Osgoode Hall Law Journal

Volume 48, Number 2 (Summer 2010)

Article 2

National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits

Steven Penney

National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits

Abstract
The communications surveillance powers granted to Canada's national security agencies have rarely resulted in prosecution and, as a result, have been subject to very little judicial, academic, or public scrutiny. However, as the state increasingly seeks to prosecute alleged terrorists, courts will have to interpret the scope of these powers and decide whether they violate section 8 of the Canadian Charter of Rights and Freedoms (the Charter). A review of the powers granted to police, the Canadian Security Intelligence Service (CSIS), and the Communications Security Establishment Canada (CSEC) reveals two constitutional infirmities: allowing police to conduct communications surveillance in terrorism investigations without establishing "investigative necessity," and allowing CSEC to intercept domestic communications without prior judicial authorization. Put simply, these powers should be found to violate section 8 of the Charter because they substantially infringe on the privacy of innocent Canadians, especially of Muslim or Arab background, while doing little to advance national security.

Keywords
Electronic surveillance--Law and legislation; Terrorism--Prevention--Law and legislation; Civil rights; Privacy; Right of; National security--Law and legislation; Canada. Canadian Charter of Rights and Freedoms. Section 8; Canada

National Security Surveillance in an Age of Terror: Statutory Powers & *Charter* Limits

STEVEN PENNEY*

The communications surveillance powers granted to Canada's national security agencies have rarely resulted in prosecution and, as a result, have been subject to very little judicial, academic, or public scrutiny. However, as the state increasingly seeks to prosecute alleged terrorists, courts will have to interpret the scope of these powers and decide whether they violate section 8 of the *Canadian Charter of Rights and Freedoms* (the *Charter*). A review of the powers granted to police, the Canadian Security Intelligence Service (CSIS), and the Communications Security Establishment Canada (CSEC) reveals two constitutional infirmities: allowing police to conduct communications surveillance in terrorism investigations without establishing "investigative necessity," and allowing CSEC to intercept domestic communications without prior judicial authorization. Put simply, these powers should be found to violate section 8 of the *Charter* because they substantially infringe on the privacy of innocent Canadians, especially of Muslim or Arab background, while doing little to advance national security.

Alors que les pouvoirs de surveillance des communications accordés aux organismes de sécurité nationale du Canada ont rarement entraîné des poursuites, ils ont fait l'objet de fort peu d'examens judiciaires, universitaires ou publics. Toutefois, à mesure que l'État cherche de plus en plus à poursuivre de prétendus terroristes, les tribunaux devront interpréter la portée de ces pouvoirs et décider si l'un d'entre eux enfreint l'article 8 de la *Charte canadienne des droits et libertés* (la *Charte*). Un examen des pouvoirs accordés aux services de police, au Service canadien du renseignement de sécurité (SCRS) et au Centre de la sécurité des télécommunications Canada (CSTC) révèle deux déficiences constitutionnelles, notamment de permettre à la police de procéder à la surveillance des communications lors d'enquêtes sur le terrorisme sans établir la « nécessité de tenir une enquête », et de permettre au CSTC d'intercepter des communications nationales sans autorisation judiciaire préalable. Plus simplement, on devrait trouver que ces pouvoirs contreviennent à l'article 8 de la *Charte*, étant donné qu'ils portent considérablement atteinte à la protection des renseignements personnels de Canadiens innocents (plus particulièrement de ceux d'ascendance

* Steven Penney, Faculty of Law, University of Alberta. The author wishes to thank Julia Herscovitch for her research assistance.

musulmane ou arabe), tout en accomplissant fort peu pour ce qui est de faire progresser la sécurité nationale.

I. POLICE 253
A. Context and Legislation 253
B. Constitutionality 258

II. CSIS 268
A. Context and Legislation 268
B. Constitutionality 271

III. CSEC 275
A. Context and legislation 275
B. Constitutionality 279

IV. CONCLUSION 285

IN RESPONSE TO recent terrorist attacks, many nations have passed laws broadening the surveillance capacities of law enforcement and national security agencies.[1] Some have argued that these laws unduly diminish the liberty, privacy, and equality interests of non-terrorists, especially those who innocently share racial, ethnic, religious, or ideological affiliations with terrorist groups.[2] Some of these laws have also been challenged for violating constitutional rights.[3]

To date, Canada has experienced little of this controversy. Like many other countries, Canada introduced a raft of legislative changes in the aftermath of 11 September 2001 (9/11), including enhancements to terrorism-related surveillance powers.[4] But challenges to counter-terrorism laws have thus far centred on other issues, such as immigration procedures[5] and the definition of terrorist offences.[6]

1. See *e.g. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (United States); *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23 (United Kingdom); and *Telecommunications Interception Legislation Amendment Act 2002* (Cth.) (Australia).
2. See *e.g.* Jack M. Balkin, "The Constitution in the National Surveillance State" (2009) 93 Minn. L. Rev. 1; Kent Roach, "The Role and Capacities of Courts and Legislatures in Reviewing Canada's Anti-Terrorism Law" (2008) 24 Windsor Rev. Legal Soc. Issues 5.
3. See *e.g. Mayfield v. U.S.*, 599 F.3d 964 (9th Cir. 2010), petition for cert. filed, 79 USLW 3018 (22 June 2010).
4. See *Anti-terrorism Act*, S.C. 2001, c. 41 [*Anti-terrorism Act*].
5. See *Charkaoui v. Canada (Citizenship and Immigration)*, [2007] 1 S.C.R. 350 [*Charkaoui*].

The reason for this is simple: before 9/11, Canada's national security agencies already had broad surveillance powers. But as the use of these powers rarely resulted in prosecution, they have been subjected to very little judicial, academic, or public scrutiny.[7]

This may be changing. As the state increasingly seeks to prosecute alleged terrorists,[8] courts will have to interpret the scope of these powers and decide whether any of them violate section 8 of the *Canadian Charter of Rights and Freedoms*, which grants everyone "the right to be secure against unreasonable search or seizure."[9]

This simple and concise right has undergone extensive judicial elaboration. The baseline rules, however, were set out by the Supreme Court of Canada in *Hunter et al. v. Southam Inc.*[10] At the broadest level of generality, section 8 requires courts to balance our interest in being free of state-sponsored privacy invasions against our interest in using such invasions to combat threats to the public good.[11] Somewhat more precisely, the Court in *Hunter* directed that the former interest should generally prevail over the latter, unless an arbiter independent of the state's law enforcement apparatus (such as a judge) authorizes

---

6. See *R. v. Khawaja* (2006), 214 C.C.C. (3d) 399 (Ont. Sup. Ct. J.), leave to appeal to S.C.C. refused, (2007) 233 O.A.C. 395 [*Khawaja* 2006].

7. Most national security prosecutions have been for contraventions of the *Official Secrets Act*, now the *Security of Information Act*, R.S.C. 1985, c. O-5. Befitting the Cold War era, this legislation was directed at offences of subversion or diplomatic impropriety. See Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Policy Review, *The RCMP and National Security: A Background Paper to the Commission's Consultation Paper* (Ottawa: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2004) at 8-9, 33-34 [Arar Inquiry, *RCMP and National Security*].

8. See *e.g.* Isabel Teotonio, "Was teen a terrorist or just troubled?" *Toronto Star* (3 July 2008) A18 (wiretap evidence presented in terrorism trial); Kent Roach, "The Toronto Terrorism Arrests" (2006) 51 Crim. L.Q. 389; and Anthony Depalma, "Terror Arrests Reveal Reach of Canada's Surveillance Powers" *The New York Times* (8 June 2006) A12, online: <http://www.nytimes.com/2006/06/08/world/americas/08canada.html>.

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

10. [1984] 2 S.C.R. 145 [*Hunter*].

11. *Ibid.* at 159-60. See also Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J. Crim. L. & Criminology 477 at 479 [Penney, "Reasonable Expectations"].

the invasion *ex ante* on the basis that there are "reasonable and probable grounds ... to believe that an offence has been committed and that there is evidence to be found at the place of the search."[12] In other words, privacy invasions meeting both of these conditions, which I refer to as "prior authorization" and "reasonable grounds," are prima facie reasonable under section 8; invasions that do not are prima facie unreasonable.[13]

The Court has recognized many exceptions to these requirements. Occasionally, privacy interests may be so strong that prior authorization and reasonable grounds are not enough on their own to make an intrusion reasonable.[14] Most relevant here, the Court has stated (in *obiter*) that state agents may also have to show that there is "no other reasonable alternative method of investigation"[15] before obtaining an authorization to intercept electronic communications. This is known as the "investigative necessity" requirement.[16]

More frequently, intrusions have been found to be reasonable without compliance with the requirements laid out in *Hunter*, especially outside the domain of criminal law enforcement.[17] State agents may thus sometimes conduct searches

---

12. *Hunter*, *supra* note 10 at 168. This assumes that the person alleging a s. 8 violation had a "reasonable expectation of privacy" in the circumstances. Absent such an expectation, there is no "search or seizure" and hence no violation of s. 8. See *Hunter* at 159; *R. v. Dyment*, [1988] 2 S.C.R. 417 at 426 (state surveillance of electronic communications content (whether voice or text) clearly invades a reasonable expectation of privacy). See *R. v. Duarte*, [1990] 1 S.C.R. 30 at para. 18 [*Duarte*]; *R. v. Wiggins*, [1990] 1 S.C.R. 62; *R. v. Thompson*, [1990] 2 S.C.R. 1111 at para. 35 [*Thompson*]; *R. v. Weir*, [1998] 8 W.W.R. 228 at paras. 70-77 (Alta. Q.B.), aff'd (2001), 156 C.C.C. (3d) 188 (Alta. C.A.); and Robert W. Hubbard, Peter DeFreitas & Susan Magotiaux, "The Internet – Expectations of Privacy in a New Context" (2002) 45 Crim. L.Q. 170 at 196-97.

13. *Hunter*, *ibid.*

14. See *Lavallee, Rackel & Heintz v. Canada (Attorney General)*; *White, Ottenheimer & Baker v. Canada (Attorney General)*; *R. v. Fink*, [2002] 3 S.C.R. 209 [*Lavallee*] (special conditions always required for searches of lawyers' offices); *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1991] 3 S.C.R. 459 [*Canadian Broadcasting Corp.*] (special conditions sometimes required for searches of journalistic materials); and *Thompson*, *supra* note 12 (special conditions required for wiretapping public payphone to minimize invasion of non-suspects' privacy).

15. *R. v. Araujo*, [2000] 2 S.C.R. 992 at paras. 24, 29 [*Araujo* 2000]. See also *Duarte*, *supra* note 12 at para. 24.

16. See generally *Araujo* 2000, *ibid.*

17. See *e.g. Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425; *R. v. McKinlay Transport Ltd.*, [1990] 1

without prior authorization as well as searches based on standards lower than reasonable grounds.[18] Most relevant here, the Court has hinted, without elaborating, that the reasonable grounds requirement might have to be modified in the context of national security.[19]

For national security surveillance, the Court's section 8 jurisprudence thus pulls in opposing directions. On the one hand, it suggests that, since communications surveillance is such a grave and pernicious threat to privacy, it should not be used unless truly necessary. On the other, the jurisprudence reflects the concern that since terrorism is such a grave and diffuse threat to security, we should not condition national security surveillance on reasonable grounds.

Fortunately, it is not as difficult to reconcile these principles as it may appear. As parliament, courts, and legal theorists have long recognized, communications surveillance is exceptionally intrusive and ought not to be conducted in the absence of investigative necessity, whether in the context of national security or that of conventional policing. Investigative necessity is not especially onerous, and it serves as a real check on abusive surveillance. Without it, communications surveillance should not be considered "reasonable" under section 8 of the *Charter*.

