SURVEILLANCE AND SECURITY IN AN AGE OF TERROR: CANADIAN PERSPECTIVES

To be presented at the 22nd International Conference of the
International Society for the Reform of the Criminal Law
Dublin, Ireland ~ July 15, 2008

Steven Penney
Associate Professor
Faculty of Law, University of Alberta
spenney@ualberta

INTRODUCTION

In response to the recent spate of Islamist terrorism, many nations have adopted laws enlarging the search and surveillance capacities of law enforcement and national security agencies. Some have argued that any benefit of these laws to counter-terrorism efforts is offset by their negative impact on the liberty and privacy of non-terrorists, especially those who innocently share racial, ethnic, religious, or ideological affiliations with terrorist groups. In some cases, these laws have also been challenged as violating national and international human rights norms.

To date, Canada has experienced little of this controversy. Like many other countries, Canada introduced a raft of legislative reforms in the aftermath of 9/11, including some that enhanced the search and surveillance powers of counter-terrorism agencies. But debates about anti-terrorism laws have largely focussed on other issues, such as immigration procedures and the definition of terrorist offences. In this paper, I explore the reasons for this silence. Put simply, before 9/11, Canada's counter-terrorism agencies already had very broad search and surveillance powers. To date, these powers have mostly been exercised in secret and have generated very little litigation or public scrutiny.

This may be in the process of changing. As counter-terrorism agencies increasingly look to arrest, detain, and prosecute persons involved in terrorist activities,[1] courts will be required to interpret the scope of these powers and decide whether they violate section 8 of the *Canadian Charter of Rights and Freedoms*, which states that "[e]veryone has the right to be secure against unreasonable search or seizure."[2]

This paper examines three sets of statutory powers: (*i*) the communications surveillance powers given to conventional police agencies, including the Royal Canadian Mounted Police (RCMP); (*ii*) the search and surveillance powers given to the Canadian Security Intelligence Service (CSIS); and (*iii*) the communications

[1] See *e.g.* Isabel Teotonio, "Court hears plan to storm Parliament, 'kill everybody' *The Toronto Star* (4 June, 2008) (wiretap evidence presented in terrorism trial); Kent Roach, "The Toronto Terrorism Arrests" (2006) 51 Crim. L.Q. 389.

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

surveillance powers given to the Communications Security Establishment Canada (CSEC). I analyze the legal and constitutional issues arising from these powers and make suggestions for reform.

POLICE SURVEILLANCE POWERS

Context

As the dividing line between national security and criminal law enforcement is often blurry, police have long been involved in national security investigations.[3] The investigative powers available to them do not generally turn on any distinction between national security and criminal matters. Police have a myriad of such powers, stemming from both common law and statute.[4] This paper discusses only one: the power to conduct electronic communications surveillance under Part VI of the *Criminal Code*. This is one of the most important (and intrusive) powers available to police investigating national security matters, and I discuss below, it is one of the few that operates differently in the context of counter-terrorism than in ordinary criminal investigations.

The surveillance powers in Part VI may be used by a wide variety of law enforcement agencies.[5] But in the realm of national security, they are used mostly by Canada's national police force, the Royal Canadian Mounted Police (RCMP).[6] RCMP national security investigators work closely with other law enforcement

---

[3] From Confederation (1867) to 1920, most national security matters were handled by the Dominion Police Force (DPF). The RCMP became increasingly involved during World War I, and absorbed the DPP in 1920. For histories of the RCMP's involvement in national security, see Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation Maher Arar, *A New Review Mechanism for the RCMP's National Security* Activities (The Honourable Dennis O'Connor, Commissioner) (Ottawa: Public Works and Government Services Canada, 2006) [O'Connor Report]; 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 44 (Chair, D.C. McDonald) [McDonald Report].

[4] Most of these powers are contained in the *Criminal Code*, R.S.C. 1985, c. C-46.

[5] See *Criminal* Code, ss. 2 (definitions of "peace officer" and "public officer") and 185(1) (giving power to apply for surveillance warrants to peace officers and public officers).

[6] The *Security Offences Act*, R.S.C. 1985, c. S-7, ss. 2, 6, specifies that RCMP members "have the primary responsibility to perform the duties that are assigned to peace officers" in relation to both national security offences (as defined in the *CSIS Act*) and offences where the victim is an "internationally protected person" (as defined in s. 2 of the *Criminal Code*). The *CSIS Act* offences are discussed *infra* notes XX-XX and accompanying text.

and national security agencies, however, and information is freely shared among them.[7] The focus here, then, is on the powers themselves, and not on the officials who exercise them.

Legislation

Subject to a number of exceptions, Part VI of the *Criminal Code* prohibits and provides criminal punishments for the electronic interception of private, domestic communications.[8] To be covered by this prohibition, a communication must be both "intercepted"[9] and attract a "reasonable expectation of privacy."[10] There are unresolved interpretive questions relating to each of these requirements,[11] but the basic scope of the prohibition is well understood. Unless an exception applies, it is a crime for any person (including a state agent) to use technological means to prospectively capture the content[12] of both oral

[7] The federal government may also enter into agreements with the provinces permitting provincial and municipal police agencies to play a role in investigating these offences. *Security Offences Act*, s. 6(2).

[8] *Criminal Code*, 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.

[9] Section 184(1) of the *Criminal Code* 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."

[10] Section 183 of the *Criminal Code* defines "private communication" to mean "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."

