
103. Under the Act, "prohibited place" means "any work of defence" owned or occupied by the government, including such things as arsenals, ships, factories, dockyards and the like. Further, a "prohibited place" may also include a privately owned establishment used to store, manufacture or repair any "munitions of war." Finally, the government may itself designate prohibited places where information relating to such a place "would be useful to a foreign power".
104. See Mackenzie Commission, *supra* note 90 at para. 204 ("In fact there is sufficient inconsistency in the Act for there to have arisen in Canada a question as to whether the words 'secret' or 'official' qualify only 'code word', or 'code word or pass word' or (more importantly) also the words 'sketch, plan, model, article, or note, or other document or information'").
105. *Ibid.*
106. Law Reform Commission of Canada, *supra* note 91 at 34 (noting that the 1972 UK Franks Committee "concluded that the English Act has much wider application, with the words 'secret and official' only qualifying 'code word or password,' and not the other items listed.").
107. *Supra* note 87 at 632–33.

son in possession of secret information to fail "to take reasonable care of," or to "endanger the safety of," the secret information.

(c) Communication of Secret Information

Second, with respect to communication of secret information, paragraph 4(4)(b) criminalizes communication of any secret official code word or password issued for exclusive use of the communicator. The broader paragraph 4(1)(a) renders it an offence for a person to communicate secret information "to any person, other than a person to whom he is authorized to communicate with, or a person to whom it is in the interest of the State his duty [*sic*] to communicate it" and also renders it an offence to "use" the information "for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the State."[108] For its part, subsection 4(2) carves out a special offence for those who possess secret information concerning a munition of war and who communicate it to "any foreign power" or "in any other manner prejudicial to the safety or interests of the State."

(d) Receipt of Secret Information

Third, with respect to receipt of secret information, subsection 4(3) makes it an offence for a person to receive secret information while "knowing, or having reasonable ground to believe, at the time he receives it," that the secret information is communicated to him or her in contravention of the Act. This person is guilty of an offence in such circumstances "unless he proves" that the communication was "contrary to his desire." Meanwhile, subsection 4(1) renders it a crime to retain secret information in the absence of a "right to retain it or when it is contrary to [the receiving person's] duty to retain it or [he or she] fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof".

(e) Disclosure or Receipt of Non-Secret but Official Information

Last, section 4 also includes a number of provisions criminalizing disclosure and receipt of even non-secret, but official, information. Thus, certain aspects of paragraph 4(4)(b) appear to make it a crime for someone authorized to have exclusive possession of an "official document" to provide that document to someone else.

---

108. Unlike in the old *Official Secrets Act*, the terms "foreign power" and "prejudicial to the safety and interests of the State" are both defined in the *Security of Information Act*. Thus, pursuant to s. 2, "foreign power" includes a foreign state, a *de facto* foreign government or a foreign political party whose purpose is to assume the role of that state's government. Section 3 defines prejudice to state safety and interests as including commission of certain criminal offences designed, for instance, to benefit a foreign entity or terrorist group, terrorism, causing an urgent or critical situation in Canada endangering the safety of Canadians or undermining the government's ability to preserve its sovereignty, interruption of essential services, and assorted other threats to what can broadly be labelled national security.

Other parts of paragraph 4(4)(b) make it a crime to have possession "without lawful authority or excuse" of "any official document...issued for the use of a person other than himself." Further, it is an offence "on obtaining possession of any official document by finding or otherwise," to fail to "restore it to the person or authority by whom or for whose use it was issued, or to a police constable."

For its part, paragraph 4(4)(a) of the Act apparently also abandons the requirement that a document be secret by rendering it a crime for a person to retain "for any purpose prejudicial to the safety or interests of the State" an "official document, whether or not completed or issued for use, when he has no right to retain it, or when it is contrary to his duty to retain it" or in contravention of instructions from the government to return or dispose of it.

(f) Discussion

Given this discussion, the breadth of section 4 is obviously staggering. Indeed, communication of information is criminalized in a fashion likely to render most civil service "whistleblowing" a crime. As the Law Reform Commission noted in 1986, the then-*Official Secrets Act* "always treats the loquacious public servant and the secret agent alike: both may be charged under the same section (section 4), the punishment is the same, and, more importantly, the terrible stigma of prosecution under the [Act] is identical for both, because the public and the news media are unable to discern whether it is a case of calculated espionage or careless retention of documents."[109]

Further, and stunningly, non-authorized possession of even non-secret, but official government documents is a crime. So broadly crafted is section 4 that is difficult to imagine the government would, for example, fail to secure convictions for the almost daily "leaks" of written government information that fill newspaper pages. More than that, it seems likely that they would secure the conviction of the journalist and newspaper reporting these leaks.

The historical absence of prosecutions brought under section 4 likely reflects an appreciation of the political consequences of such aggressive uses of secrecy law. Nevertheless, in the current, security-sensitized environment, self-imposed political restraints appear less forceful. Thus, in January 2004, the RCMP raided *Ottawa Citizen* reporter Juliet O'Neill's home and office looking for leaked information pertaining to Maher Arar, the Canadian deported by US officials to Jordan and then incarcerated (and tortured) in Syria. The warrant alleged a violation by Ms O'Neill of subsections 4(1)(a), 4(3) and 4(4)(b) of the *Security of Information Act*.[110]

---

109. *Supra* note 91 at 37.