At the same time, the Court has been right to imply that strict adherence to the reasonable grounds requirement from *Hunter* may not always be feasible in national security matters. National security surveillance efforts are typically

---

S.C.R. 627 (taxation); *R. v. Fitzpatrick*, [1995] 4 S.C.R. 154 at paras. 49-51 (fisheries); *British Columbia Securities Commission v. Branch*, [1995] 2 S.C.R. 3 at paras. 51-64 (securities); *Comité paritaire de l'industrie de la chemise v. Potash; Comité paritaire de l'industrie de la chemise v. Selection Milton*, [1994] 2 S.C.R. 406 (employment standards); *Weatherall v. Canada (Attorney General)*, [1993] 2 S.C.R. 872 (prison discipline); *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393 (school discipline); *R. v. Simmons*, [1988] 2 S.C.R. 495 [*Simmons*] (border security); *R. v. Monney*, [1999] 1 S.C.R. 652 [*Monney*] (same); and *R. v. Jacques*, [1996] 3 S.C.R. 312 [*Jacques*] (same).

18. Deviations from *Hunter* have also been recognized in the criminal context, typically where courts have found that suspects' reasonable expectations of privacy are diminished by arrest, detention, or the nature of the implicated privacy interest. See *e.g. Cloutier v. Langlois*, [1990] 1 S.C.R. 158 (search incident to arrest); *R. v. Mann*, [2004] 3 S.C.R. 59 (search incident to detention); *R. v. Kang-Brown*, [2008] 1 S.C.R. 456 [*Kang-Brown*]; and *R. v. A.M.*, [2008] 1 S.C.R. 569 (canine sniff search).

19. *Hunter*, *supra* note 10 at 168 ("[w]here the state's interest is not simply law enforcement as, for-instance, where state security is involved ... the relevant standard might well be a different one").

less targeted and more preventative than conventional criminal investigations. Advances in communications technology have also complicated the application of the reasonable grounds standard to national security surveillance. As a consequence; national security agencies should not have to demonstrate that the proposed surveillance will reveal evidence that a particular suspect has committed an offence. That said, the exigencies of national security do not justify the elision of prior authorization. Without it, the edifice of protection against abusive surveillance crumbles.

I elaborate these arguments with reference to the communications surveillance powers available to the three entities responsible for national security in Canada: (1) the police, including the Royal Canadian Mounted Police (RCMP), (2) the Canadian Security Intelligence Service (CSIS), and (3) the Communications Security Establishment Canada (CSEC). This examination reveals two constitutional infirmities: allowing police to conduct communications surveillance in terrorism investigations without establishing investigative necessity and allowing CSEC to intercept domestic communications without prior judicial authorization. Put simply, these powers should be found to violate section 8 of the *Charter* because they infringe substantially on the privacy of innocent Canadians, especially those of Muslim or Arab background, while doing little to advance national security. Perhaps not surprisingly, both powers were enacted hastily in response to the same notorious terrorist act: 9/11.

The departures from the *Hunter* decision's reasonable grounds requirement, which are found in the communications surveillance provisions applying to CSIS and CSEC, in contrast, should not be found to violate section 8. These provisions condition surveillance on the basis that it will provide either evidence of threats to national security (in the case of CSIS) or foreign intelligence essential to international affairs, defence, or security (in the case of CSEC). Given these agencies' proactive, intelligence-gathering mandates, the nature and magnitude of terrorist threats, and other privacy protections included in the relevant legislation, these requirements achieve a sensible balance between privacy and security.

I. POLICE

A. CONTEXT AND LEGISLATION

As the categories of national security offences and criminal offences overlap, police have long investigated national security threats.[20] The exercise of police powers, however, does not typically turn on any distinction between national security and criminal matters. One exception is the electronic communications surveillance power set out in part VI of the *Criminal Code* (the *Code*).[21] Though this power may be used in relation to a wide variety of offences, post-9/11 amendments have made it easier to use it in terrorism cases than in ordinary criminal cases.[22]

Communications surveillance in national security investigations is typically conducted by the RCMP. However, RCMP agents work closely with other law enforcement and national security agencies, and information is shared freely among them.[23] The focus here, then, is on the powers themselves, and not on the officials who exercise them.

Subject to several exceptions, part VI of the *Code* prohibits and provides criminal punishments for the electronic interception of private, domestic com-

---

20. For histories of police involvement in national security, see Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 5-35; Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law: Second Report*, vol. 1 (Ottawa: Supply and Services Canada, 1981) at 149-58 (Chair, D.C. McDonald) [McDonald Commission]; Canadian Committee on Corrections, *Towards Unity: Criminal Justice and Corrections* (Ottawa: Queen's Printer, 1969) at 83-86 (Chair: Roger Ouimet); and Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [Arar Inquiry, *New Review Mechanism*].

21. R.S.C. 1985, c. C-46. [*Criminal Code*].

22. See *infra* notes 47-52 and accompanying text.

23. See Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 7-8, 16-18, 30-32, 56-76. For examinations of provincial, federal, and international law governing national security information sharing, see Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis Butterworths, 2005) at 117-25, 391 [Cohen, *Privacy, Crime and Terror*]; Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008) at 439-43, 491-95. See also *Privacy Act*, R.S.C. 1985, c. P-21, ss. 8(2), 18; *Privacy Regulations*, S.O.R./83-508.

munications.[24] To be covered by this prohibition, a communication must be both "intercepted"[25] and attract a "reasonable expectation of privacy."[26] There are unresolved interpretive questions relating to each of these requirements,[27] but the basic scope of the prohibition is well understood. Absent an exception, it is a crime for any person, including a state agent, to use technological means to prospectively capture the content of both oral and electronic text communications. This includes the real-time interception of wire-line and wireless telephone conversations, as well as e-mail and other electronic text.[28]

Part VI also applies to (but does not criminalize) the observation "by means of a television camera or other similar electronic device ... [of] ... any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy."[29] It does not likely apply, in contrast, to the retrospective acquisition of stored communications, which may thus be obtained using ordinary search warrants.[30]

As mentioned, these prohibitions are subject to several exceptions, the most important of which permits police to obtain an interception authoriza-

---

24. *Criminal Code*, *supra* note 21, s. 184(1). Section 193 also makes it an offence to use or disclose intercepted private communications for any purpose not related to law enforcement or the operation of communications networks.

25. See *ibid.*, s. 184(1). This section states that anyone "who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years."

26. See *ibid.*, s. 183. This section defines "private communication" as

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

27. See Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Can. Crim. L. Rev. 115 [Penney, "Updating Canada's Communications Surveillance Laws"].

28. See *ibid.* at 118-26.

29. *Criminal Code*, *supra* note 21, ss. 487.01(4)-(5).

30. Penney, "Updating Canada's Communications Surveillance Laws," *supra* note 27 at 126-29.

tion from a judge.[31] The requirements for obtaining such an authorization are more onerous than those applying to ordinary search warrants.[32] For both ordinary search warrants and authorizations under part VI, police must show that they have reasonable and probable grounds[33] to believe that the interception will provide evidence of an offence.[34] And in both cases, evidence obtained in violation of this or any other statutory requirement may be excluded at trial under section 24(2) of the *Charter*.[35] But unlike ordinary warrants, part VI authorizations may be obtained only from superior court judges[36] and only to fur-

---

31. See *Criminal Code*, *supra* note 21, s. 184(2)(b). See also generally Robert W. Hubbard, Peter M. Brauti & Scott K. Fenton, *Wiretapping and Other Electronic Surveillance: Law and Procedure*, looseleaf (Aurora: Canada Law Book Inc., 2005) at § 2.2.2.

32. There are a number of such provisions in the *Criminal Code* and other statutes. The most frequently used is s. 487 of the *Code*, which permits searches of a "building, receptacle, or place." *Supra* note 21.

33. "Reasonable and probable grounds" is equivalent to "reasonable grounds," "probable grounds," "reasonable and probable cause," and "probable cause." See generally *Hunter*, *supra* note 10 at 167 ("[t]he state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion"); *Kang-Brown*, *supra* note 18 at paras. 10, 13, LeBel J., and 24, 75, Binnie J. Courts have not consistently articulated a precise or quantifiable definition of the standard. Some courts have treated it as equivalent to "more likely than not," but others have suggested that it signifies a lesser degree of probability. See R.E. Salhany, *Canadian Criminal Procedure*, 6th ed., looseleaf (Aurora: Canada Law Book, 2005) § 3.1140.

34. The *Criminal Code* does not explicitly require police to establish reasonable and probable grounds. Section 186(1)(a) does oblige the judge issuing the warrant to be satisfied that "it would be in the best interests of the administration of justice to do so." *Supra* note 21. This provision has been interpreted as requiring police to establish "reasonable and probable grounds to believe that an offence has been or is being committed and that the authorization sought will afford evidence of that offence." *Duarte*, *supra* note 12 at para. 24. See also *Araujo* 2000, *supra* note 15; *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1444 [*Garofoli*].

35. In most cases, failing to conform to the requirements of part VI of the *Code* constitutes a violation of s. 8 of the *Charter*. See *Thompson*, *supra* note 12.

36. Most ordinary warrants, including those available under s. 487 of the *Criminal Code*, may be granted by provincially-appointed judges. Superior court judges are appointed by the federal government. However, the requirement that only superior court judges may grant part VI authorizations does not apply in Quebec, where such authorizations may be granted by the provincially-appointed judges of the Court of Quebec. See *Criminal Code*, *supra* note 21, ss. 185(1), 552.

ther the investigation of certain listed offences.[37] In addition, the application for the authorization must include the written consent of the responsible minister or his or her designate.[38]

The most important difference between an ordinary warrant and an authorization allowed under part VI, however, is that only the latter (generally) requires police to demonstrate investigative necessity, *i.e.*, "that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed, or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[39] The Supreme Court of Canada has interpreted this requirement to mean that, "practically speaking, ... [there must be] ... no other reasonable alternative method of investigation."[40] Interception need not be an investigative method of "last resort."[41] The test can be satisfied by demonstrating that "normal investigative techniques are unlikely to succeed."[42] Nevertheless, the requirement is more rigorous than simply showing that interception would likely be the "most efficacious"[43] way to further the investigation. Such a standard, the courts have held, would "replace a standard of necessity with one of opportunity at the discretion of law enforcement bodies."[44]

---

37. *Ibid.*, ss. 183, 185(1). This list, it should be noted, is very long and includes all terrorism-related offences, including those that may not directly result in violence or harm. See *infra* notes 82-101 and accompanying text.

38. *Ibid.*, s. 185(1).

39. *Ibid.*, s. 186(1)(b). The legislative history of the investigative necessity requirement is recounted in N.J. Whitling, "Wiretapping, Investigative Necessity, and the *Charter*" (2002) 46 Crim. L.Q. 89 at 107-08.

40. *Araujo* 2000, *supra* note 15 at para. 29.

41. *Ibid.* This had been suggested in earlier decisions. See *e.g. Duarte*, *supra* note 12 at para. 46; *R. v. Commisso*, [1983] 2 S.C.R. 121 at 135, Dickson J., dissenting; *Thompson*, *supra* note 12 at para. 92, La Forest J., dissenting; and *R. v. Finlay* (1985), 23 C.C.C. (3d) 48 at 69 (Ont. C.A.), leave to appeal to S.C.C. refused, [1986] 1 S.C.R. ix [*Finlay*].