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

[12] "Content" refers to the substantive message that a human sender intends to communicate to a human recipient. It does not include the "envelope" data attaching to electronic communications, *i.e.* the accompanying addressing and other information that is analogous to the information available from unopened letter mail. Nor does include the transmission of data from a person to a computer (as in web searching and surfing) or from a computer to another computer. See Orin S. Kerr, "Internet Surveillance Law After the *USA Patriot Act*: The Big Brother that Isn't (2003) 97 Nw. U. L. Rev. 607 at 611-16; Robert W. Hubbard, Peter DeFreitas and Susan Magotiaux, "The Internet: Expectations of Privacy in a New Context" (2002) 45 Crim. L.Q. 170 at 190. Though it is not entirely free from doubt, this definition likely inheres in the word "communication" as used in Part VI. See generally *R. v. Goldman*, [1980] 1 S.C.R. 976 at 995 ("A communication involves the

communications and electronic text communications. This includes the real-time interception of wire-line and wireless telephone conversations as well as email and other forms of electronic text.[13] Retrospective acquisition of stored communications, in contrast, is probably not covered by Part VI and may be effected with ordinary search warrants.[14] A separate provision extends the protections of Part VI 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."[15]

As mentioned, these prohibitions are subject to several exemptions. The most important permits police to obtain an interception authorization (*i.e.* a warrant) from a judge.[16] The requirements for obtaining such an authorization are more onerous than those applying to ordinary search warrants.[17] For both ordinary search warrants and Part VI authorizations, police must show that they have

---

passing of thoughts, ideas, words or information from one person to another."). The envelope data attaching to electronic communications may be obtained (prospectively and retrospectively) under separate, and less onerous, warrant procedures. None of these makes any exception for criminal organization or terrorism investigations. See *Criminal Code*, ss. 487, 487.01, 492.2; Penney, *supra* note 11 at 143-45.

[13] See Penney, *supra* note 11 at 118-26.

[14] *Ibid*. at 126-29.

[15] *Criminal Code*, ss. 487.01(4)-(5).

[16] See *Criminal Code*, s. 184(2)(*b*). Other exceptions permit intercepts by: operators or regulators of communications networks for maintenance or security purposes (ss. 184(2)(*c*)-(3)); police to prevent one of the parties to the communication from causing immediate, serious harm (s. 184.4); and persons authorized by one of the parties to the communication (s. 184(2)(*a*)). The last exception exempts one-party "consent" or "participant" surveillance from the criminal prohibition. Conducting such surveillance without judicial authorization, however, will normally violate section 8 of the *Charter* and result in the exclusion of any evidence obtained. See *R. v. Duarte*, [1990] 1 S.C.R. 30; *Criminal Code*, s. 184.2. The evidence obtained in violation of s. 8 was admitted in *Duarte* on the basis of the good faith of the police. The breach, the Court stated at XX, "stemmed an entirely reasonable misunderstanding of the law." After *Duarte* such a misunderstanding would presumably no longer be reasonable and typically result in exclusion. See Robert W. Hubbard, Peter M. Brauti and Scott K. Fenton, *Wiretapping and other Electronic Surveillance: Law and Procedure*, looseleaf (Aurora, Ont.: Canada Law Book Inc., 2005) § 2.2.2.

No warrant is needed when such surveillance is used solely to ensure the safety of undercover agents, but any evidence collected is inadmissible except in proceedings relating to the infliction of bodily harm upon the agent. If no such violence occurs, any intercepted private communications must also be destroyed. See *Criminal Code*, s. 184.1.

[17] 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."

reasonable and probable grounds to believe that the interception will provide evidence of an offence.[18] And in both cases, evidence obtained in violation of this or any other statutory requirements may be excluded at trial under section 24(2) of the *Charter*.[19] But unlike ordinary warrants, Part VI authorizations may be obtained only from superior court judges[20] and only to further the investigation of certain listed offences.[21] In addition, the application for the authorization must

---

[18] The *Code* does not explicitly require police to establish reasonable and probable grounds. Section 186(1)(*a*) does oblige the issuing judge issuing the warrant to be satisfied that "it would be in the best interests of the administration of justice to do so." 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 16 at 45. See also *R. v. Araujo*, [2000] 2 S.C.R. 992 at para. 20; *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1444.

"Reasonable and probable grounds" means the same thing as "reasonable grounds," "probable grounds," "reasonable and probable cause" and "probable cause." See generally *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at 167 ("The 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."); *R. v. Kang-Brown*, 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, Ont.: Canada Law Book, 2005) § 3.1140.

[19] Initially, the *Code* specified that unlawfully intercepted private communications were inadmissible as evidence against the parties to the communication. See *Criminal Code*, R.S.C., 1970, c. C-34, ss. 178.16(1)-(3.1) (as amended). Parliament repealed these provisions in 1993. See *An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunications Act*, S.C. 1993, c. 40, s. 10. Since 1993, the admission of unlawfully obtained private communications has been governed by s. 24(2) of the *Charter*, which empowers judges to exclude unconstitutionally obtained evidence "if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute." 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 *e.g. R. v. Thompson*, [1990] 2 S.C.R. 1111. In such cases, the admission of intercepted evidence will turn on a consideration of the seriousness of the constitutional infringement as well as the seriousness of the offence. See *R. v. Fliss*, [2002] 1 S.C.R. 535 at paras. 75-89. See also *Duarte*, *supra* note 16 at 59-60; *Thompson*, *ibid*. at 1154-56; Steven Penney, "Taking Deterrence Seriously: Excluding Unconstitutionally Obtained Evidence Under Section 24(2) of the *Charter*" (2004) 49 McGill L.J. 105 at 133-41.