110. Gowling LaFleur Henderson LLP, "Media Advisory: Juliet O'Neill and CanWest Attack Unconstitutional Search and Seizure" (28 January 2004), online: CanWest Advisory <http://www.gowlings.com/resources/pdfs/CanwestAdvisory.pdf>; See also "Notice of Application and Constitutional Issue" (11 February 2004) at para. 4, online: Notice of Application <http://www.gowlings.com/resources/pdfs/NoticeOfApplication4.pdf>.

That case has now sparked a constitutional challenge to section 4.[111] Specifically, Ms O'Neill and the *Ottawa Citizen* contend that paragraph 4(1)(a), subsection 4(3) and subsection 4(4)(b) violate subsection 2(b) of the *Charter* by infringing on the freedom of the press to gather and disseminate information of public interest and concern, and violate section 7 of the *Charter* on the basis of vagueness and overbreadth. Further, subsection 4(3) is said to create a reverse onus provision in violation of the presumption of innocence set out in subsection 11(d) of the *Charter*, and also criminalizes conduct on the basis of a standard of "reasonable ground to believe," in violation of section 7 fundamental justice.

This case is now proceeding. However, to its credit the government has acknowledged the shortcomings of section 4. Liberal MP Andy Scott has indicated that

> [t]he Government of Canada recognizes that Section 4, which was largely not amended under the new Security of Information Act, needs to be reviewed and modernized.... While there is scope for the courts to interpret section 4 properly, it is appropriate for Parliament to have the opportunity to consider many of the policy issues section 4 raises, such as what information should be protected and in what circumstances should disclosure be justified in the public interest.[112]

In January 2004, the government announced a review of section 4.[113] By the time of this writing in early Fall 2004, this review had not commenced, and it remains to be seen how the government will proceed.

2) National Security Exemptions under the Access Act

The *Security of Information Act* is not the only statute deterring release of national security information. Indeed, the *Access to Information Act* itself curbs such releases.

i. Key Provisions

Thus, section 16 of the Act allows the government to refuse release of requested records less than 20 years old containing information prepared by a government investigative body in the course of lawful investigations of activities, *inter alia*, suspected of constituting "threats to the security of

111. *Ibid.*

112. The Honourable Andy Scott, "Topical Issues," online: Andy Scott-Fredericton MP-Hot topics <http://www.andyscott.parl.gc.ca/hottopics/review.htm>.

113. Office of the Deputy Prime Minister, News Release, "Deputy Prime Minister Announces Public Inquiry into the Maher Arar Matter" (28 January 2004), online: <http://www.psepc-sppcc.gc.ca/publications/news/20040128-3_e.asp>.

Canada" within the meaning of the *Canadian Security Intelligence Service Act*.[114] Section 16 contains a number of other potential national security provisions, such as information that could facilitate an offence, including in relation to critical infrastructure, and information the disclosure of which could be injurious to law enforcement.

Meanwhile, under section 15—an exception whose *Privacy Act* equivalent the Supreme Court of Canada has labelled a "national security"[115] exemption—the government may refuse to disclose any record requested under the Act "that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities."[116]

While "international affairs" is not defined, the term "defence of Canada or any state allied or associated with Canada" is limited to efforts by Canada and foreign states "toward the detection, prevention or suppression of activities of any foreign state directed toward actual or potential attack or other acts of aggression against Canada or any state allied or associated with Canada."[117] Meanwhile, the expression "subversive or hostile activities" is also carefully delimited.[118]

Other national security-like exemptions in the *Access Act* include "information the disclosure of which could reasonably be expected to threaten the safety of individuals" (section 17). Also notable is the section 13 exemptions for information (including intelligence information) obtained in confidence from other countries.

---

114. R.S.C. 1985, c. C-23. Section 2 of the Act defines "threats to the security of Canada" as: "(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage, (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person, (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada". Obviously, each of these categories of national security threat is broad and vague, and thus capable of expansive definition. On the other hand, much like the *Johannesburg Principles*, this definition constrains the potential for abuse, not least because of a caveat to the definition that expressly excludes "lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to" above.
115. *Ruby*, *supra* note 58 at para. 5.
116. *Access Act*, s. 15. See also *Privacy Act*, *supra* note 25 at s. 21.
117. *Access Act*, s. 15(2).
118. *Ibid.* The expression means: "espionage against Canada or any state allied or associated with Canada,...sabotage,...activities directed toward the commission of terrorist acts, including hijacking, in or against Canada or foreign states,...activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means,...activities directed toward gathering information used for intelligence purposes that relates to Canada or any state allied or associated with Canada, and...activities directed toward threatening the safety of Canadians, employees of the Government of Canada or property of the Government of Canada outside Canada."

ii. Government Performance

Read together, these provisions provide government with substantial power to shield national security secrets from the effects of the *Access Act*. In 2002–03, the section 16 law enforcement exemption ranked as the fourth most frequently employed exemption under the Act, used in 8.6% of all cases in which exemptions were invoked. The section15 international affairs and defence exception followed as the fifth most common exemption, at 7%. The section 13 information obtained in confidence exemption ranked sixth, at 5.1%. Finally, the section 17 harm to others justification was used very infrequently, in only 0.3% of instances.