42. *Araujo* 2000, *ibid.* at para. 29.

43. *Ibid.* at para. 39. This had also been suggested in previous decisions, including that of the court below in *Araujo* 2000. *R. v. Araujo* (1998), 127 C.C.C. (3d) 315 at para. 30 (B.C. C.A.) [*Araujo* 1998]. See also *R. v. Paulson* (1995), 97 C.C.C. (3d) 344 (B.C. C.A.); *R. v. Cheung* (1997), 119 C.C.C. (3d) 507 (B.C. C.A.).

44. *Araujo* 2000, *ibid.* at para. 39.

Investigative necessity can be demonstrated in numerous ways, for example, by showing that alternative methods, such as the use of physical surveillance, informants, undercover agents, and ordinary search warrants, would likely be dangerous or ineffective.[45] Such conditions are often present when investigating "a large-scale crime organization, a close-knit family or a drug conspiracy," where "counter-surveillance methods" are common.[46]

In 1997, in response to a spate of gang violence,[47] parliament removed the investigative necessity requirement for investigations of "criminal organization"[48] offences. In 2001, in response to 9/11, it did the same for "terrorism" offences.[49] Two additional exemptions for criminal organization and terrorism investigations accompanied these amendments. First, the maximum period of interception, subject to renewal, was extended from the ordinary sixty days[50] to one year.[51] Second, investigators wishing to extend the deadline for disclosing the authorization to targets were exempted from the usual requirement to show that their investigation was "continuing."[52]

In summary, police may conduct electronic surveillance of private, domestic communications and activities when they have reasonable grounds to believe that such surveillance will reveal evidence of a broad range of criminal offences, including all terrorism-related offences. If they are investigating suspected terror-

45. *Ibid.* at paras. 41-43.

46. *Ibid.*

47. See Don Stuart, "Time to Recodify Criminal Law and Rise Above Law and Order Expediency: Lessons From the Manitoba Warriors Prosecution" (2000) 28 Man. L.J. 89 at 92.

48. *An Act to amend the Criminal Code (criminal organizations) and to amend other Acts in consequence*, S.C. 1997, c. 23, ss. 4-5. For the definitions of "criminal organization" and "criminal organization offence," see *Criminal Code*, *supra* note 21, ss. 2, 467.1. For criticisms of the breadth of these definitions, see Stuart, *ibid.* To date, constitutional challenges to these definitions have failed. See *R. v. Terezakis* (2007), 223 C.C.C. (3d) 344 (B.C. C.A.) (upholding s. 467.13), leave to appeal to S.C.C. refused, [2007] S.C.C.A. No. 487; *R. v. Lindsay* (2009), 245 C.C.C. (3d) 301 (Ont. C.A.), leave to appeal to S.C.C. refused, [2009] S.C.C.A. No. 540 (upholding ss. 467.1 and 467.12); and *R. v. Smith* (2006) 280 Sask. R. 128 (Q.B.) (upholding ss. 467.1, 467.12, and 467.13).

49. *Anti-terrorism Act*, *supra* note 4, ss. 6.1, 133(8.1). The criminal organization and terrorism exemptions to the investigative necessity requirement are codified by the *Criminal Code*, *ibid.*, ss. 185(1.1), 186(1.1).

50. *Criminal Code*, *ibid.*, ss. 186(4)(e), 186(7).

51. *Ibid.*, s. 186.1.

52. *Ibid.*, s. 196(5).

ists (or other criminal groups), they: (1) do not have to demonstrate investigative necessity ("the investigative necessity exemption"), (2) may be permitted to conduct the surveillance for a longer period of time ("the surveillance period extension"), and (3) will have an easier time justifying delays in informing the targets of the surveillance ("the notice exception").

B. CONSTITUTIONALITY

Before the gang and terrorism amendments, the Supreme Court upheld part VI of the *Code* in the context of section 8 *Charter* challenges.[53] The question here is whether any of the terrorism amendments are likely to alter this conclusion. First consider the surveillance period extension. In theory, the maximum surveillance period is just that—a maximum. The issuing judge must still determine the proper length of the surveillance after considering all of the circumstances.[54] But in practice, the maximum could become the norm, as it has in cases governed by the ordinary time period.[55] Nevertheless, if and when the Court deals with this issue, it is much more likely to stress the importance of critically assessing the justification for a longer time period than it is to strike down the provision.[56]

The Court is also unlikely to strike down the notice exception. Like the surveillance period extension, the notice exception appears to rest on the assumption that terrorism investigations are almost always lengthy. As will be discussed below, the *Code*'s expansive definition of terrorism calls this assumption into question. Even in terrorism cases, however, the judge cannot authorize a delay unless the applicant shows that the "interests of justice" require it.[57] What could such a showing entail, other than demonstrating that notification would compromise an ongoing investigation?[58]

---

53. See *Duarte*, *supra* note 12 at para. 45; *Garofoli*, *supra* note 34 at para. 25.

54. See *R. v. Doiron* (2004), 274 N.B.R. (2d) 120 at para. 48 (Q.B.), aff'd (2007), 315 N.B.R. (2d) 205 (C.A.) [*Doiron*]. Recall as well that authorizations for both exempted and non-exempted offences are renewable in any case. *Criminal Code*, *supra* note 21, s. 186(6).

55. See Hubbard, Brauti & Fenton, *supra* note 31, § 3.7.9.

56. See *Doiron*, *supra* note 54 (upholding the criminal organization time period extension). One court has ruled that so long as one gang or terrorism offence is named in the authorization, the maximum time period is one year, even if other, non-exempted offences are also named. See *R. v. Lam* (2004), 355 A.R. 363 at paras. 5, 43-52 (Q.B.).

57. *Criminal Code*, *supra* note 21, s. 196.

58. See Hubbard, Brauti & Fenton, *supra* note 31, § 3.11.5.1.

The constitutionality of the investigative necessity exemption is more questionable. Though it has not ruled on the question, the Supreme Court has indicated that the sweeping invasion of privacy entailed by electronic surveillance is not justified without investigative necessity. As Justice La Forest stated in *R. v. Duarte*,

> [I]f the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White*, supra, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the State may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.[59]

Put more instrumentally, the legal regulation of electronic surveillance encourages people to communicate more candidly than they otherwise would.[60] As Richard Posner explains, the "principal effect of allowing eavesdropping would not be to make the rest of society more informed about the individual but to make conversations more cumbersome and less effective."[61] Regulation also lessens the need to protect privacy by other means.[62] Without it, people may

---

59. *Duarte*, *supra* note 12 at para. 45. See also Law Reform Commission of Canada, *Electronic Surveillance* (Working Paper 47) (Ottawa: The Commission, 1986) at 31 (describing wiretap authorizations as "a huge electronic vacuum cleaner").

60. See generally Penney, "Reasonable Expectations," *supra* note 11 at 492-93; Richard Posner, "Privacy, Secrecy, and Reputation" (1979) 28 Buff. L. Rev. 1 at 17; Charles J. Hartmann & Stephen M. Renas, "Anglo-American Privacy Law: An Economic Analysis" (1985) 5 Int'l Rev. L. & Econ. 133 at 145; and Anthony Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minn. L. Rev. 349 at 388.

61. Richard Posner, "The Right To Privacy" (1978) 12 Ga. L. Rev. 393 at 403.

62. See David Friedman, "Privacy and Technology" (2000) 17 Soc. Phil. & Pol'y 186 at 192-93; Andrew Song, "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches" (Berkman Center Research Publication No. 2003-04, Harvard Law School, Public Law Working Paper No. 73, 2003) at 15-16, online: <http://papers.

wastefully expend resources to enhance the security of their communications, for example, by using more costly, anonymous communications tools (such as public payphones or prepaid cellphones) instead of less costly, non-anonymous ones (such as registered phones).

Of course, as Justice La Forest recognized in *Duarte*, privacy's benefits must be balanced with its costs to law enforcement.[63] An appropriate balance was achieved, in his view, by the then-existing protections of part VI, including the reasonable grounds, prior authorization, and investigative necessity requirements.[64] Similarly, in *R. v. Araujo*, the leading decision in 2000 defining investigative necessity, Justice LeBel stated for a unanimous Court that

> we must not forget that the text of s. 186(1) represents a type of constitutional compromise. In particular, the investigative necessity requirement embodied in s. 186(1) is *one of the safeguards* that made it possible for this Court to uphold these parts of the *Criminal Code* on constitutional grounds.[65]

As the constitutionality of the investigative necessity exemption was not at issue, this passage is *obiter dicta*.[66] However, it does reflect a consistent theme in the Court's part VI and section 8 jurisprudence: communications surveillance should not occur unless an independent arbiter is satisfied that it is truly necessary to combat serious crime.[67]

---

ssrn.com/abstract=422220>; Amsterdam, *supra* note 60 at 403; and *United States v. Dunn*, 480 U.S. 294 at 319 (1987), Brennan J., dissenting.

63. *Duarte*, *supra* note 12 at para. 24.

64. *Ibid.* at paras. 24-26. See also *Garofoli*, *supra* note 34 at 1444.

65. *Araujo* 2000, *supra* note 15 at para. 26 [emphasis added]. See also *R. v. S.A.B.*, [2003] 2 S.C.R. 678 at para. 53 [*S.A.B.*] (referring, in the context of assessing the constitutionality of the *Criminal Code*'s DNA warrant provisions, to investigative necessity as a "constitutional requirement" for wiretap authorizations).

66. LeBel J. specifically noted that the criminal organization amendment was "not invoked or examined in the case at bar." *Araujo* 2000, *ibid.* at para. 2.

67. Other than electronic surveillance, the Supreme Court has considered whether investigative necessity is constitutionally required in the following contexts. It found that it is always required for searches of potentially privileged material in lawyers' offices (see *Lavallee*, *supra* note 14); sometimes required for searches of media offices (*Canadian Broadcasting Corp.*, *supra* note 14 at 478); *Canadian Broadcasting Corporation v. Lessard*, [1991] 3 S.C.R. 421 at 446); and never required for the taking of bodily samples for identification purposes (*S.A.B.*, *supra* note 65 at paras. 53-54).

No court has yet considered the investigative necessity exemption for terrorism offences. However, despite the Supreme Court's *obiter*, lower courts in other contexts have concluded that investigative necessity is not constitutionally required. The first decision to do so, *R. v. Bordage*,[68] considered the *Code*'s one party consent surveillance provisions. Before 1993, this type of surveillance was unregulated. After the Supreme Court decided that this violated section 8, parliament enacted the authorization process referred to above.[69] It did not, however, include an investigative necessity requirement.

This omission is understandable. Though rightly deserving of section 8 regulation, consent surveillance poses a substantially lesser threat to privacy than third party surveillance. In the former case, one of the parties to the communication (usually an informer or undercover police officer) is aware of the interception. Such schemes are often dangerous and carry a high risk of exposure. Police are unlikely to use them when effective, alternative measures are available. An investigative necessity requirement would thus do little to decrease the frequency of consent surveillance. Third party surveillance, in contrast, is both less dangerous and less likely to be exposed. In the absence of an investigative necessity requirement, it would likely be used more frequently.

Compared to third party surveillance, consent surveillance is also less invasive. In revealing confidences to another, there is always a chance that our confidant will use the information to our detriment, for example by conveying it to police. This risk is magnified when the conversation is overheard (and potentially recorded) by state agents.[70] It is not as great, however, as the risk that the state will intercept and record confidences that have not been betrayed. Third party surveillance renders trust irrelevant—the state may be listening even if we are conversing with a faithful confidant.