[20] 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. This requirement does not apply in the Province of Quebec, where authorizations may be granted by the provincially-appointed judges of the Court of Quebec. *Criminal Code*, ss. 185(1), 552.

[21] *Criminal Code*, 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

include the written consent of the responsible Minister or his or her designate.[22]

The most important difference between an ordinary warrant and a Part VI authorization, however, is that only the latter (generally) requires police to demonstrate "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."[23]

This "investigative necessity" requirement has been interpreted to mean that "practically speaking" there must be "no other reasonable alternative method of investigation."[24] Interception need not be an investigative method of "last resort."[25] The test can be satisfied by demonstrating that "normal investigative techniques are unlikely to succeed."[26] On the other hand, the requirement is more rigorous than simply showing that interception would likely the "most efficacious" way to further the investigation.[27] Such a standard, the courts have held, would "replace a standard of necessity with one of opportunity at the discretion of law enforcement bodies."[28] Investigative necessity can be demonstrated in a variety of ways, for example by showing that alternative methods, such as physical surveillance, informants, undercover agents, and ordinary search warrants, would likely be too dangerous or ineffective.[29] Such conditions may be particularly prevalent in an investigation of "a large-scale crime organization, a close-knit family or a drug conspiracy," where "counter-surveillance methods" are common.[30]

---

discussion *infra* notes XX-XX and accompanying text.

[22] *Criminal Code*, s. 185(1).

[23] *Criminal Code*, s. 186(1)(*b*).

[24] *Araujo*, *supra* note 18 at para. 29.

[25] *Ibid*. This had been suggested in earlier decisions. See *e.g. Duarte*, *supra* note 16 at 55, La Forest J.; *R. v. Commisso*, [1983] 2 S.C.R. 121 at 135, Dickson J., dissenting; *Thompson*, *supra* note 19 at 1160, La Forest J., dissenting; *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.

[26] *Araujo*, *supra* note 18 at para. 29.

[27] *Araujo*, *supra* note 18 at para. 39. This had also been suggested in previous decisions, including that of the court below in *Araujo*. *R. v. Araujo* (1998), 127 C.C.C. (3d) 315 at para. 30 (B.C.C.A.). 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.).

[28] *Araujo*, *supra* note 18 at para. 39.

[29] *Ibid*. at paras. 41-43.

[30] *Ibid*.

In 1997, in response to concerns about violent competition between gangs, Parliament deleted the investigative necessity requirement for investigations of "criminal organization" offences.[31] And in 2001, in response to 9/11, it did the same for "terrorism" offences.[32] Two additional exemptions for criminal organization and terrorism investigations accompanied these amendments: (*i*) the maximum period of interception (subject to renewal) was extended from the ordinary sixty days[33] to one year;[34] and (*ii*) investigators seeking to extend the deadline for informing people that they were targeted by an interception were exempted from the ordinary requirement of showing that the investigation of the offence (or another offence for which an intercept authorization is available) is "continuing."[35]

In summary, police may conduct electronic surveillance of private, domestic communications and activities when they have probable cause to believe that such surveillance will reveal evidence of a broad range of criminal offences,

---

[31] *An Act to amend the Criminal Code (criminal organizations) and to amend other Acts in consequence*, S.C. 1997, c. 23, s. 5. For the definitions of "criminal organization" "criminal organization offence," see *Criminal Code*, ss. 2, 467.1. For criticisms of the breadth of these definitions, see Don Stuart "Time to Recodify Criminal Law and Rise Above Law and Order Expediency: Lessons From the Manitoba Warriors Prosecution" (2002) 112 Man. L.J. 89. To date constitutional challenges to these definitions have failed. See *R. v. Lindsay* (2004) 182 C.C.C. (3d) 301 (Ont. S.C.J.); *R. v. Terezakis* (2007) 223 C.C.C. (3d) 344 (B.C.C.A.); *R. v. Smith* (2006) 280 Sask. R. 128 (Q.B.).

[32] *Anti-terrorism Act*, S.C. 2001, c. 41, ss. 6.1 and 133(8.1). The criminal organization and terrorism exemptions to the investigative necessity requirement are codified at *Criminal Code*, ss. 185(1.1), 186(1.1).

[33] *Criminal Code*, ss. 186(4)(*e*), 186(7).

[34] *Criminal Code*, s. 186.1.

[35] Targets must usually be notified of the interception no later than ninety days after the authorization has expired. However, investigators may apply to the authorizing judge, either at the time the authorization is sought or at any time before its expiry, to have this period extended up to a (perpetually renewable) maximum of three years. If the application is made at the time the authorization is sought, it must be personally approved by the responsible Minister. Such an application will be granted if the judge believes that the "interests of justice" require it. This procedure applies in the same manner to all offences. If the application for an extension of the notification requirement is made after the authorization is granted, it need not be accompanied by the Minister's personal approval. Normally, such an application will be granted if the judge is satisfied not only that the "interests of justice" require it but also that the investigation of the offence (or another offence for which an intercept authorization is available) is "continuing." The latter requirement is waived, however, for criminal organization and terrorism investigations. *Criminal Code*, ss. 185(2)-(3), 196.

including all of those related to terrorism. If they are investigating possible terrorists (or other criminal groups), then they need not demonstrate investigative necessity and may be permitted to surveil for a longer period of time.