No statistics are publicly available assessing the number of complaints made by exemption, or whether the use of these exemptions was proper. Thus, it is impossible to assess whether these national security exceptions are being employed reasonably. The Information Commissioner has, however, commented adversely on the performance of national security agencies under the *Access Act*, noting "Canadians continue to complain about excessive secrecy on the part of government institutions which play a role in ensuring public safety."[119] In the Commissioner's words:

> The *Access to Information Act* was intended to move us beyond a form of government accountability based solely on trusting the word and good faith of public officials. While trust in our public officials is important, and usually deserved, the *Access Act* allows us to verify that our trust is well-placed. This important role of openness in our society is not given adequate weight by our public officials who are involved in security-related work.[120]

That being said, the limited data available does not suggest any particular abuse at present of the *Access Act* exemptions by agencies with national security responsibilities. As noted above, the number of meritorious complaints relating to the use of all exemptions as a proportion of total requests was 2.6%, government-wide, in 2002–03.[121] The performance of agencies with some national security functions for which data were available was mixed, but generally not far off this average.

Thus, the number of meritorious complaints filed with the Information Commissioner as a proportion of total requests was low at Citizenship and Immigration Canada, at 0.75%, but high at the Department of Foreign Affairs and International Trade, at 5.67%. Other agencies with national security responsibilities for which data were available fell in-between 4% for the RCMP, 3.8% at National Defence, 2.09% at Canada

---

119. Information Commissioner, *Annual Report 2002–2003* (Ottawa: Minister of Public Works and Government Services, 2003) at 26, online: Office of the Information Commissioner: Annual Reports <http://www.infocom.gc.ca/reports/section_display-e.asp?intSectionId=339> at Chapter 1, Part D.

120. *Ibid.*

121. See *supra* note 73, and accompanying text.

Customs and Revenue Agency, and 1.87% at Transport Canada.[122]

It is also notable that the security and intelligence community itself apparently has few quibbles with the scope of the *Access Act* exemptions. In an August 2001 study prepared for the government's Access to Information Review Task Force, security and intelligence specialist Wesley Wark reported that "[b]oth the Canadian Security and Intelligence Service and the Communications Security Establishment, the two main collectors of sensitive intelligence in the community, regard the *Access Act* as offering sufficient protection."[123] Indeed, given the breadth of these exemptions, Wark labels access to contemporary intelligence records under the Act "a fiction" and concludes that "[t]he current Access exemptions provide powerful and sufficient tools" for protecting intelligence information.[124]

3) Canada Evidence Act

Notwithstanding the breadth of existing Canadian secrecy law and exemptions from Canada's access statute, the government moved to enhance its power to keep information secret in Bill C-36, the government's 2001 anti-terrorism law. Specifically, since Bill C-36, the *Canada Evidence Act*[125] now has a central place in government secrecy law.

i. Key Provisions

While primarily a law setting out important evidentiary rules for "proceedings,"[126] the Act contains special rules limiting access to certain sensitive information during these proceedings. Thus, the statute defines "potentially injurious information" as "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security". "Sensitive information," meanwhile, "means information relating to international relations or national defence or national security" that the Government of Canada is "taking measures to safeguard."[127] These terms are not defined in greater detail.

Participants in a civil or criminal proceeding must notify the federal

---

122. *Ibid.* at 50 ("resolved" column in "Complaints finding by government institution" table); Treasury Board, *InfoSource 2002–2003*, online: InfoSource Bulletin 2003–Privacy Act and Access to Information Act <http://www.infosource.gc.ca/bulletin/2003/bulletin03_e.asp> ("Institutions ranked in 'Most Requests Received' order" table). Percentage = resolved/requests x 100%.

123. Wesley Wark, "The Access To Information Act and the Security and Intelligence Community in Canada" *Report 20–Access to Information Review Task Force* (August 2001), online: Government of Canada's Access to Information Review Task Force <http://www.atirtf-geai.gc.ca/paper-intelligence2-e.html>.

124. *Ibid.*

125. *Supra* note 12 at s. 38.

126. *Ibid.*, s. 38. A "proceeding" "means a proceeding before a court, person or body with jurisdiction to compel the production of information".

127. S. 38.

Attorney General when they intend (or believe another participant or person intends) to disclose these classes of information. The Attorney General may then authorize disclosure, or alternatively, may deny this authorization, in which case the matter is taken up by the Federal Court. Under section 38.06, the court authorizes disclosure unless persuaded that disclosure would be injurious to international relations, national defence or national security. Even where disclosure would be injurious, the information may still be released if the public interest in disclosure exceeds the injury.[128]

However, section 38.13 of the *Canada Evidence Act* empowers the Attorney General to personally issue a certificate "in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security."[129]

The expressions "national defence" and "national security" are not defined. Moreover, there is an important ambiguity in this provision. Should it be read as relating to information obtained from a "foreign entity" in confidence or from that entity for the purpose of protecting national defence or security? If so, then the certificate may only issue for information with a foreign origin. Alternatively, should the section cover information obtained in confidence from a foreign entity, *and* also information obtained to protect national defence or security, regardless of its origins? At least some Parliamentarians thought that the provision had the latter, broader meaning.[130]

Notably, the Minister may only issue the certificate in response to an order or decision requiring the disclosure of that information under any federal statute. However, issuance of the certificate has the effect of barring any subsequent disclosure of the information in a proceeding. In other words, the certificate may reverse an order from the Federal Court authorizing disclosure under section 38.06.

ii. Interaction with the Access Act

The certificate may also bar disclosure under the *Access to Information Act*. Indeed, amendments introduced to the *Access to Information Act* in Bill C-36 give certificates clear primacy over the right to access by establishing a new exclusion. Thus, new section 69.1 specifies that the *Access Act* "does not

---

128. S. 38.06.

129. S. 38.13.

130. See *e.g.* Senator Bryden and Senator Joyal, describing the provision as having two purposes: first, protection of confidential foreign information and second, protection of national defence and national security information. The Special Senate Committee On Bill C-36, *Evidence*, (6 December 2001), online: Parliament of Canada <http://www.parl.gc.ca/37/1/parlbus/commbus/senate/com-e/sm36-e/38483-e.htm>.

apply" to information covered by a *Canada Evidence Act* certificate issued before an access complaint is filed with the Information Commissioner.[131] At first blush, this appears to permit the government to stamp information as "top secret" and to use a certificate to remove, *ab initio*, that information from the carefully tailored balance of access and exceptions set out in the *Access Act* regime.