Third party surveillance is also more likely than consent surveillance to capture innocent communications.[71] Consent intercepts capture only the con-

---

68. (2000), 146 C.C.C. (3d) 549 (Qc. C.A.). See also *R. v. G.L.*, [2004] O.J. No. 5675 at paras. 86-90 (Sup. Ct.) (QL), *sub nom. R. v. Largie*, [2004] O.T.C. 1193 (holding that while police need not demonstrate investigative necessity in every case, it is a "factor to be considered" in deciding whether to exercise the discretion to issue the authorization).

69. See *An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication* Act, S.C. 1993, c. 40, s. 4; *supra* note 31.

70. See *Duarte*, *supra* note 12 at paras. 27-32.

71. See *Thompson*, *supra* note 12 at paras. 47-49.

versations of a single, named person (along with, of course, the person(s) conversing with that individual).[72] The authorizing judge may also permit only a subset of these conversations to be captured, such as those with named targets, with unnamed persons located at a particular place, or in furtherance of a bona fide investigation.[73] Third party authorizations may include analogous conditions, such as live monitoring[74] and retrospective editing,[75] but they are more costly and thus less likely to be imposed.[76]

The investigative necessity requirement, moreover, is not the only difference between third party and consent surveillance. The less invasive nature of the latter is also evidenced by the fact that applications may be made by the police, instead of agents of the responsible minister. They may be made to provincial court judges as well as superior court judges, obtained in relation to any federal offence, and obtained by tele-warrants.[77]

---

72. See Hubbard, Brauti & Fenton, *supra* note 31, § 3.5.5.2.

73. *Ibid.* Unlike in the United States, in Canada such "minimizing" conditions are not mandatory, except in the case of video monitoring. Instead, judges may impose them when they are "advisable in the public interest." *Criminal Code*, *supra* note 21, ss. 186(4)(*d*), 487.01(4). This decision is discretionary, but in certain circumstances a failure to minimize may constitute a violation of s. 8 of the *Charter*. See *Finlay*, *supra* note 41; *Thompson*, *supra* note 12 at paras. 1143-46; and *Garofoli*, *supra* note 34 at 1468.

74. Such monitoring, which may be effected by either visual or audio observation, is designed to ensure that interception only occurs (or continues) if police confirm that a target is a party to the communication. Audio monitoring conditions may also require the interception to cease after a certain period if there is no indication that relevant matters are being discussed. See *Thompson*, *supra* note 12; Hubbard, Brauti, & Fenton, *supra* note 31, § 4.4-4.4.1.

75. This condition permits the recording of all authorized interceptions, but requires investigators to cease listening to and seal irrelevant portions of the communication. See *e.g. R. v. Steel* (1995), 34 Alta. L.R. (3d) 440 at para. 11 (C.A.), leave to appeal to S.C.C. refused, 187 A.R. 318*n*.

76. See *Finlay*, *supra* note 41 at 75; *R. v. Taylor*, [1998] 1 S.C.R. 26 at para. 18; and Stanley A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (Toronto: Carswell, 1983) at 174.

77. *Criminal Code*, *supra* note 21, ss. 184.2-184.3. It has also been suggested that investigative necessity was not made a prerequisite of consent surveillance because one party to the conversation is by definition a state agent and can relay the information to police, prosecutors, and the court in *viva voce* form. See Hubbard, Brauti, & Fenton, *supra* note 31, § 2.2.5; *R. v. Rosebush* (1992), 77 C.C.C. (3d) 241 (Alta. C.A.), leave to appeal to S.C.C. refused, 78 C.C.C. (3d) vi. On this view, it would be impossible in these circumstances to show that there is "no other reasonable alternative method of investigation."

The consent surveillance cases do not help us decide, therefore, whether section 8 requires investigative necessity for third party criminal organization and terrorism authorizations. To date, the courts have addressed, and upheld, only the criminal organization exemption.[78] The argument in favour of the terrorism exception, however, is likely to be similar. That argument, in short, is that compared to the average, solitary wrongdoer, criminal and terrorist organizations are more sophisticated, impenetrable, and dangerous.[79] In this view, the investigative necessity requirement unduly hampers the ability of police to conduct surveillance of these groups. If organized criminals and terrorists are by definition "hard targets,"[80] a categorical exemption would save resources and prevent unjustified dismissals of authorization applications.

If the exemption were truly limited to sophisticated criminal enterprises, this argument might have some purchase. Who would contest the necessity of electronic surveillance to combat biker gangs, transnational mafias, or Al-Qaeda? As the authors of a leading text on electronic surveillance have written, compared to criminal organization exemptions, "there is even greater justification for more intrusive state conduct and extraordinary police powers when the security of the nation is at risk."[81]

On close inspection, however, we see that the exemptions are not limited to investigations of sophisticated or (especially) dangerous groups. Others have examined the criminal organization exemption,[82] so the focus here is on the exemption for any "terrorism offence,"[83] which, by definition, includes any one of the following:

---

78. *R. v. Doucet* (2003), 18 C.R. (6th) 103 (Qc. Sup. Ct.); *R. v. Pangman* (2000), 147 Man. R. (2d) 93 (Q.B.); and *Doiron, supra* note 54.

79. See *e.g. Doiron, ibid.* at paras. 59-61, 64 (noting the "sophisticated methods" of "criminal organizations").

80. See *House of Commons Debates*, No. 160 (21 April 1997) at 9976 (statement of Minister of Justice, Hon. Alan Rock, that in the context of investigations of criminal organizations, wiretapping is "almost always the last resort" and that police should thus not have to "go through the empty process of establishing it").

81. Hubbard, Brauti & Fenton, *supra* note 31, § 16.2. See also Martin L. Friedland, "Police Powers in Bill C-36" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 269 at 274.

82. See Whitling, *supra* note 39.

83. *Criminal Code, supra* note 21, ss. 185(1.1), 186(1.1).

> (a) an offence under sections 83.02 to 83.04 or 83.18 to 83.23 of the *Criminal Code*;
>
> (b) an indictable federal offence "committed for the benefit of, at the direction of or in association with a terrorist group";
>
> (c) an indictable federal offence which "also constitutes a terrorist activity"; or
>
> (d) conspiracies, attempts, counselling, and being an accessory after the fact in relation any of the above offences.[84]

The offences listed in (a) capture activities far removed from the causing of actual harm. Sections 83.02 through 83.04 prohibit the provision, collection, making available, use, or possession of property or financial or "other" services, knowing that it will be used, at least in part, for terrorist purposes. Sections 83.18 through 83.23 prohibit, *inter alia*, various forms of secondary participation in terrorist offences, including participating in or contributing to "any activity of a terrorist group"; facilitating a terrorist activity; instructing another person to "carry out any activity for the benefit, at the direction of or in association with a terrorist group"; and harbouring or concealing a person who has "carried out a terrorist activity."

Notably, a person may be convicted of participating in or contributing[85] to a terrorist group even if no terrorist activity actually occurs, the person's contribution does not enhance the group's ability to carry out an offence, or the person does not know the specific nature of any terrorist activity that may be carried out.[86] The "instructing" offence may capture general public admonitions to engage in terrorism.[87] Similarly, a person may be convicted of facilitating a terrorist activ-

---

84. *Ibid.*, s. 2.

85. The definition of "participating or contributing" is also very broad and includes "entering or remaining in any country," and "making oneself ... available to facilitate" a terrorist offence. *Ibid.*, s. 83.18(3).

86. *Ibid.*, s. 83.18(2). See also *Khawaja* 2006, *supra* note 6 at para. 39 ("[i]t is unnecessary that an accused be shown to have knowledge of the specific nature of terrorist activity he intends to aid, support, enhance or facilitate, as long as he knows it is terrorist activity in a general way"); *R. v. Khawaja* (2008), 238 C.C.C. (3d) 114 at para. 80 (Ont. Sup. Ct. J.) [*Khawaja* 2008].

87. See Kent Roach, *September 11: Consequences for Canada* (Montreal: McGill-Queen's University Press, 2003) at 44; Forcese, *supra* note 23 at 286-87.

ity even if no such activity was actually foreseen, planned, or carried out, and even if the person did not know that any particular activity was facilitated.[88]

The offences in (b) and (c) hinge on the *Code*'s definition of "terrorist activity."[89] This definition is also expansive and includes any act or omission committed with the intention of intimidating the public with respect to its security, including "economic security,"[90] or "compelling a person, government or ... organization to do or to refrain from doing any act,"[91] and that intentionally creates either a risk to public safety or causes "serious interference with or serious disruption of an essential public service, facility, or system."[92] It also includes any conspiracy, attempt, counselling, or threat to commit any such act or omission, as well as being an accessory after the fact. As noted, all of these offences must be indictable federal crimes. Such crimes include, however, all hybrid offences that the Crown may choose to prosecute by way of summary conviction,[93] including minor offences like mischief,[94] theft under five thousand dollars,[95] and common assault.[96]

By adding various forms of inchoate and secondary liability to the list, category (d) further expands the breadth of activity exempted from the investigative necessity requirement.[97] As discussed, many of the offences in categories (a) to (c) already prohibit acts that may be only dimly, potentially, or indirectly related

---

88. *Criminal Code*, *supra* note 21, s. 83.19. See also *Khawaja* 2008, *supra* note 86 at para. 139.

89. This is because "terrorist group" is defined, *inter alia*, as "an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity." *Criminal Code*, *ibid.*, s. 83.01(1).

90. The inherent vagueness of this phrase is highlighted in Kent Roach, "Terrorism Offences and the *Charter*: A Comment on *R. v. Khawaja*" (2007) 11 Can. Crim. L. Rev. 271 at 283-84 [Roach, "Terrorism Offences"].

91. As Kent Roach has noted, "[I]t is a stretch to define terrorism to include attempts to compel individuals or corporations to act." *Ibid.* at 298.

92. *Criminal Code*, *supra* note 21, s. 83.01(1). An exception is made for "advocacy, protest, dissent or stoppage of work" not intended to endanger public safety. *Ibid.*

93. *Interpretation Act*, R.S.C. 1985, c. I-21, s. 34(1)(*a*).

94. *Criminal Code*, *supra* note 21, s. 430(3).

95. *Ibid.*, s. 334(*b*)

96. *Ibid.*, s. 266.

97. See Maureen Webb, "Essential Liberty or a Little Temporary Safety? The Review of the Canadian *Anti-terrorism Act*" (2006) 51 Crim. L.Q. 53 at 65.

to the causing of serious harm. Coupling these offences with inchoate liability threatens to capture conduct carrying an even more negligible risk of harm.[98]

My point is not to question either the wisdom[99] or constitutionality[100] of these offences. It is simply to show that the investigative necessity exemption applies to a great deal of low-level (or even marginal) criminal activity.[101] Police may thus intercept the communications of unsophisticated suspects who would have been vulnerable to conventional investigative techniques.[102] Without the investigative necessity requirement, such surveillance may be justified solely by reasonable grounds to believe that evidence of one of the designated offences will be uncovered.

The next question, then, is whether the interception of terrorist suspects' communications, when it is not strictly necessary to do so, violates section 8. In my view, it does. Without investigative necessity, there is a substantially greater risk that police will disproportionately and unfairly conduct surveillance of Muslim and Arab Canadians. When an enactment invades privacy in a roughly equitable way or when it disproportionately harms politically powerful segments of society, judges should be reluctant to intervene, even if they dislike it.[103] In such cases, the matter should usually be left to the legislative process to

---

98. See Forcese, *supra* note 23 at 28; Roach, "Terrorism Offences," *supra* note 90 at 284, n. 33. See also *R. v. Déry*, [2006] 2 S.C.R. 669 (refusing to recognize offence of attempted conspiracy).