Constitutionality

The next question, then, is whether this regime comports with section 8 of the *Charter*. Though it has not ruled on the question, the Supreme Court of Canada has intimated that a demonstration of investigative necessity is needed to justify the sweeping invasion of privacy entailed by electronic surveillance. 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.[36]

Put in more instrumental terms, restrictions on electronic surveillance encourage people to communicate more candidly than they otherwise would.[37] As Richard

---

[36] See especially *R. v. Duarte*, [1990] 1 S.C.R. 30 at XXX.

[37] See generally Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies" (2007) 97 J. Crim. L. & Criminology 477 at 492-93; Richard Posner, "Privacy, Secrecy, and Reputation" (1979) 28 Buff. L. Rev. 1 at 17; Charles J. Hartmann and Stephen M. Renas, "Anglo-American Privacy Law: An Economic Analysis" (1985) 5 Int'l Rev. Law Econ. 133 at 145; Anthony Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minn. L. Rev. 349 at 388.

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."[38] Legal restrictions on electronic surveillance also diminish the need to protect privacy by other means.[39] Instead of avoiding the disclosure of sensitive information, people may wastefully expend resources to enhance the security of their communications. Without laws against wiretapping, for example, people would be more likely to use public payphones (where they still exist) instead of their own phones.

Of course, as Justice La Forest recognized in *Duarte*, the benefits of privacy must be balanced against those of law enforcement.[40] The protections of Part VI, he concluded, provide for this balance. Though it is clear that he considered the probable cause and prior authorization requirements to be the lynchpins of this protection,[41] he also noted that the investigative necessity requirement is part of a legislative scheme that "sets a high standard" for obtaining authorizations.[42] Similarly, in *R. v. Araujo*, the leading decision interpreting the meaning of investigative necessity, Justice LeBel stated the following for a unanimous Court:

> . . . [W]e 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 . . ..[43]

---

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

[39] 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.ssrn.com/abstract=422220>; Amsterdam, *ibid*. at 403; *United States v. Dunn*, 480 U.S. 294 at 319, Brennan J., dissenting.

[40] *Duarte*, *supra* note 36 at 45.

[41] *Ibid*. ("the law recognizes that a person's privacy is intruded on in an unreasonable manner whenever the state, without a prior showing of reasonable cause before a neutral judicial officer, arrogates to itself the right surreptitiously to record communications that the originator expects will not be intercepted by anyone other than the person intended by its originator to receive them, to use the language of the *Code*").

[42] *Ibid*. See also *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1444.

[43] *Supra* note 18 at para. 26 [emphasis added]. See also *R. v. S.A.B.*, [2003] 2 S.C.R. 678 at paras. 53 (referring, in the context of assessing the constitutionality of the *Code*'s DNA warrant provisions, to investigative necessity as a "constitutional requirement" for wiretap authorizations).

As the constitutionality of the investigative necessity exemptions was not at issue, this passage is technically *obiter dicta*.[44] It reflects, however, a consistent theme in the court's Part VI and section 8 jurisprudence: electronic surveillance is a grave threat to privacy and should not be employed unless an independent arbiter is satisfied, to a reasonable level of certainty, that it necessary to combat serious crime.[45]

Despite these *dicta*, the lower courts that have considered the matter have held that investigative necessity is not a constitutional requirement. The first case to do so, *R. v. Bordage*, considered the validity of the *Code*'s one-party consent surveillance provisions.[46] Before 1993, the *Code* contained no authorization procedure for such surveillance. As a consequence of this, and of the fact that such surveillance was (and is still) not criminally prohibited, police used it without restriction. In *Duarte*, the Supreme Court decided that warrantless consent surveillance violated section 8 of the *Charter*. Parliament responded by enacting the authorization process referred to above,[47] but it did not include an investigative necessity requirement.

Though the *Duarte* Court was correct to subject consent surveillance to the requirements of section 8, such 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.[48] Police are unlikely to attempt them if effective, alternative measures

---

[44] Justice LeBel specifically noted that the criminal organization amendment was "not invoked or examined in the case at bar." *Araujo*, *supra* note 18 at para. 2.

[45] The Supreme Court has considered whether investigative necessity is constitutionally required in three other contexts. It found that it is required for searches of potentially privileged material in lawyers officers (See *Lavallee, Rackel & Heintz v. Canada (Attorney General); White, Ottenheimer & Baker v. Canada (Attorney General); R. v. Fink*, [2002] 3 S.C.R. 209 at paras. XXX-XXX; but not for searches of media offices (*Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1991] 3 S.C.R. 459 at 478; *Canadian Broadcasting Corporation v. Lessard*, [1991] 3 S.C.R. 421 at 446) or the taking of bodily samples for identification purposes (*S.A.B.*, *supra* note 43 at XXX).

[46] *R. v. Bordage* (2000) 146 C.C.C. (3d) 549 (Que. 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, 64 W.C.B. (2d) 201 (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).

[47] See S.C. 1993, c. 40, s. 4 and *supra* note 16.