This drastic result appears to be ruled out, at least in part, by the requirement in section 38.13 of the *Canada Evidence Act* that the certificate only be issued in response to an order or decision requiring disclosure. In defending C-36, the government argued that since the Information Commissioner has no power to "order" or make a decision "requiring" disclosure, in theory, a certificate should only be issued once a Federal Court has ordered disclosure on judicial review under the *Access Act*.[132]

However, as correctly noted by the Information Commissioner, the Commissioner does have power under the *Access Act* to order disclosure to the Office of the Information Commissioner itself, in the course of investigating an access complaint.[133] Thus, it is now "open to the Attorney General to issue a secrecy certificate for the purpose of resisting an order made by the Information Commissioner requiring that records be provided to him" or her.[134]

Indeed, this seems to be the exact intent of the Bill C-36 amendment to the *Access Act*. Subsection 69.1(2) of the *Access Act* indicates that a certificate "discontinues" "all proceedings under this Act in respect of the complaint, including an investigation, appeal or judicial review."[135] Since an "investigation" under the *Access Act* is undertaken by the Information Commissioner, this section anticipates a certificate being issued to circumscribe the Commissioner's powers precisely in the fashion feared. Indeed, the government has tried to bar disclosure to the Information Commissioner using the *Canada Evidence Act* in the past.[136]

The breadth of subsection 69.1(2) also exceeds that strictly necessary to bring the *Access Act* into conformity with the amended *Canada Evidence Act*.

---

131. *Access Act*, s. 69.1(1).

132. *Annual Report Information Commissioner 2001-2002* (Ottawa: Minister of Public Works and Government Services Canada, 2001) at 19, online: Office of the Information Commissioner of Canada <http://www.infocom.gc.ca/reports/section_display-e.asp?intSectionId=179> (citing then-Minister of Justice McClellan, "the certificate could only be issued after the judicial review of an access or privacy request") [Information Commissioner Report].

133. *Access Act*, s. 36.

134. *Ibid.*

135. *Ibid.*, s. 69.1(2).

136. See *e.g. Canada (Attorney General) v. Canada (Information Commissioner)*, [2002] 3 F.C. 606 at para. 9, 18 C.P.R. (4th) 925 (F.C.T.D.) ("Three of the applications were brought by the Information Commissioner for orders in the nature of *certiorari* quashing Certificates issued pursuant to ss. 37 and 38 of the *Canada Evidence Act*, pursuant to which certain information and documents...were not provided to the Information Commissioner.").

While the *Canada Evidence Act* precludes the specific information covered in a certificate from being disclosed in a proceeding, the new *Access Act* provision discontinues all proceedings in respect to the "complaint".

In critiquing this language, the Information Commissioner noted that access requests are typically on a subject matter, rather than individual government record, basis. Various exemptions on access may apply to assorted records falling within this subject matter. In response to a complaint concerning non-disclosure, the Commissioner reviews the use of each exemption in relation to *each* record. Under new subsection 69.1(2), the application of a certificate to a single record covered in an access complaint discontinues "all proceedings" in respect of the *complaint*, not simply proceedings in relation to that single record. The Information Commissioner summarizes the impact of this language as follows: "The federal government has given itself the legal tools to stop in its tracks any independent review of denials of access under the *Access to Information Act*. The interference is not even limited to the information covered by the secrecy certificates,"[137] as it also captures all other information raised in the complaint.

The Information Commissioner also views the new amendments as an unnecessary over-reaction: "the *Access to Information Act* posed no risk of possible disclosure of sensitive intelligence information,...no such information had ever been disclosed under the Act in the 18 years of its life and...the *Access to Information Act* régime offered as much or more secrecy to intelligence information as do the laws of our allies."[138] As noted above, this conclusion is supported, at least in part, by Professor Wesley Wark's assessment of national security protection under the regular *Access Act* exemptions.

In a mild response to criticisms sparked by its changes, the government introduced in Bill C-36 an appeal mechanism for certificate determinations under the *Canada Evidence Act*. Thus, the Minister's certificate decision may be challenged before a single judge of the Federal Court of Appeal. The role of this judge is simply to determine that the information covered by the certificate relates to the permissible grounds for issuing a certificate, in which case the judge must confirm the certificate.[139] The Information Commissioner, in his review of this appeal mechanism, called it "woefully inadequate." In his words:

> The reviewing judge is not permitted by this amendment to conduct any of the usual types of judicial review of an administrative decision (*de novo*, legality, correctness); rather the reviewing judge's sole authority is to review the information covered by the certificate for the purpose of deciding whether or not it "relates to":

---

137. Information Commissioner Report, *supra* note 132 at 16.

138. *Ibid.* at 20. For an academic critique of the amendments, see Patricia McMahon, "Amending the Access to Information Act: Does National Security Require the Proposed Amendments of Bill C-36" (2002) 60 U.T. Fac. L. Rev. 89.

139. *Supra* note 12, s. 38.131.