99. For commentary on these issues, see Forcese, *ibid.* at 263-89; Roach, "Terrorism Offences," *ibid.*; W. Wesley Pue, "The War on Terror: Constitutional Governance in a State of Permanent Warfare?" (2003) 41 Osgoode Hall L.J. 267 at 271-74; David Paciocco, "Constitutional Casualties of September 11: Limiting the Legacy of the *Anti-terrorism* Act" (2002) 16 Sup. Ct. L. Rev. (2d) 185; Webb, *supra* note 97 at 61-69; and Stanley Cohen, "Safeguards in and Justifications for Canada's New *Anti-terrorism Act*" (2002-2003) 14 N.J.C.L. 99 at 119-22.

100. In *Khawaja* 2006, *supra* note 6, the court rejected a variety of constitutional challenges to these provisions, save for striking down the requirement to prove that the act was committed "in whole or in part for a political, religious or ideological purpose, objective or cause." *Criminal Code*, *supra* note 21, s. 83.01(1)(*b*)(i)(A).

101. Note that the terrorist offences definitions in the *Criminal Code* are broader than equivalent definitions in comparable jurisdictions and international instruments. See Table 7.1 in Forcese, *supra* note 23 at 265-66.

102. See Whitling, *supra* note 39 at 118-19.

103. See Orin S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Mich. L. Rev. 801 at 839-58 [Kerr, "The Fourth Amendment and New Technologies"]; Ronald F. Wright, "Parity of Resources for Defense Counsel and the Reach of Public Choice Theory" (2004) 90 Iowa L. Rev. 219 at 254-60;

sort out. Judicial intervention is more justified, in contrast, when the enactment disproportionately harms groups whose interests were unreasonably discounted in that process.[104]

Most innocent Canadians have little reason to fear that police will intercept their electronic communications. Canadians with Muslim or Arab backgrounds may not be as confident.[105] The "profiling"[106] of these groups by national security investigators could have a variety of pernicious effects, including the alienation and radicalization of suspects who are innocent of any criminal or terrorist in-

---

James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers and the *Charter*" (2005) 31 Queen's L.J. 1 at 47-48; Penney, "Reasonable Expectations," *supra* note 11 at 503-05; and William J. Stuntz, "Accountable Policing" (Harvard Public Law Working Paper No. 130, 2006), at 19, 53, online: <http://ssrn.com/abstract=886170>.

104. See John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge: Harvard University Press, 1980) at 172-73; William J. Stuntz, "The Pathological Politics of Criminal Law" (2001) 100 Mich. L. Rev. 505; Donald A. Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse L. Rev. 1079; Richard C. Worf, "The Case for Rational Basis Review of General Suspicionless Searches and Seizures" (2007) 23 Touro L. Rev. 93 at 138-58; and Silas J. Wasserstrom & Louis Michael Seidman, "The Fourth Amendment as Constitutional Theory" (1988) 77 Geo. L.J. 19 at 92-112.

105. For evidence of—and commentary on—the disproportionate targeting of Muslim and Arab Canadians in national security investigations, see Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006) at 355-58 (Commissioner: Dennis R. O'Connor); Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 18-20; *Khawaja* 2006, *supra* note 6 at para. 53; Kent Roach, "Ten Ways to Improve Canadian Anti-Terrorism Law" (2006) 51 Crim. L.Q. 102 at 122-23; and Teem Bahdi, "No Exit: Racial Profiling and Canada's War Against Terrorism" (2003) 41 Osgoode Hall L.J. 293.

106. Canadian courts have increasingly recognized both the phenomenon of discriminatory profiling and the importance of instituting *ex ante* and *ex post* checks on police discretion in combating it. See *e.g. R. v. Golden*, [2001] 3 S.C.R. 369 at para. 85; *R. v. Brown* (2003), 9 C.R. (6th) 240 (Ont. C.A.); and *R. v. Harris* (2007), 225 C.C.C. (3d) 193 at para. 63 (Ont. C.A.). See generally David M. Tanovich, *The Colour of Justice: Policing Race in Canada* (Toronto: Irwin Law, 2006) (reviewing evidence of racial profiling in Canada); Jerry Kang, "Trojan Horses of Race" (2004) 118 Harv. L. Rev. 1489 at 1499-1520 (reviewing experimental psychological and other empirical evidence of the subtlety and pervasiveness of racial stereotyping).

volvement.[107] By ensuring that an exceptionally intrusive police power is only used when there is no reasonable alternative, investigative necessity helps to minimize these harms.

At the same time, requiring police to demonstrate investigative necessity is unlikely to thwart surveillance of truly dangerous targets. Many comparable jurisdictions have imposed investigative necessity as a statutory or super-statutory condition of electronic surveillance without exempting terrorism investigations.[108] And, as discussed in Part II(A), below, CSIS agents must always show investigative necessity to conduct communications surveillance.[109] There is no evidence that this prerequisite has hampered CSIS's efforts to monitor suspected terrorists;[110] it is difficult to see why this would be different in the context of the *Code*.

The courts should thus confirm that communications surveillance is not reasonable under section 8 of the *Charter* without investigative necessity, and accordingly strike down the reference to terrorism offences in sections 185(1.1) and 186(1.1) of the *Code*.

II. CSIS

A. CONTEXT AND LEGISLATION

CSIS was established in 1984[111] in the aftermath of a Royal Commission report detailing abuse and incompetence in the RCMP's national security activities.[112]

---

107. See Tom Tyler, Stephen J. Schulhofer & Aziz R. Huq, "Legitimacy and Deterrence Effects in Counter-Terrorism Policing: A Study of Muslim Americans" (2010) 44 Law & Soc'y Rev. 365; Penney, "Reasonable Expectations," *supra* note 11 at 492-500; Tracey Maclin, "'Black and Blue Encounters' – Some Preliminary Thoughts about Fourth Amendment Seizures: Should Race Matter?" (1991) 26 Val. U. L. Rev. 243; and Ontario Human Rights Commission, *Paying the Price: The Human Cost of Racial Profiling (Inquiry Report)* (Toronto: Ontario Human Rights Commission, 2003), online: <http://www.ohrc.on.ca/en/resources/discussion_consultation/RacialProfileReportEN>.

108. See *e.g. Interception of Communications Act 1985* (U.K.), 1985, c. 56, s. 2(3); *Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2518(1)(c) and (3)(c); and *Klass v. Federal Republic of Germany* (1978) 2 E.H.R.R. 214.

109. See *infra* note 120 and accompanying text.

110. See *e.g.* Michelle Shephard, "Much at Stake in Terror Case" *Toronto Star* (10 June 2006) A14; San Grewal, "CSIS Erased Crucial Tapes; Rivalry Between RCMP, Spy Agency Hobbled Probe Suspect's Phone Tapped Months Before Bombings" *Toronto Star* (17 March 2005) A9.

111. *An Act to establish the Canadian Security Intelligence Service*, S.C. 1984, c. 31 [*CSIS Act*].

CSIS is a civilian entity, and its agents accordingly have no special powers to arrest, lay charges, or use force. Rather, the agency's purpose is to gather and analyze intelligence relating to "threats to the security of Canada."[113] "Threats to the security of Canada" means

> (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, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).[114]

Where there are reasonable grounds to believe that it is necessary to investigate one of these threats, CSIS agents may apply for a judicial warrant author-

---

112. McDonald Commission, *supra* note 20. See also *Atwal v. Canada*, [1988] 1 F.C. 107 at 139-40 (C.A.) [*Atwal*].

113. *CSIS Act*, *supra* note 111, s. 2. This information may be passed on to the RCMP or other police agencies for enforcement purposes. Specifically, s. 17 of the *CSIS Act* permits the agency, on ministerial approval, to "enter into an arrangement or otherwise cooperate" with federal and provincial governments and police agencies. Section 19(2) also specifies that the agency may disclose information "obtained in the performance of its duties and functions" to, *inter alia*, police "where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province." Such disclosures must be reported to the Security Intelligence Review Committee (SIRC). See *infra*, notes 143-47 and accompanying text; *CSIS Act*, s. 19(3). As noted by the Arar Inquiry, "as a result of post 9/11 legislative changes, most, if not all, actions which affect the national security of Canada have been criminalized"; consequently, "virtually all information and intelligence that CSIS would be interested in is potentially also of interest to the RCMP in connection with its national security, crime prevention, and law enforcement mandate." Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 41. See also Cohen, *Privacy, Crime and Terror*, *supra* note 23 at 407-08; *Charkaoui*, *supra* note 5 at para. 27.

114. *CSIS Act*, *ibid.*, s. 2.

izing the interception of "any communication."[115] To this end, its agents may be authorized to "enter any place or open or obtain access to any thing"; "search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing"; and "install, maintain or remove any thing."[116]

In many ways, this regime protects privacy at least as robustly as part VI of the *Code*.[117] For example, warrant applications that are made under the *CSIS Act* must be approved by the responsible minister,[118] made by certain designated officials, and heard by a federally-appointed judge.[119] Most notably, the *CSIS Act* requires applicants to demonstrate investigative necessity for *all* warrants, including the equivalent of ordinary *Code* search warrants.[120] There is no exception for terrorism investigations.

In some respects, however, the *CSIS Act* offers less protection than part VI of the *Code*. There is no requirement to inform targets or report to parliament;[121] CSIS intercepts may last for up to one year[122] (though, as we have seen, this is now also the case for criminal organization and terrorism investigations under part VI), and CSIS warrant applicants do not have to show that an offence has been committed or that evidence is likely to be obtained. There need only be reasonable grounds to believe that the warrant "is required to enable the Service to investigate a threat to the security of Canada or perform its duties and functions under section 16."[123]

---

115. *Ibid.*, ss. 21(1), (3).

116. *Ibid.*, s. 21(3).

117. See *ibid.*, ss. 21(2), (4).

118. *Ibid.*, s. 21(1).

119. *Ibid.*, s. 21. The applicant must be either the director of CSIS or an employee designated by the minister. The judge must be a judge of the Federal Court (Canada) who is designated to hear CSIS warrant applications by the chief justice of that court.

120. *Ibid.*, ss. 21(2)(b), 21(3). This requirement had been recommended by the McDonald Commission, *supra* note 20 at 526, n. 56.

121. See *CSIS Act*, *ibid.*, s. 26 (specifying that part VI of the *Criminal Code* does not apply to authorized CSIS intercepts).

122. In "subversion" investigations (defined in s. 2(d) of the *Act*), a sixty-day maximum applies. Like *Criminal Code* authorizations, *CSIS Act* warrants are renewable. *CSIS Act*, *ibid.*, ss. 21(5), 22.

123. *Ibid.*, s. 21(1).

B. CONSTITUTIONALITY

It is this latter aspect of the *CSIS Act*'s warrant procedure that is constitutionally problematic. On its face, it does not satisfy the Court's directive in *Hunter* that investigators establish reasonable grounds "to believe that an offence has been committed and that there is evidence to be found at the place of the search."[124] As we have seen, however, the Supreme Court has indicated that national security concerns might justify a different standard.[125] The *CSIS Act* does require reasonable grounds,[126] but this requirement is in relation to the belief that surveillance is necessary to investigate national security threats, not in relation to any belief that it is necessary to discover evidence of an offence.