[48] See Hubbard, Brauti and Fenton, *supra* note 16 § 4.3.2.

are available. As a consequence, requiring investigative necessity would probably do little to decrease the frequency of consent surveillance. Third party surveillance, in contrast, is 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 of privacy, and less likely to generate the social costs referred to above. In relaying confidences to another, there is always a possibility that our confidant will betray us and use the information to our detriment, for example by conveying it to police. The extent of this risk is undoubtedly magnified, as Justice La Forest noted in *Duarte*, when the conversation is overheard, and potentially recorded, by state agents. That Court was thus correct to conclude that our awareness of these risks does not justify excluding consent surveillance from the ambit of section 8. The risk is not of the same magnitude, however, as the risk that the state will intercept and record confidences that have not been betrayed. With third party surveillance, the trust that we have in our confidants is irrelevant. The state may be listening even if we are conversing with a close family member.

Third party surveillance is more likely than consent surveillance to capture innocent communications.[49] Interceptions of the latter sort may only capture the communications of a specific, named, consenting person.[50] The authorizing judge may also permit only a subset of these communications to be captured, such as conversations with named targets, with unnamed persons located at a particular place, or in furtherance of a *bona fide* investigation.[51] Analogous conditions are

[49] See *Thompson*, *supra* note 19 at XXXX.

[50] See Hubbard, Brauti and Fenton, *supra* note 16 § 3.5.5.2.

[51] *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*, 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 25; *Thompson*, *supra* note 19 at XXX-XXX; *Garofoli*, *supra* note 18 at XXX.

available for third party intercepts, such as live monitoring[52] or retrospective editing,[53] but they are less likely to be imposed because they are so costly.[54]

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 fact that applications may be made by the police (instead of agents of the responsible Minister); made to provincial court judges as well as superior court judges; obtained in relation to any federal offence; and obtained via a tele-warrant.[55]

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 relay the information to police, prosecutors, and the court in *viva voce* form.[56] 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, then, do little to resolve the question of whether investigative necessity is constitutionally required for third party surveillance in criminal organization and terrorism offences. To date, the courts have addressed, and upheld, only the criminal organization exemption.[57] 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,

---

[52] 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 19; Hubbard, Brauti, and Fenton, *supra* note 16 § 4.4-4.4.1.

[53] This condition permits the recording of all authorized interceptions, but requires investigators to cease listening to and seal irrelevant portions. 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*.

[54] See *Finlay*, *supra* note 25 at 75; *R. v. Taylor*, [1998] 1 S.C.R. 26 at para. 18; Stanley A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (1983) at 174.

[55] *Criminal Code*, s. 184.2-184.3.

[56] See Hubbard, Brauti, and Fenton, *supra* note 16 § 2.2.5; *R. v. Rosebush* (1992) 77 C.C.C. (3d) 241 (C.A.), leave to appeal to S.C.C. refused 78 C.C.C. (3d) vi.

[57] *R. v. Doucet* (2003), 18 C.R. (6th) 103 (Que. Sup. Ct.); *R. v. Pangman* (2000), 147 Man. R. (2d) 93 (Q.B.); *R. v. Doiron* (2004) 274 N.B.R. (2d) 120 (Q.B.), aff'd (2007) 315 N.B.R. (2d) 205, 221 C.C.C. (3d) 97 (C.A.).

criminal and terrorist organizations are more sophisticated, impenetrable, and dangerous.[58] We should respect Parliament's choice, the argument runs, to give law enforcement the tools it needs (including electronic surveillance) to combat these groups. The investigative necessity requirement, on this view, unduly hampers this effort.

But if police are investigating truly sophisticated enterprises, shouldn't it be easy for them to show that conventional investigative methods are unlikely to succeed? As discussed above, the Supreme Court has interpreted the requirement in a flexible and pragmatic fashion, taking into account the investigative challenges posed by criminal groups. If applicants provide authorizing judges with a proper evidential foundation, and if judges apply the standard as the Court has instructed, the investigative necessity requirement should not hinder investigators.

Law enforcement agencies may have believed, however, that some authorizing judges were asking too much of them, and that establishing investigative necessity was either too onerous or redundant. On this view, if organized crime and terrorists are by definition "hard targets," we are better off with a bright-line, categorical exemption.

If the exemption really were limited to sophisticated criminal enterprises, this argument might have some purchase. Who but hardened defence lawyers would complain about the necessity of electronic surveillance to combat "biker gangs," international "mafias," or Al-Qaeda? As the authors of a leading text on electronic surveillance have written, as compared with the 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."[59]

On close inspection, however, it is apparent that the exemptions are in no way limited to investigations of sophisticated or (especially) dangerous groups. As the focus of this paper is national security surveillance, and as others have criticized the criminal organization exemption,[60] I focus here on the scope of the

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

[59] Hubbard, Brauti and Fenton, *supra* note 16 § 16.2. Friedland at 274.

[60] See Nathan Whitling, "Wiretapping, Investigative Necessity, and the *Charter*" (2002) 46 Crim. L.Q. 89.

terrorism exemption.

This exemption applies to any "terrorism offence,"[61] which is defined to mean one of the following:

1. an offence under sections 83.02-83.04 or 83.18-83.23 of the *Criminal Code*;
2. an indictable federal offence "committed for the benefit of, at the direction of or in association with a terrorist group;"
3. an indictable federal offence which "also constitutes a terrorist activity;" or
4. conspiracies, attempts, counselling, and being an accessory after the fact in relation any of the above offences.[62]

As detailed immediately below, the definitions of many of these offences are very broad.[63] Police will consequently often be able to intercept the communications of unsophisticated suspects who would have been vulnerable to conventional investigative techniques.[64] In the absence of an investigative necessity requirement, the private communications and activities of these people may be justified simply by showing probable cause to believe that interception will afford evidence of one of the designated offences.