> 1. information disclosed in confidence from, or in relation to, a foreign entity;
> 2. national defence; or
> 3. security.
>
> One would be hard pressed to imagine any operational information held by any of our investigative, defence, security, intelligence, immigration or foreign affairs institutions, which would not "relate to" one or more of these three broad categories.... This form of judicial review is significantly less rigorous than the independent review of secrecy certificates available in our major allied countries. This form of review has been aptly termed "window dressing" because it does not subject the Attorney General to any meaningful accountability for the use of certificates.[140]

To this criticism might be added the observation that the expressions "national defence" and "security" are undefined, rendering it very difficult for a judge to second-guess the executive branch.

4) Extraneous Secrecy Provisions in Other Statutes

Layered onto the secrecy regime created by the key statutes discussed above is a potpourri of other federal laws restricting access to government information for reasons of national security. Strangely, none of these laws are referenced in Schedule II of the *Access Act*. They are therefore not covered independently by the exemption in section 24 of the *Access Act*, barring disclosure of information "restricted by or pursuant to any provision set out in Schedule II."

For instance, pursuant to the *Corrections and Conditional Release Act*, the Correctional Investigator, or his or her delegate, may disclose information required for his or her investigation, but may not disclose "information obtained or prepared in the course of lawful investigations pertaining to...activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* [*CSIS Act*],...if the information came into existence less than twenty years before the anticipated disclosure."[141]

For its part, the *Official Languages Act* instructs the Commissioner of Official Languages to "avoid disclosing any matter the disclosure of which would or might be prejudicial to the defence or security of Canada or any state allied or associated with Canada" in his or her annual report to Parliament.[142] The expression "defence or security of Canada" is not defined.

Under the *Expropriation Act*, where land is expropriated for "a purpose related to the safety or security of Canada or a state allied or associated with Canada" and the public interest so demands, the government need not pro-

---

140. Information Commissioner Report, *supra* note 132 at 20.
141. S.C. 1992, c. 20, s. 183.
142. R.S.C. 1985, (4th Supp.), c. 31, s. 68.

vide specifics on this purpose in its notice of intent to expropriate.[143] Again, "safety or security of Canada" is not defined.

Under the *Canadian Human Rights Act*,[144] members of the Human Rights Commission receiving information in the course of their investigations are to "take every reasonable precaution to avoid disclosing any matter the disclosure of which...might be injurious to international relations, national defence or security or federal-provincial relations." Similarly, they are to guard against disclosing "information obtained or prepared by any investigative body of the Government of Canada...in relation to national security." The expressions "national security" or its similes are not defined.

III. Assessing Canada's Secrecy Law Complex

AS THIS ARTICLE IS COMPLETED, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar is conducting hearings behind closed doors, reviewing documents the government claims must be kept secret. Commission counsel Paul Cavalluzzo recently described the process of vetting these documents as "unbelievably complicated."[145]

Without a doubt, the Arar inquiry is grappling in their deliberations with many of Canada's secrecy laws discussed above. As that analysis suggests, and as Mr Cavalluzzo's comments intimate, these statutes weave a vast, complex, convoluted, and at times, unintelligible web. No consistent understanding of what should or should not be secret runs through the statute book.

A. THE THOUGHTFUL *ACCESS ACT*

The most thoughtful law is the *Access Act*. The national security exceptions in this statute are fairly precisely defined, creating intelligible standards and not simply invoking "national security" or "secret" or some other murky concept. In many instances, the Act includes an injury requirement, precluding disclosure only where there is some deleterious impact on a usually defined national security interest associated with the release of information.

Moreover, all the national security exemptions are discretionary, importing into government decision-making on disclosure an implicit balancing of interests rather than imposing a strict non-disclosure requirement. In this respect, therefore, the Act's national security exemptions are more or less consistent with the international "best practices" standards cited above: they are clearly and narrowly drawn and subject to harm and at least

143. R.S.C. 1985, c. E-21, s. 5.
144. R.S.C. 1985, c. H-6, s. 33.
145. Kate Jaimet "Arar inquiry stalled by 'unbelievably complicated' secrecy rules" *The Ottawa Citizen* (15 July 2004) A.1.

an implicit public interest test. Moreover, the sorts of national security interests captured by the exceptions are in keeping with a reasonable interpretation of Article 19(3) of the *International Covenant on Civil and Political Rights*, and the *Johannesburg Principles*.

B. THE OVERBROAD *CANADA EVIDENCE ACT*

Unfortunately, the relative clarity of the *Access Act* is not matched by the Bill C-36 changes to the *Canada Evidence Act*. First, as the discussion above makes evident, section 38 of the *Canada Evidence Act* creates three different classes of information: potentially injurious information, defined as "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security;" sensitive information, defined as "information relating to international relations or national defence or national security" that the government is safeguarding; and, in the context of certificates, "information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security."

The first concept—potentially injurious information—is generally consistent with the injury-based exemption in the *Access Act*. However, the other two concepts are significantly broader and very uncertain as to their precise scope.

Second, while the *Canada Evidence Act* provisions anticipate adjudication of government national security claims and expressly enable the Federal Court to consider the public interest, this process may be short-circuited by the issuance of a certificate. This certificate quashes not only any decision by a Federal Court judge to order release under the *Canada Evidence Act*, but also may be employed to quash proceedings under the *Access Act* itself.

The added government secrecy muscle that the *Canada Evidence Act* grafts onto the *Access Act* is particularly troubling, given the failure to define carefully the national security grounds justifying the issuance of a certificate. In other words, the careful attention to detail and balancing found in the *Access Act* is entirely circumvented by a *Canada Evidence Act* provision that provides minimal guidance on when governments are empowered to issue certificates.