In the only decision to date that has fully considered the question, the Federal Court of Appeal nonetheless concluded that the CSIS warrant provisions complied with section 8 of the *Charter*.[127] Communications surveillance serves different purposes, the court stressed, in the criminal law enforcement and national security contexts. "The *Code* contemplates interception as an investigative tool after or during the event," it reasoned, "while the [*CSIS*] *Act* is directed primarily to gathering information in an attempt to anticipate future occurrences."[128] Consequently, it would be inappropriate, in the latter case, to insist that the issuing judge "be satisfied that an offence has been committed and that evidence thereof will be found in execution of the warrant."[129]

---

124. *Supra* note 10 at 168.

125. *Ibid.*

126. *Supra* note 111, s. 21(1). The specific language used is "reasonable grounds," but as noted, the courts have treated this phrase as having the same meaning as "reasonable and probable grounds" or "probable cause." See *supra* note 33.

127. *Atwal, supra* note 112 at 131-34. See also *Canadian Civil Liberties Assn. v. Canada (Attorney General)*, (1997) 126 C.C.C. (3d) 257 at para. 88 (Ont. C.A.), leave to appeal to SCC refused, [1998] S.C.C.A. No. 487 [*CCLA*] (noting, in denying standing on other grounds, that the applicant's s. 8 arguments were so weak that there was "probably" no serious issue of invalidity).

128. *Atwal, ibid.* at 127.

129. *Ibid.* at 133. In *Atwal*, however, the court did hold that the judge who issued the warrant erred in refusing to disclose the affidavit supporting the warrant to its target, who had applied to that judge under Federal Court Rules to vacate the warrant. According to *Atwal*, such disclosure should generally follow unless the government establishes under applicable evidentiary legislation that the disclosure would be damaging to the national security interest (at 143-44). The government may also be able to assert other forms of statutory and com-

It is difficult to take issue with this analysis. CSIS's main purpose is not to investigate and collect evidence of crime. While other agencies may ultimately use information acquired by CSIS in criminal investigations and prosecutions, CSIS's mandate is to collect "security intelligence," not "criminal intelligence."[130] There is a risk that CSIS could systematically deploy its search and surveillance powers to bolster the somewhat more limited powers available to law enforcement agencies.[131] This risk is best mitigated, however, by independent oversight,[132] not by requiring CSIS to search and conduct surveillance only in relation to discrete, criminal investigations. Doing so would unduly hamper the agency's ability to conduct long-term, proactive, and preventative monitoring of security threats.

The *Act*'s definition of such threats, moreover, is reasonably restrictive. Most terrorism-related investigations would fall within the scope of paragraph (c) of the definition of "threats to the security of Canada." Obtaining a warrant in such cases would require reasonable grounds to believe that the intrusion was necessary to enable the investigation of activities "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."[133] CSIS may only conduct intrusive surveillance, therefore, when it can demonstrate a serious risk of harm.

Atwal was not unanimous. In his dissenting reasons, Justice Hugessen faulted the *CSIS Act* for failing to require any direct connection "between the information it is hoped to obtain from the intercepted communication and the alleged threat to

---

mon law privilege (such as informer or public interest privilege) to prevent disclosure. See *R. v. Malik*, [2002] B.C.J. No. 3219 (S.C.) (QL) (negligent destruction of wiretap recording held to violate disclosure obligation under s. 7 of the *Charter*). See generally *Charkaoui*, *supra* note 5 at paras. 58-61; *Suresh v. Canada (Minister of Citizenship & Immigration)*, [2002] 1 S.C.R. 3 at para. 122; *Ruby v. Canada (Solicitor General)*, [2002] 4 S.C.R. 3 at paras. 43-51; *Canada (Minister of Employment and Immigration) v. Chiarelli*, [1992] 1 S.C.R. 711 at 744; Hubbard, Brauti & Fenton, *supra* note 31, § 12.8.1-4; and *Canada Evidence Act*, R.S.C. 1985, c. C-5, ss. 37-38.16.

130. See Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 26-27.

131. See generally Balkin, *supra* note 2 at 11-12.

132. For a discussion of these mechanisms, see *infra* notes 143-48 and accompanying text.

133. *CSIS Act*, *supra* note 111, s. 2(c) [emphasis added]. Roach, "Terrorism Offences," *supra* note 90 at 295-96.

the security of Canada."[134] All that is needed, in his view, is a connection between the interception and the investigation itself. This would allow CSIS to target innocent people, such as the intended victims of a terrorist attack, or worse, persons who could be compelled to become informants (by threatening to disclose damaging information).[135]

Justice Hugessen's fears are greatly exaggerated. If it is reasonably possible, statutes must be interpreted in a constitutional manner.[136] As discussed, though section 8 does not require mandatory minimization provisions, undue invasions of the privacy of non-suspects may be unreasonable in individual cases.[137] Section 8 also clothes judges with a residual discretion to refuse to issue a warrant, even where the statutory requirements for issuance have been met.[138] In exercising this discretion, judges must weigh the interests of individuals to be "free of intrusions of the state [against those of the state] to intrude on the privacy of the individual for the purpose of law enforcement."[139] In light of these principles, it makes little sense to invalidate a warrant provision because it does not expressly forbid intrusions that would inevitably be found to violate the *Charter*.[140]

The greatest problem with the *CSIS Act*'s investigative powers is not their breadth; rather, it is the secrecy accompanying their exercise. The few reported decisions suggest that authorizing judges take their supervisory role seriously.[141] But as the *Act* contains no notice requirement, and as investigations rarely lead

---

134. *Atwal, supra* note 112 at 151.

135. *Ibid.*

136. See *Slaight Communications Inc. v. Davidson*, [1989] 1 S.C.R. 1038.

137. *Supra* note 73.

138. *Baron v. Canada*, [1993] 1 S.C.R. 416.

139. *Ibid.* at 435.

140. See generally *Application for warrants pursuant to s. 21 of the Canadian Security Intelligence Act* (1997) 10 C.R. (5th) 273 (F.C.T.D.) (stressing the importance of careful judicial scrutiny in assessing CSIS warrant applications).

141. In addition to the cases cited at *supra* note 127, see Canada, Security Intelligence Review Committee, *SIRC Annual Report 2005-2006: An operational review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2007) at 48-49 (noting the dismissal of two applications as well as several instances where the judge requested additional information before issuing the warrant).

to criminal proceedings, it is difficult to know whether the process is working as it should.[142]

To help alleviate this problem, while at the same time accommodating the need for secrecy in national security matters, the *Act* establishes the Security Intelligence Review Committee (SIRC), an independent oversight body.[143] As part of its responsibilities, SIRC investigates and reports on CSIS's use of its warrant powers.[144] Specifically, SIRC reviews a sample of warrants to determine whether the application accurately reflected the information held, the justification for requesting the warrant was reasonable, and CSIS complied with the legal and policy requirements attaching to warrant powers.[145] While some have suggested that CSIS should be subjected to a greater degree of parliamentary oversight,[146] most commentators have concluded that SIRC is effective in holding CSIS accountable.[147] In my view, the combination of this oversight and a rigorous judicial warrant process renders the *CSIS Act* compatible with section 8 of the *Charter*.[148]

---

142. See Hubbard, Brauti & Fenton, *supra* note 31, § 12.3-4. The same problem has been noted with respect to the RCMP's use of its investigative powers in national security investigations, and led to Justice O'Connor's recommendation that the government provide effective monitoring of national security bodies. See Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 33-35.

143. *CSIS Act*, *supra* note 111, ss. 34-55. See generally Murray Rankin, "The Security Intelligence Review Committee: Reconciling National Security with Procedural Fairness" (1990) 3 Can. J. Admin. L. & Pol'y 173 at 177-79. Another oversight mechanism, the office of the CSIS "Inspector General," is charged with monitoring the agency's operational activities. *CSIS Act*, ss. 29-33.

144. See Reg Whitaker, "Designing a Balance Between Freedom and Security" in Joseph F. Fletcher, ed., *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999) 126 at 135. SIRC's annual reports, which contain reviews and statistics on the use of the warrant powers, are available online: <http://www.sirc-csars.gc.ca/anrran/index-eng.html>.

145. See Canada, Security Intelligence Review Committee, *SIRC Annual Report 2006-2007: An operational review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2007) at v, 52-53.

146. See Whitaker, *supra* note 144 at 144-45; Jean-Paul Brodeur, "The Invention of Outsiders: The Relationship between Operatives and Civilian Experts" in Fletcher, *supra* note 144, 150 at 163-64.

147. See Whitaker, *ibid.*; Hubbard, Brauti & Fenton, *supra* note 31, § 12.4.

148. See generally *CCLA*, *supra* note 127 at paras. 14, 73 (taking note of SIRC's role in suggesting that the *Act's* warrant powers likely do not violate the *Charter*).

III. CSEC

A. CONTEXT AND LEGISLATION

CSEC[149] is charged with collecting "signals intelligence."[150] This includes the covert acquisition and processing of foreign electronic communications for the purpose of advancing the nation's interests in defence, security, and international relations.[151] These intercepts are typically "processed through arrays of advanced computer systems programmed to search for specific telephone numbers or internet addresses, voice recognition patterns or key words, and to decrypt text."[152]

CSEC was established in 1975, but predecessor agencies had been capturing and decrypting foreign communications for many decades.[153] Shortly after World War II, a signals intelligence sharing alliance that is still active today was created by the United States, the United Kingdom, Canada, Australia, and New Zealand.[154] CSEC and its immediate predecessor, the Communications Branch of

149. CSEC is a civilian unit of the Department of National Defence. Administrative and financial matters are controlled by the Department; however, policy direction comes from the National Security Advisor, a Deputy Secretary in the Privy Council Office. See Martin Rudner, "Canada's Communications Security Establishment from Cold War to Globalization" (2001) 16 Intelligence & Nat'l Security 97 at 97 [Rudner, "Canada's Communications Security Establishment"].

150. "Signals intelligence" has been defined as "a category of intelligence that includes transmissions associated with communications, radars, and weapons systems." National Security Agency, "Signals Intelligence," online: National Security Agency Central Security Service <http://www.nsa.gov/sigint/index.shtml>.

151. The Canadian military also conducts signals intelligence in support of its operations. It is not authorized to conduct domestic surveillance, except in aid of another agency, in which case its activities are subject to the regulatory regime governing that agency. See Arar Inquiry, *RCMP and National Security*, *supra* note 7 at 72; Forcese, *supra* note 23 at 453.

152. Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism" (2007) 22 Intelligence and Nat'l Security 473 at 474 [Rudner, "Signals Intelligence and Counter-Terrorism"].

153. See Rudner, "Canada's Communications Security Establishment," *supra* note 149 at 99-114.

154. *Ibid.* at 108-09; Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance" in Hayden B. Peake & Samuel Halpern, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (Washington: NIBC Press, 1994) 95. The centrepiece of this alliance is a large-scale, sophisticated computer network enabling the automated processing and sharing of information relevant to each nation's intelligence requirements. See Rudner, "Signals Intelligence and Counter-Terrorism," *supra* note 152 at 111-14, 479-82; Martin Rudner, "The Globalization of Terrorism: Canada's Intelligence Response to the Post-

the National Research Council, participated actively in this alliance, and during the Cold War era, they directed most of their intercepts at the Soviet Bloc.[155] Clothed in secrecy, the government did not formally acknowledge their existence until 1983;[156] they operated without any statutory mandate.[157] They were prohibited, however, from intercepting communications within Canada.[158]

The enactment of the *Anti-terrorism Act* in 2001 changed much of this.[159] CSEC was given a statutory home in a new part of the *National Defence Act*,[160] which defined the agency's mandate to include the acquisition and use of "in-

---

September 11 Threat Environment" *Canadian Issues* (September 2002) 24. It has been reported that the agreement governing the alliance prohibits signatories from targeting each other's territory or nationals. See Rudner, "Canada's Communications Security Establishment," *ibid.* at 479. The CSEC Commissioner has provided assurances that the agency "does not use its partners to circumvent the laws of Canada, nor does it provide partners with communications they could not legally collect for themselves." Canada, Communications Security Establishment Commissioner, *Annual Report: 2000-2001* (Ottawa: Minister of Public Works and Government Services Canada, 2001) at 4.