The offences listed in (1) capture activities that may be very far removed from the causing of actual harm. Sections 83.02-83.04 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 83.18-83.23 prohibit, *inter alia*, various forms of secondary participation in terrorist offences, including participating 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 or

---

[61] *Criminal Code*, ss. 185(1.1), 186(1.1).

[62] *Criminal Code*, s. 2.

[63] 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; See also *R. v. Terezakis*, 2007 BCCA 384 (upholding constitutionality of s. 467.13); *R. v. Lindsay*, 182 C.C.C. (3d) 301 (Ont. S.C.J.) (upholding the constitutionality of s. 467.12).

[64] See Whitling, *supra* note 60 at 118-19.

contributing[65] 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.[66] Similarly, a person may be convicted of facilitating a terrorist activity 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.[67]

The scope of the offences in (2) and (3) both hinge on the *Code*'s definition of "terrorist activity."[68] This definition is also expansive and includes any act or omission committed with the intention to intimidate the public with respect to its security (including "economic security"[69]) or to "compel a person, government or ... organization to do or to refrain from doing any act,"[70] 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."[71] 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 may attach only to indictable federal offences. Such offences include, however, all "hybrid" offences that may prosecuted (at the prosecution's election) by way of summary conviction or indictment.[72] These include a number of less serious offences, such as mischief,[73] theft under $5,000,[74] and common assault.[75]

---

[65] 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. *Criminal Code*, s. 83.18(3).

[66] *Criminal Code*, s. 83.18(2).

[67] *Criminal Code*, s. 83.19. For criticism of this provision, see Kent Roach, "Terrorism Offences and the *Charter*: A Comment on *R. v. Khawaja*" (2007) 11 Can. Crim. L. Rev. 271 at 285-86.

[68] 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*, s. 83.01(1).

[69] The inherent vagueness of this phrase is highlighted in Roach *supra* note 67 at 283-84.

[70] As Kent Roach has noted, "it is a stretch to define terrorism to include attempts to compel individuals or corporations to act." Roach, *supra* note 67 at 298.

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

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

[73] *Criminal Code*, s. 430(3).

[74] *Criminal Code*, s. 334(*b*)

[75] *Criminal Code*, s. 266.

By adding various forms of inchoate and secondary liability to the list, category (4) further expands the breadth of activity exempted from the investigative necessity requirement.[76] As discussed, many of the offences in categories (1) to (3) already prohibit acts that may only be dimly, potentially, or indirectly related to the causing of serious harm. Coupling these offences with inchoate liability threatens to capture conduct carrying an even more negligible risk of harm.[77]

My point is not to question either the wisdom or constitutionality of these offences.[78] It is simply to show that the investigative necessity exemption applies to a great deal of low level or even marginal criminal activity.[79] Consequently, if section 8 does not require investigative necessity for terrorism offences, then it is likely not required for any offence. The question is thus squarely raised: does the terrorism offence investigative necessity exemption violate section 8 of the *Charter*?

---

[76] 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.

[77] As Kent Roach has noted, in the absence of express statutory language to the contrary, the courts have been reluctant to recognize "inchoate forms of inchoate liability." Roach, *supra* note 67 at 284 n.33. See also *R v. Déry*, [2006] 2 S.C.R. 669 (refusing to recognize offence of attempted conspiracy).

[78] For commentary on these issues, see Roach, *supra* note 67; Kent Roach, "The New Terrorism Offences in Canadian Criminal Law" in David Daubney *et al.*, eds., *Terrorism, Law and Democracy: How is Canada Changing Following September 11?* (Montreal: Editions Themis, 2002) XX; Kent Roach, "The New Terrorism Offences and the Criminal Law" in Ronald J. Daniels, Patrick Macklem and Kent Roach, ed. *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 151 [Roach, New Terrorist Offences]; Webb, *supra* note 76 at 61-9; Stanley Cohen, "Safeguards in and Justifications for Canada's New *Anti-terrorism Act* (2002-2003) 14 N.J.C.L. 99 at XXX-XXX. See also generally, Kent Roach, *September 11: Consequences for Canada* (Montreal: McGill-Queen's University Press, 2003).

In *R. v. Khawaja* (2006) 214 C.C.C. (3d) 399 (Ont. S.C.J.), leave to appeal to S.C.C. refused, (2007) 233 O.A.C. 395 (note), 368 N.R. 400 (note), 153 C.R.R. (2d) 374 (note), the court rejected a variety of constitutional challenges to these provisions. It did strike down the requirement, set out in the definition of "terrorist activity," to prove that the act was committed "in whole or in part for a political, religious or ideological purpose, objective or cause." *Criminal Code*, s. 83.01(1)(*b*)(i)(A). Perhaps ironically, to the extent that other courts adopt this holding, this remedy may make it easier for the prosecution to obtain convictions in terrorism cases.

[79] Note as well that with the passage of the *Anti-terrorism Act*, all of the terrorism offences were added to the list of offences eligible for third party surveillance. *Criminal Code*, s. 183. As a consequence, many low-level offences that are not generally not eligible for interception may be intercepted if they are believed to be connected to terrorism.