In light of evidence suggesting that the regular *Access Act* exemptions were doing their job in protecting legitimate national security interests, the Bill C-36 amendments are clear overkill. They also have the effect of bumping the *Access Act* regime out of alignment with the "best practices" standards noted above. The national security grounds are no longer so narrowly prescribed and the new exclusion in section 69.1 is not subject to either a harm test or a public interest override.

C. A MIXED BAG OF OTHER LAWS

Compounding this problem are the assorted secrecy provisions in other statutes that use language similar in some respects to the national security exceptions in the *Access Act*. To the extent the language in these statutes vary from that in the *Access Act*, a prospect arises that information not covered by an *Access Act* exemption will be covered by the secrecy provisions in one of these other statutes. This raises a question as to whether an agency can comply with both the *Access Act* and the other secrecy exclusion that may apply to it. The simple answer is that the *Access Act* obligation should prevail. Section 4 of the *Access Act* provides that the right to access exists "notwithstanding any other Act of Parliament."[146] In practical terms, however, the existence of multiple secrecy provisions limiting access outside of the *Access Act* sends confusing signals to the civil servants subject to these provisions, and likely clouds disclosure decision-making for risk-adverse government bureaucrats.

D. THE BIG STICK OF A SWEEPING *SECURITY OF INFORMATION ACT*

Indeed, in the face of uncertainty, these officials have reason to be wary and to err on the side of limiting disclosure, given the *Security of Information Act*. Under section 4 of that Act, unauthorized disclosure of even non-secret but "official" government documents brings with it the possibility of criminal prosecutions. Where the document is "secret" within the (undefined) meaning of the Act, the prospect of being found criminally culpable multiplies, including potentially when the document is shared internally within the government itself.

Further, since the Act extends to "persons" and not just civil servants, and because it criminalizes receipt as much as disclosure, it makes leaked government information a "hot potato" that most risk-adverse people would rather not receive. The net effect cannot be other than to chill the sharing of information, even when a clear public interest in disclosure and dissemination may exist.

Ironically, the Bill C-36 amendments to the *Security of Information Act* at least nominally impose a less demanding set of secrecy requirements on "persons permanently bound by secrecy" than they do the regular civil servants and general members of the public captured by section 4. First, these persons bound by secrecy are liable for unauthorized disclosure of "special operational information," a much more carefully defined concept than the throw-away reference to "secret official" information in section 4. Second, these persons are entitled to a public interest defence for their unauthorized disclosure.

---

146. See also *Canada Post Corporation v. Canada (Minister of Public Works)*, [1995] 2 F.C. 110 at 129, 20 Admin. L.R. (2d) 242 (F.C.A.) ("subsection 4(1) contains a 'notwithstanding clause' which gives the Act an overriding status with respect to any other Act of Parliament.").

Of course, members of the government's security and intelligence community probably should take little solace from these more carefully drafted sections. They are, after all, still "persons," and thus are captured by section 4 of the Act as much as any other individual. The overbreadth of section 4, in other words, makes a mockery of the careful drafting in the newer sections of the law, including the public interest override.

All told, therefore, the *Security of Information Act* is so overbroad as to be deeply inconsistent with both the *Charter* and Article 19 of the *International Covenant on Civil and Political Rights*. Specifically, the Act criminalizes access to information and, arguably, speech and freedom of the press, without paying any attention to whether these constraints comport with Article 19(3)'s justification for limitations on these rights or the various rights contained in sections 2, 7 and 11(d) of the *Charter*.

The section also fails miserably when measured against Principle 15 of the *Johannesburg Principles*. Specifically, criminalization of disclosure in section 4 exists even in the absence of damage stemming from the disclosure. Further, the section lacks any sort of public interest override.

In an era where Canada is anxious about its international credentials in the security and intelligence community, it is also worth noting that the *Security of Information Act* compares unfavourably to its closest equivalent, the UK *Official Secrets Act of 1989*.[147] Certainly, in some respects, this UK law is less measured than its Canadian counterpart. Thus, the 1989 UK Act does include provisions covering the security services, and broadly equivalent to the Canadian statute's "persons permanently bound by secrecy" sections. Here, the UK Act is more unforgiving, imposing a blanket prohibition on unauthorized disclosure of "any information, document or other article relating to security or intelligence" in the person's possession by virtue of his or her security services employ.[148] There is no requirement that damage stem from the disclosure. Further, unlike the Canadian law, no public interest exception exists. The sole defence anticipated by the Act is if the person did not know of the security or intelligence nature of the information.[149]

Yet, in so far as its other "leakage" provisions are concerned, the UK Act is much more moderate (and intelligible) than section 4 of the *Security of Information Act*. Thus the 1989 Act makes it an offence, in section 1, for civil servants to disclose information relating to security or intelligence, but only if this disclosure is damaging. This damage is measured by any actual damage

147. 1989 c. 6 [UK *Official Secrets Act*], online: Her Majesty's Stationery Service <http://www.hmso.gov.uk/acts/acts1989/Ukpga_19890006_en_2.htm#mdiv1>; for a full discussion of the UK Act, see John Wadham and Kavita Modi, "National security and open government in the United Kingdom," *National Security and Open Government: Striking the Right Balance* (Syracuse: Campbell Public Affairs Institute, 2003), online: Campbell Public Affairs Institute <http://www.maxwell.syr.edu/campbell/opengov/>.