155. See Rudner, "Canada's Communications Security Establishment," *ibid.* at 99; Philip Rosen, *The Communications Security Establishment: Canada's Most Secret Intelligence Agency*, Parliamentary Research Branch, Background Paper BP-343E (September 1993) at 2-3.

156. See Senate, Special Committee on the Canadian Security Intelligence Service, *Proceedings* (22 September 1983) at 11 (Jean-Luc Pépin). Informal acknowledgments of Canada's participation in the UK/US Agreement were made as early as 1975. See House of Commons, Standing Committee on Miscellaneous Estimates, *Proceedings* (24 March 1975) at 18 (C.M. Drury).

157. Until 2001, Canada's signal intelligence agencies operated under the mandate of a classified order-in-council. See Rudner, "Signals Intelligence and Counter-Terrorism," *supra* note 152 at 474.

158. Before 2001, neither the *Criminal Code* nor any other statute exempted CSEC from the *Code*'s prohibition on the interception of private communications originating or terminating in Canada. See Canada, House of Commons, Standing Committee on Public Safety and National Security, "Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues" in *Final Report of the Standing Committee on Public Safety and National Security* (March 2007) at 53, online: <http://cmte.parl.gc.ca/Content/HOC/committee/391/secu/reports/rp2798914/sterrp07/sterrp07-e.pdf>. However, former CSEC agents have alleged that, before 2001, the agency sometimes intercepted private communications in Canada, including communications between Quebec separatists and the government of France. See Nomi Morris, "Inside Canada's Most Secret Agency" *Maclean's* 109:36 (9 February 1996) 32.

159. *Supra* note 4, s. 102.

160. R.S.C. 1985, c. N-5, part V.1 [*National Defence Act*].

formation from the global information infrastructure"[161] to provide "foreign intelligence."[162] Consistent with past practice, the legislation does not regulate the interception of non-Canadians' communications that are occurring wholly outside Canada.[163] It does, however, prevent the targeting of "Canadians or any person in Canada."[164] To account for the possibility that information about such persons may nonetheless be acquired incidental to foreign-directed surveillance, the statute also requires CSEC to take "measures to protect the privacy of Canadians in the use and retention of intercepted information."[165] The nature of these measures is not specified, but CSEC uses the following protocol to comply with this mandate:

> [information about Canadians] may only be retained if it is assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (*i.e.*, replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal government departments and agencies to explain their authority to collect this information under their own respective mandates

161. Section 273.61 of the *National Defence Act* defines "global information infrastructure" to include "electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks." *Ibid.*

162. Section 273.61 of the *National Defence Act* defines "foreign intelligence" to mean "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security." *Ibid.* Section 273.64 of the *National Defence Act* also directs the agency to help to protect "electronic information" and "information infrastructures" of "importance to the Government of Canada" and "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties." Notably, section 273.64(1)(*c*) of the *National Defence Act* does not give the agency any powers to assist in fulfilling the latter mandate, and it specifically directs that any such assistance is "subject to any limitations imposed by law on federal law enforcement and security agencies." See Forcese, *supra* note 23 at 453-54.

163. This follows from the use of the phrase "private communication," which is defined as having the same meaning as in s. 183 of the *Criminal Code*, *supra* note 21. *National Defence Act*, *ibid.*, s. 273.61. See also Canada, Communications Security Establishment Commissioner, *Annual Report: 2003-2004* (Ottawa: Minister of Public Works and Government Services Canada, 2006) at 6 [*Annual Report: 2003-2004*].

164. *National Defence Act*, *ibid.*, s. 273.64(2).

165. *Ibid.*

> and to provide an operational justification of their need to know this information. If these conditions are met, CSEC may release the suppressed information.[166]

Though the *Anti-terrorism Act* forbids CSEC from targeting Canadians, whether here or abroad, it breaks with the previous regime in permitting the surveillance of communications in Canada as a by-product of intercepts directed at foreign targets. Specifically, the responsible minister[167] "may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization."[168] The authorization may only issue if the Minister is satisfied that

> a. the interception will be directed at foreign entities located outside Canada;
>
> b. the information to be obtained could not reasonably be obtained by other means;
>
> c. the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
>
> d. satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.[169]

Such authorizations may persist for up to one year and are renewable for further one-year periods.[170] As with CSIS warrants, there is no notification requirement.

---

166. Canada, Communications Security Establishment Commissioner, *Annual Report: 2007-2008* (Ottawa: Minister of Public Works and Government Services Canada, 2008) at 10 [*Annual Report: 2007-2008*].

167. "Minister" is defined as "the Minister of National Defence or such other member of the Queen's Privy Council as may be designated by the Governor in Council to be responsible for the Communications Security Establishment." *National Defence Act*, *supra* note 160, s. 273.61.

168. *Ibid.*, ss. 273.65(1), 273.65(3). Section 273.69 of the *National Defence Act* states that "Part VI of the *Criminal Code* does not apply in relation to an interception of a communication under the authority of an authorization issued under this Part or in relation to a communication so intercepted."

169. *Ibid.*, s. 273.65(2). The minister may also impose "any conditions that the Minister considers advisable to protect the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications." *Ibid.* s. 273.65(5).

170. *Ibid.*, s. 273.68.

B. CONSTITUTIONALITY

As of yet, there are no decisions interpreting these provisions or deciding their constitutionality. Section 8 of the *Charter* is not likely engaged by purely foreign surveillance, *i.e.*, where none of the parties to the communication is either Canadian or in Canada.[171] So long as reasonable measures are taken to prevent it, it is also unlikely that the unintentional capture of communications of Canadians abroad would violate section 8.[172]

The situation is very different when there is a reasonable likelihood that one of the parties to the communication is in Canada. When such a communication is intercepted, the surveillance invades a reasonable expectation of privacy by definition, and the protection of section 8 is triggered.[173] There are good reasons to think, however, that foreign intelligence intercepts should operate under a different set of rules than criminal wiretaps. There is no doubt that a robust communications surveillance capacity is needed to combat the threats of foreign and foreign-influenced terrorism.[174] Further, as discussed in relation to the *CSIS Act*, national security investigations are often less targeted and more preventative than conventional criminal investigations. Advances in communications technology, including the move from circuit to packet-switched communications and the globalization of telecommunications infrastructure, require further departures from the orthodox, part VI model of wiretap regulation.[175]

---

171. See *Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841 at paras. 19-25, Lamer C.J., concurring (no reasonable expectation of privacy in foreign banking records). Note as well that purely foreign communications fall outside the definition of "private communication" in the *Criminal Code*, *supra* note 21, part VI. See *supra* note 26.

172. See *Thompson*, *supra* note 12 at para. 113 (noting that the interception of the communications of non-targeted people is "an unfortunate cost of electronic surveillance").

173. See *Hunter*, *supra* note 10.

174. See generally Richard Posner, "Commentary: A New Surveillance Act" *Wall Street Journal* (15 February 2006) A16. There is some evidence that, in recent years, CSEC has played a role in collecting communications aiding the detection and disruption of Al-Qaeda-inspired terrorist cells in Canada and elsewhere. See Rudner, "Signals Intelligence and Counter-Terrorism," *supra* note 152 at 482-83.

175. See Orin S. Kerr, "Updating the *Foreign Intelligence Surveillance Act*" (2008) 75 U. Chi. L. Rev. 225 at 233-36, 243 [Kerr, "Updating"]; K.A. Taipale, "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance" (2007) 9 Yale J.L. & Tech. 128 at 143-50; and *Annual Report: 2003-2004*, *supra* note 163 at 6.

It thus makes sense that CSEC warrants should be granted for "an activity or class of activities specified in the authorization" as opposed to a discrete, target-centered investigation.[176] This phraseology should be interpreted to encompass content filtering, traffic analysis, pattern analysis, data mining, and other staples of twenty-first century surveillance.[177] To comply with its statutory mandate and section 8 of the *Charter*, in using these techniques CSEC should have to show that it has adopted measures minimizing the risk of invading the privacy of innocent Canadians, such as access controls, rule-based processing, anonymization and selective revelation, addressing false positives, and audit and accountability functions.[178]

Similarly, it is appropriate that CSEC surveillance is not conditioned on reasonable grounds to believe that any particular target is a terrorist or an agent of a foreign power. In the context of transnational digital communications networks, investigators cannot always be expected to know the identity or location of their targets.[179] As the relevant provisions specify, it is reasonable that CSEC justify proposed intercepts with reference to their expected "foreign intelligence value."[180] CSEC should be permitted to show, for example, that a particular surveillance technique (say, the use of certain pattern recognition software to analyze data passing through certain internet switches) is likely to reveal valuable intelligence.[181]

---

176. *National Defence Act, supra* note 160, s. 273.65(1). This interpretation of this provision appears to accord with the interpretation proffered by the Department of Justice, and applied by CSEC. See generally *infra* note 198 and accompanying text. It differs from the interpretation favoured by the CSEC Commissioner, who has argued that "activity or class of activities" refers to the activities of surveillance targets. See *Annual Report: 2007-2008*, *supra* note 166 at 4; Canada, Communications Security Establishment Commissioner, *Annual Report: 2005-2006* (Ottawa: Public Works and Government Services, 2006) at 9-11 [*Annual Report: 2005-2006*].

177. See Taipale, *supra* note 175 at 150-55; Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) 75 U. Chicago L. Rev. 261.

178. See Rubinstein, Lee & Schwartz, *ibid.* at 266-70. These measures are analogous to the various minimization tools that may be required of traditional wiretap authorizations to comply with section 8. See generally *supra* note 73.

179. See Balkin, *supra* note 2 at 18; Paul M. Schwartz, "Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture" (2009) 97 Cal. L. Rev. 407 at 419.

180. *National Defence Act, supra* note 160, s. 273.65(2).

181. See Kerr, "Updating," *supra* note 175 at 16-17.

However, it is difficult to see how the absence of a judicial authorization requirement, at least in the absence of exigent circumstances,[182] could be reasonable under section 8. Ministerial authorization, of course, is not the same as judicial authorization. As Justice Dickson explained in *Hunter*,

> The purpose of a requirement of prior authorization is to provide an opportunity, before the event, for the conflicting interests of the state and the individual to be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are thus demonstrably superior. For such an authorization procedure to be meaningful it is necessary for the person authorizing the search to be able to assess the evidence as to whether that standard has been met, in an entirely neutral and impartial manner. ... The person performing this function need not be a judge, but he must at a minimum be capable of acting judicially.[183]

In other words, the person deciding whether to allow the intrusion must be independent of the state's investigative machinery. A minister of the government, especially one responsible for the operations of an investigative agency, cannot fulfill this role.