In my view, it does. While courts should be reluctant to overturn the legislature's judgment of the reasonableness of an investigative power, there are two reasons why they should do so in this case. The first reason, already discussed, is that the means that Parliament has chosen to achieve its objective (combating the concededly substantial threat of terrorist violence[80]) are so patently overbroad.

The second is that Parliament's decision to eliminate the investigative necessity requirement has a disproportionately negative impact on racial, ethnic, and religious minorities: persons who are or appear to be Muslims or Arabs. As I have argued elsewhere, when a legislature enacts a measure that invades individuals' privacy in a roughly equitable way, or when such a measure disproportionately (and negatively) affects politically powerful segments of society,[81] courts should be very wary of intervening, even if the measure (in the courts' view) is undesirable.[82] In such cases the matter should often be left to the usual political process to sort out.

Where the measure is more likely to act to the detriment of groups whose interests are unfairly discounted in that process, courts have more reason to intervene. There is ample evidence that, in the realm of national security and counter-terrorism, intrusive surveillance powers are likely be deployed against Muslim and Arab Canadians.[83] This kind of profiling may have a variety of

---

[80] See generally *Application Under s. 83.28 of the Criminal Code, Re*, [2004] 2 S.C.R. 248 at para. 40 ("We conclude that the purpose of the [*Anti-terrorism Act*] is the prosecution and prevention of terrorism offences.").

[81] This is arguably the case for intrusions in the realm of digital and electronic privacy, which disproportionately affect relatively wealthy and well educated users of advanced technologies. See Penney, *supra* note 37.

[82] Other factors may influence the degree of deference that courts should give to legislatures in section 8 cases, including the relative knowledge, information, and experience that the two bodies have with the issue in question. See Penney, *supra* note 37. As both Parliament and the courts have expertise and experience in the realm of electronic surveillance (and in particular on the question of investigative necessity), in this case this factor does not strongly favour either deference or non-deference.

[83] See *Khawaja*, *supra* note 78 at para. 53; Kent Roach, "Ten Ways to Improve Canadian Anti-Terrorism Law" (2006) 51 Crim. L.Q. 102 at 122-23 [Roach, Ten Ways]; Kent Roach, "The Three Year Review of Canada's Anti-Terrorism Act: The Need for Greater Restraint and Fairness, Non-Discrimination and Special Advocates" (2005) 54 U.N.B.L.J. 308 at 322-26; Webb, *supra* note 76 at 70-1; Canadian Council on American-Islamic Relations, *Presumption of Guilt: A National Survey on Security Visitations of Canadian Muslims* (2005); Teem Bahdi, "No Exit: Racial Profiling and Canada's War Against Terrorism" (2003) 41 Osgoode Hall L.J. 293. See also generally Kent Roach and Sujit Choudhry, "Racial and Ethnic Profiling: Statutory Definition, Constitutional Remedies and

pernicious effects, including the alienation and radicalization of targeted persons who are entirely innocent of any criminal or terrorist involvement.

The investigative necessity requirement can help to minimizing discriminatory profiling by ensuring that one the most intrusive investigative powers is deployed only when there is no reasonable alternative. Properly applied, it should not prevent investigators from using conducting electronic surveillance of truly dangerous targets. But it should diminish the frequency of the kind of widespread, stereotype-fuelled surveillance that may cause law-abiding Canadians to distrust the authorities and feel unwanted in their own country. As a consequence, the courts should rule that the reference to terrorism offences in sections 185(1.1) and 186(1.1) of the *Criminal Code* violates section 8 of the *Charter*.[84]

The other terrorism exemptions in Part VI – the extension of the maximum surveillance period nor the elimination of need to show a "continuing" investigation to obtain an extension of the notice requirement – are less likely to be found to infringe section 8.[85] The time period extension is likely to increase the quantity (and hence intrusiveness) of terrorism-related surveillance. In theory, the maximum surveillance period is just that – a maximum. The issuing judge is still required to determine the proper length of the surveillance based on a consideration of all the relevant circumstances.[86] There is a danger, however, that in practice, however, the maximum will become the norm, as it has in cases governed by the ordinary time period.[87] Nevertheless, if and when the Supreme

---

Democratic Accountability" (2003) 41 Osgoode Hall L.J. 1; Don Stuart, "Avoiding Myths and Challenging Minister Cotler to Undo the Injustices of Our Anti-Terrorism Laws" (2006) 51 Crim. L.Q. 11 at 22-26.

[84] Many comparable jurisdictions have imposed investigative necessity as a statutory or super-statutory precondition of electronic surveillance. 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); *Klass v. Federal Republic of Germany* (1978) 2 E.H.R.R. 214. As discussed *infra* notes XX-XX, investigative necessity is also a prerequisite to interception under the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, s. 21(2)(*b*) [*CSIS Act*]. Presumably, many such intercepts are conducted in terrorism investigations. There is no evidence that this prerequisite has hampered these investigations; it is difficult to see why this would be different in the *Criminal Code* context.

[85] The time period extension was upheld in *Doiron*, *supra* note 57.

[86] *Doiron* (Q.B.), *supra* note 57 at para. 48. Recall as well that authorizations for both exempted and non-exempted offences are renewable in any case. *Criminal Code*, s. 186(6).