148. UK *Official Secrets Act*, *ibid.*, s. 1(1).

149. *Ibid.* s. 1(5).

it causes to "the work of, or of any part of, the security and intelligence services." Alternatively, that civil servant is liable if the information is of the sort that disclosure is "likely to cause such damage."[150] Ignorance of the security and intelligence nature of the information is a defence, as is the reasonable absence of belief that disclosure would be damaging.

Parallel provisions regulating disclosure of information relating to "defence" and to "international relations" are contained in sections 2 and 3 of the Act. The concepts of "defence" and "international relations" are both defined. Further, in both sections the disclosure is only an offence if it causes damage, a concept spelled out in detail in each instance. A lack of knowledge of (or reasonable belief as to) the subject-matter nature of the information is again a defence.

The Act also creates other offences for secondary leaking of secrets by recipients of wrongfully leaked documents. Thus, a person who receives a document relating to defence or international relations commits an offence under section 5 if they subsequently disclose it, knowing or having reasonable cause to believe, that the information is protected by section 2 or 3. However, this subsequent disclosure must itself be damaging and the person must know, or have reasonable cause to believe, the disclosure to be damaging.

Thus, unlike the draconian section 4 of the *Security of Information Act*, the UK *Official Secrets Act* carefully defines the sorts of information captured by the criminalization of disclosure. Again, unlike the Canadian law, it also layers on a requirement that disclosure of even this sensitive information be "damaging" (within the meaning of the Act) before criminal culpability will attach. While there is no public interest override, these requirements are much more consistent with the *Johannesburg Principles* than is the Canadian statute.

Conclusion: Quick Fixes for Canada's Secrecy Laws

IN SUM, Canada's information and secrecy laws deserve a failing grade. Read together, they are inconsistent with international standards and best practices. In their criminal dimension, they are more restrictive than the secrecy laws of a least one key ally, the United Kingdom. Further, past commentary from the security and intelligence community itself suggests that their breadth is more than is necessary to protect legitimate national security secrets. At the same time, their incoherence—and the uncertainty it produces—create conditions likely to curb information exchanges that could actually enhance national security. Finally, the limits they impose on information access—and the draconian penalties they level in some instances—are deeply inconsistent with the very democratic society they are supposed to

150. *Ibid.* s. 1(4).

protect. They are broad enough to let government sidestep embarrassment and mask incompetence, all in the name of national security.

Correcting these deficiencies is not an overwhelming task. Three simple fixes would go a long way in rebalancing the secrecy law regime. First, the government should repeal section 4 of the *Security of Information Act*—the recent provisions relating to persons bound by secrecy cover-off leakage from the intelligence services. What remains, with the repeal of section 4, would be the drafting of a more measured provision covering other civil servants and persons receiving protected information. In this respect, the new law could follow the precedent of the UK *Official Secrets Act* by defining extremely carefully and narrowly, the sorts of secrets covered by criminal provisions, and by introducing a prerequisite that damage, as defined by the Act, stem from disclosure. The amended *Security of Information Act* could then apply the existing public interest override currently applicable to persons bound by secrecy.

Second, the government should standardize its definition of national security across the statute book. Currently, exemptions from disclosure on national security grounds are conveyed by a confusing array of terms, including "international affairs, national defence and national security," "national security," "security of Canada," "Canadian interests," "information that is of a type that the Government of Canada is taking measures to safeguard" and the like.

It makes sense, as a first step, to harmonize what the government means by national security. To a certain extent, the government has already done this haphazardly with the term "security of Canada" in the *CSIS Act*. Employing this definition in lieu of other, undefined references to "national security" or its similes in the Canadian statute book would have two salutary effects. First, it would provide a necessary metre stick against which to measure the legitimacy of national security justifications in the many statutes that lack a definition of the term. Second, it would standardize and centralize the understanding of national security throughout Canadian federal law. Debate could then focus on the adequacy of this standardized and centralized definition, and not be distracted by questions of whether national security might be approached differently in the other, sometimes obscure circumstances in which statutes invoke it.

It is true, however, that the concept of "security of Canada" defining the mandate of CSIS may not always overlap with the classes of information that the government seeks legitimately to protect on national security grounds. Special definitions of national security secrets will also have to be articulated. For instance, the *Security of Information Act* has attempted to provide a definition of national security secrets with its concept of "special operational information". The *Access Act*, meanwhile, has comprehensive definitions for its national security exemptions. Lining up these two sources of

definitions of national security secrets, and then using this reconciliation to contribute greater certainty to the invocation of international relations, defence and national security in the *Canada Evidence Act*, will require some modest redrafting.

In this respect, section15 of the *Access Act* is the logical nexus point for a common understanding of national security secrets. First, its use of the expression "international affairs" should be defined. A starting point might be the UK *Official Secrets Act of 1989* which defines international relations as "any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation."[151] Second, the reference to "prevention or suppression of subversive or hostile activities" in subsection15(1) should be replaced with "national security". The section should then define "national security" consistently with the proposed, standard definition in the *CSIS Act*. Finally, section 15 should also capture "special operational information," as defined by the *Security of Information Act*.

The *Canada Evidence Act* should be amended to eliminate its creation of three new and slightly different classes of national security information. Instead, the Act should only apply to "potentially injurious information," defined to mean information as defined in section 15 of the newly amended *Access Act*.

Notably, fixing section 15 as the litmus test would incorporate that section's injury test into the *Canada Evidence Act*. Such a change would probably add little to *Canada Evidence Act* section 38.06 determinations. This section already incorporates an injury test and allows a Federal Court judge to contemplate the balance of public interests in reaching a disclosure decision. The proposed amendment would, however, provide greater latitude for a Federal Court of Appeal judge to contemplate the balance of interests in assessing the merits of a ministerial certificate issued under section 38.13 of the Act.