It is true that courts have traditionally been reluctant to interfere with the executive's power in matters of national defence and foreign relations.[184] The deference that courts rightly afford the government in this domain, however, is not unlimited.[185] As David Dyzenhaus has written, whatever the threat of international terrorism, the rule of law demands that judges check "each particular provision or act of discretion" for compliance with governing norms.[186]

It might also be argued that there is a "diminished" expectation of privacy in electronic communications flowing across Canada's borders. It is true that in other transborder contexts, such as immigration and customs, courts have

---

182. As in the criminal law context, warrantless national security surveillance may be justified (at least temporarily) by exigent circumstances. See generally *Charkaoui*, *supra* note 5 at para. 24 (noting that, in the national security context, "the executive branch of government may be required to act quickly, without recourse, at least in the first instance, to the judicial procedures normally required for the deprivation of liberty or security of the person").

183. *Hunter*, *supra* note 10 at 161-62.

184. See generally *Canada (Prime Minister) v. Khadr*, [2010] 1 S.C.R. 44 at paras. 2, 33-39 [*Khadr*].

185. See generally *Operation Dismantle v. The Queen*, [1985] 1 S.C.R. 441.

186. David Dyzenhaus, "The Permanence of the Temporary: Can Emergency Powers be Normalized?" in Daniels, Macklem & Roach, *supra* note 81, 21 at 32.

countenanced warrantless searches of persons, vehicles, and goods.[187] Imposing a warrant requirement in these circumstances would severely curtail the state's ability to prevent dangerous persons and substances from entering Canada.[188] As noted by the Court in *R. v. Simmons*, "travellers seeking to cross national boundaries fully expect to be subject to a screening process."[189] It is doubtful, however, that Canadians reasonably expect their international telephone and other electronic communications to be monitored by the state without judicial authorization. Such communications are much more ubiquitous, and their interception much more invasive, than searches of persons and goods crossing the nation's borders. As mentioned, the strength of the privacy interest in domestic-foreign electronic communications is recognized in the *Criminal Code*, which requires the police to obtain warrants to perform surveillance of them and, in the context of criminal law enforcement, at least, criminalizes unauthorized interception.[190]

To justify warrantless surveillance by CSEC, we thus need evidence that either a warrant requirement would unduly hamper its ability to collect national security intelligence, or that the legislation provides an adequate substitute. This evidence is lacking. As we have seen, CSIS must obtain warrants before conducting communications surveillance, and there is no indication that this requirement has thwarted that agency's national security efforts. As noted in *Atwal*, judicial authorization was made part of the *CSIS Act* not only to protect citizens against "unjustified surveillance,"[191] but also to bolster public confidence in the agency's activities. The court stated that "[t]he credibility of the Service has a direct and positive, but by no means exclusive, dependency on the credibility of the judicial presence in the system."[192] This reasoning applies equally to CSEC's domestic surveillance activities.

Nor does the *National Defence Act* provide anything to replicate the protections of *ex ante* judicial review. The legislation does subject CSEC's surveillance activities to *ex post* oversight. The CSEC Commissioner, who must be a former

187. See *Simmons*, *supra* note 17; *Monney*, *supra* note 17; and *Jacques*, *supra* note 17.

188. See *Simmons*, *ibid.* at 527-29.

189. *Ibid.* at 528.

190. *Supra* note 26.

191. *Atwal*, *supra* note 112 at 139.

192. *Ibid.* at 140.

superior court judge,[193] is required, *inter alia*, to review "activities carried out" under intercept authorizations "to ensure that they are authorized and report annually to the Minister on the review."[194] As discussed, rigorous and independent oversight mechanisms are a helpful complement to judicial authorization, especially in the national security context where investigative intrusions are so rarely subject to *ex post* review. For several reasons, however, such mechanisms are not a sufficient substitute for judicial authorization.

First, unlike *ex ante* authorization, *ex post* review obviously cannot prevent unlawful invasions of privacy before they occur.[195] Second, effective review requires full information. On several occasions, the commissioner has reported that CSEC failed to provide him with sufficient documentation to verify the lawfulness of ministerial authorizations.[196] Third, the commissioner has no enforcement powers. The public availability of annual reports undoubtedly encourages compliance, but neither the minister nor CSEC is obliged to follow the commissioner's recommendations or advice.[197] Lastly, unlike a judge deciding an authorization application, the commissioner is not empowered to issue authoritative interpretations of the governing legislation. In recent years, the commissioner has disputed the government's interpretation of the ministerial authorization provisions.[198] However, in keeping with his advisory role, he has

193. *National Defence Act*, *supra* note 160, s. 273.63. Since 2003, all commissioners have been former justices of the Supreme Court of Canada. The current commissioner is Peter Cory, who was appointed for a three-year term in December 2009.

194. *Ibid.*, s. 273.65(8).

195. See Canada, Communications Security Establishment Commissioner, *Annual Report: 2004-2005* (Ottawa: Minister of Public Works and Government Services Canada, 2005) at 7 [*Annual Report: 2004-2005*].

196. *Annual Report: 2007-2008*, *supra* note 166 at 11-14; *Annual Report: 2005-2006*, *supra* note 176 at 10.

197. See *e.g. Annual Report: 2007-2008*, *ibid.* at 13 (noting that, in the case of one authorization, "CSEC had not complied with expectations set out in the ministerial directive"); Canada, Communications Security Establishment Commissioner, *Annual Report: 2008-2009* (Ottawa: Public Works and Government Services, 2009) at 13 [*Annual Report: 2008-2009*] (noting failures to meet expectations set out in authorizations and reporting an increase in the number of inadvertent intercepts).

198. See *Annual Report: 2007-2008*, *ibid.* at 4; Canada, Communications Security Establishment Commissioner, *Annual Report: 2006-2007* (Ottawa: Public Works and Government Services, 2007) at 2-3 [*Annual Report: 2006-2007*]; and *Annual Report: 2005-2006*, *supra* note 176 at 9-11.

assessed compliance on the basis of the government's position.[199] For obvious reasons, it is inappropriate to leave the interpretation of privacy-invasive surveillance powers to the government.

Whatever the merits of judicial authorization in principle, it has been suggested that courts lack jurisdiction to authorize foreign surveillance.[200] A warrant issued by a Canadian court authorizing a search in a foreign country would certainly not be recognized under that country's law. Parliament can, however, empower judges to authorize Canadian officials to invade the privacy of Canadian residents, even if the invasion is executed, in a physical sense, outside Canada.[201] As the Court has held, parliament "has the legislative competence to enact laws having extraterritorial effect."[202] Indeed, parliament has given jurisdiction to courts to try numerous criminal offences committed in whole or in part outside of Canada.[203]

Allowing courts to authorize foreign-executed intercepts of domestic communications, moreover, is consistent with the law's general approach to territorial jurisdiction. Jurisdiction is typically recognized when the subject matter has a

199. See *Annual Report: 2008-2009*, *supra* note 197 at 3, 10; *Annual Report: 2007-2008*, *ibid.* at 10-11; and *Annual Report: 2005-2006*, *ibid.* at 11.

200. See *Annual Report: 2008-2009*, *ibid.* at 8; *Annual Report: 2005-2006*, *ibid.* at 7-8; *Annual Report: 2006-2007*, *supra* note 198 at 5; and Special Senate Committee on the Anti-terrorism Act, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act* (February 2007) at 77.

201. See Friedland, *supra* note 81 at 276, n. 52. Transnational electronic communications are transmitted by a variety of means (including wireless technologies like satellite and line-of-sight microwave radio-relay as well as wire-line technologies like copper and fibre optic cable), and may be intercepted at a variety of "places" (including terrestrial and space-based wireless receivers, terrestrial and submarine cables, and telecommunications switching centres). CSEC likely conducts all of these types of intercepts, some of which occur within Canada in a physical sense (such as interceptions by satellite and microwave receivers on Canadian soil or by wiretaps installed at the switching stations of Canadian telecommunications service providers). See Rudner, "Canada's Communications Security Establishment," *supra* note 149 at 105-08. Even if it is admitted, *arguendo*, that a Canadian court would not have the jurisdiction to authorize an intercept placed outside of Canada, this does not explain or justify the absence of a judicial authorization requirement for CSEC intercepts that *are* executed here.

202. *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427 at para. 54 [*SOCAN*].

203. See *e.g. Criminal Code*, *supra* note 21, ss. 7, 46(3), 74, 75, 76-78.1, 83.08(1), 290(1)(*b*), 354(1)(b), 462.3, 465(4)-(5).

"real and substantial" connection to Canada, and the granting of jurisdiction would not unduly compromise the principle of comity between nations.[204] As discussed, under the current legislative regime, CSEC is required to obtain ministerial authorizations only for intercepts that may collect a "private communication," *i.e.*, where one party to the communication is located in Canada. This is surely a sufficient nexus to Canada. Indeed, in the context of telecommunications transmissions, the Court has held that Canadian courts have jurisdiction when Canada is either the country of origin[205] or the country of reception.[206] And as for the question of comity, to the extent that a foreign intercept intrudes upon the sovereignty or territorial integrity of other nations, the intrusion is no greater if authorized by a judge than by a minister.[207]

Jurisdiction should not, therefore, be an impediment to instituting a scheme of prior authorization for CSEC intercepts of the communications of Canadian residents. Parliament should amend the *National Defence Act* to provide for a judicial authorization procedure for domestic intercepts. If it does not, the courts should rule that the *Act* violates section 8 of the *Charter*.[208]

IV. CONCLUSION

The threat of terrorism, in Canada and other nations, is undoubtedly very real and must be taken with the utmost seriousness. Legal responses to this fear, however, must be tempered by a rational analysis of risks and a commitment to preserving as many of our liberties as are compatible with our need for genuine

---

204. *Libman v. The Queen*, [1985] 2 S.C.R. 178 at 212-14.

205. *Ibid.*

206. See *SOCAN*, *supra* note 202 at para. 59 ("a telecommunication from a foreign state to Canada, or a telecommunication from Canada to a foreign state, 'is both here and there'; [r]eceipt may be no less 'significant' a connecting factor than the point of origin (not to mention the physical location of the host server, which may be in a third country").

207. The principle of comity may indeed suggest that such intercepts receive ministerial authorization, but as a prerequisite to, and not a substitute for, judicial authorization. See generally *Criminal Code*, *supra* note 21, s. 185(1); *CSIS Act*, *supra* note 111, s. 21(1).

208. See Hubbard, Brauti & Fenton, *supra* note 31, § 17.3; Forsese, *supra* note 23 at 457-58; Irwin Cotler, "Terrorism, Security and Rights: The Dilemma of Democracies" (2002-2003) 14 N.J.C.L. 13 at 45; and Friedland, *supra* note 81 at 276. For contrary views, see Cohen, *Privacy, Crime and Terror*, *supra* note 23 at 228-31; *Annual Report: 2004-2005*, *supra* note 195 at 9.

security. Many of Canada's legislative answers to the events of 9/11 have failed to live up to this ideal. This is certainly true of the changes to communications surveillance law effected by the *Anti-terrorism Act*. Both the exemption of terrorist offences from the investigative necessity requirement in part VI of the *Criminal Code* and the creation of domestic surveillance powers under the *National Defence Act* compromise privacy without achieving appreciable security gains. They should be struck down as violations of section 8 of the *Charter*.

The search and surveillance provisions in the *CSIS Act*, in contrast, set out a reasonable accommodation between these competing interests. Is it a coincidence that the former provisions were rushed through parliament soon after a brutal and traumatizing act of terror, whereas the latter were enacted in the aftermath of a comprehensive, independent, and scholarly review of the RCMP's national security operations?[209] To ask the question is to answer it.

209. See generally Andrew Goldsmith, "The Governance of Terror" (2008) 30 Law & Pol'y 141 at 156-59 (relating the hasty legislative process that resulted in the enactment of the *Anti-terrorism Act*).