In essence, the amended Act would allow the Minister to certify *Access Act* section 15 information as exempt from the *Access Act*, disallow its use in proceedings, and bring it under the different appeal and review regime established by the *Canada Evidence Act*. These are still extremely potent powers. In the absence of compelling evidence that more is needed, these changes seem more than sufficient to secure legitimate government secrecy. Meanwhile, these changes would reduce the extreme uncertainty created by the proliferation of undefined terms in the current *Canada Evidence Act* and bring that statute back in line with international principles encouraging an injury test.

---

151. *Ibid.* s. 3(5).

Finally, the government should repeal the several secrecy provisions in other statutes that interact with the national security exemptions in the *Access Act* in potentially contradictory ways. In those instances where the government believes a special obligation not to disclose sensitive information need be imposed, it should simply standardize the test to be applied by incorporating, by reference, section 15 of the *Access Act*, as amended.

These amendments would not put national security at risk. Disclosure would still be carefully circumscribed by the now even more generous *Access Act* exemptions—exemptions, to repeat, that the Canadian security services saw as sufficient even before the new post-9/11 restrictions. Wrongful leakage of information that raises legitimate national security threats would still be penalized. On the other hand, these changes would simplify and standardize government secrecy law, eliminate much uncertainty as to its scope, and leave good governance in Canada less dependent on benign executive branch interpretations of today's perplexing secrecy laws.

Put another way, these amendments would not produce the feared sinking ships. Instead, these amendments would help remove government secrecy laws as an obstacle to legitimate public scrutiny. To paraphrase the Standing Senate Committee on Defence and National Security, this public pressure could do exactly what secrecy might fail to do: motivate governments to repair the holes that do sink ships.

Appendix: Access Act Exemptions[152]

	CLASS TEST	INJURY TEST
MANDATORY EXEMPTIONS	1. Section 13—Information received in confidence from other governments or an international organization. If body gives disclosure permission (or this body has itself made public the information), the information may be disclosed. 2. Sub-section 16(3)—Information obtained or prepared by the RCMP while performing policing services for a province or municipality 3. Section 19—Personal information as defined in section 3 of the Privacy Act. If disclosure permission has been obtained, the information is publicly available, or the information may be disclosed under the Privacy Act, the information may be disclosed. 4. Paragraph 20(1)(a)—Trade secrets of a third party 5. Paragraph 20(1)(b)—Financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party, subject to a public interest override 6. Section 24—Information protected under other, listed statutes	1. Paragraph 20(1)(c)—Information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party, subject to a public interest override 2. Paragraph 20(1)(d)—Information the disclosure of which could reasonably be expected to interfere with contractual or other negotiations of a third party, subject to a public interest override
DISCRETIONARY EXEMPTIONS	1. Paragraph 16(1)(a)—Information obtained or prepared by listed investigative bodies pertaining to crime prevention, law enforcement or threats to the security of Canada, if less than 20 years old 2. Paragraph 16(1)(b)—Information on techniques or plans for specific lawful investigations 3. Paragraph 18(a)—Trade secrets or financial, commercial, scientific or technical information that belongs to the Government of Canada or a government institution and has substantial value or is reasonably likely to have substantial value 4. Paragraph 21(1)(a)—Advice or recommendations developed by or for a government institution or a minister of the Crown 5. Paragraph 21(1)(b)—An account of consultations or deliberations involving officers or employees of a government institution, a minister of the Crown or the staff of a minister of	1. Section 14—Injury to the conduct of federal-provincial affairs, including federal strategy or information on federal-provincial consultations or negotiations 2. Section 15—Injury to the conduct of international affairs or to the defence of Canada or an allied state, or the prevention or suppression of subversive or hostile activities 3. Sub-section 16(1)(c)—Injury to law enforcement or to the conduct of lawful investigations, including information on confidential sources 4. Sub-section 16(2)—Information that could reasonably be expected to facilitate the commission of an offence, including information that is technical information relating to weapons or potential weapons; or on the vulnerability of particular buildings or other structures or systems 5. Section 17—Information the disclosure of which could reasonably be

152. Adopted from Access to Information Review Task Force, *supra* note 61 at 41.

the Crown
6. Paragraph 21(1)(c)—Positions or plans developed for the purpose of negotiations carried on or to be carried on by or on behalf of the Government of Canada and considerations relating thereto
7. Paragraph 21(1)(d)—Plans relating to the management of personnel or the administration of a government institution that have not yet been put into operation, if the record came into existence less than twenty years prior to the request
8. Section 23—Information that is subject to solicitor-client privilege
9. Section 26—Information will be published by the government within ninety days

expected to threaten the safety of individuals
6. Paragraph 18(b)—Information the disclosure of which could reasonably be expected to prejudice the competitive position of a government institution
7. Paragraph 18(c)—Scientific or technical information obtained through research by an officer or employee of a government institution, the disclosure of which could reasonably be expected to deprive the officer or employee of priority of publication
8. Paragraph 18(d)—Information the disclosure of which could reasonably be expected to be materially injurious to the financial interests of the government or its ability to manage the economy or could reasonably be expected to result in an undue benefit to any person
9. Section 22—Information relating to testing or auditing procedures or techniques or details of specific tests to be given or audits to be conducted if the disclosure would prejudice the use or results of particular tests or audits