[87] See Hubbard, Brauti and Fenton, *supra* note 16 § 3.7.9.

Court of Canada deals with this issue, it is much more likely to stress to authorizing judges the importance of critically assessing the justification for a longer time period than it is to strike down the provision as unconstitutional.[88]

The notice exemption is even less likely to be declared unconstitutional. As mentioned, this provision exempts investigators seeking to delay notifying targets of expired authorizations that their communications were intercepted from the usual requirement to show that the investigation is "continuing."[89] Though its rationale is obscure, this exemption is of little consequence, since investigators must still demonstrate in such cases that the "interests of justice" warrant the delay. It is difficult to imagine what such a demonstration could entail, other than showing that notification would compromise an ongoing investigation.[90]

CSIS SEARCH AND SURVEILLANCE POWERS

Context and legislation

Parliament has also given electronic communications surveillance and other search powers to CSIS, Canada's foreign intelligence and national security agency. Created in 1984[91] in the aftermath of the McDonald Report, which detailed abuse and incompetence in the RCMP's national security services,[92] CSIS is a civilian agency with no powers relating to arrest, the laying of charges, or the use of force. Its purpose is to gather and analyze intelligence relating to "threats to the security of Canada."[93] These threats are defined in the agency's enabling

---

[88] 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.).

[89] See *Criminal Code*, ss. 185(2)-(3), 196 and discussion *supra* note 35.

[90] See Hubbard, Brauti and Fenton, *supra* note 16 § 3.11.5.1.

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

[92] See also *Atwal v. Canada*, [1988] 1 F.C. 107 at XXX-XXX (para. 45) (C.A.).

[93] As mentioned, this information may be passed along 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."

statute to mean:

> (*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*).[94]

To facilitate the collection of intelligence on these threats, the *CSIS Act* authorizes investigators to "intercept any communication or obtain any information, record, document or thing."[95] To this end, they may "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."[96]

The exercise of these powers, however, must be specifically authorized by a warrant.[97] In many respects, the privacy protections attaching to the warrant

---

[94] *CSIS Act*, s. 2.

[95] *CSIS Act*, s. 21(3).

[96] *Ibid*.

[97] Precursor, s. 16 official secrets act; McDonald recommendation for judicial approval RCMP and National at 18. In addition to the limitations that the *CSIS Act* imposes on the use of these search and seizure powers, the agency is under a general duty not to collect any information or intelligence unless it has reasonable grounds to suspect a "threat to the security of Canada."

procedure are at least as robust as those found in the *Criminal Code*.[98] For example, warrant applications must receive ministerial approval,[99] be made by certain designated officials and be heard by a federally appointed judge.[100] Most notably, the *CSIS Act* requires applicants to demonstrate investigative necessity for *all* warrants, including the equivalent of ordinary search warrants.[101] There is no exception for terrorism investigations.

In other respects, the *CSIS Act* offers less protection than the *Code*. Several of the provisions in Part VI of the *Code*, such as the punishments for unlawful interception, duty to inform targets, non-disclosure obligations, and annual reporting requirement, do not apply to CSIS intercepts.[102] CSIS warrants, moreover, may authorize interception for up to one year for most types of investigations; though as we have seen this is also now the case for criminal organization and terrorism investigations under the *Criminal Code*.[103]

The most important difference between the two regimes, however, is that CSIS warrant applicants do not have to show that an offence has been committed or 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."[104]

Constitutionality

CSIS Act, s. 12.

[98] See *CSIS Act*, ss. 21(2) and (4).

[99] *CSIS Act*, s. 21(1).

[100] The applicant must be either the Director of CSIS or an employee designated by the Minister. *CSIS Act*, ss. 21. The judge must be a judge of the Federal Court of Canada who is designated to hear CSIS warrant applications by the Chief Justice of that court.

[101] *CSIS Act*, s. 21(2)(*b*) and 21(3) (demonstration that "other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under [s. 16(a)] would not be obtained").

[102] See *CSIS Act*, s. 26 (specifying that Part VI of the *Criminal Code* does not apply to authorized CSIS intercepts).

[103]

[104] *CSIS Act*, s. 21(1).

On its face, this provision does not meet the default standard for compliance with section 8 of the *Charter*. As Justice Dickson (as he then was) put it in *Hunter v. Southam Inc*., probable cause "to believe that an offence has been committed and that there is evidence to be found at the place of the search, constitutes the minimum standard, consistent with s. 8 of the *Charter*, for authorizing search and seizure."[105]

The Supreme Court has since recognized of a broad array of circumstances, however, in which a search or seizure may be "reasonable" under section 8 without adhering to this standard.[106] This is particularly true outside the realm of the ordinary criminal investigative process, for instance in the context of regulatory investigations,[107] institutional discipline,[108] and border crossings.[109] In such cases, the Court has stressed, a compelling state interest other than law enforcement coupled with a diminished privacy expectation may justify warrantless searches as well as searches based on standards lower than reasonable and probable grounds.

The compelling state interest inhering in the *CSIS Act*, of course, is national security. This interest was specifically mentioned in *Hunter v. Southam Inc.* as one that might justify the use of a different standard.[110] In the only decision to date to fully consider the question, the Federal Court of Appeal seized upon this *dictum* in upholding the *CSIS Act* warrant provisions under section 8 of the *Charter*.[111] "The *Code* contemplates interception as an investigative tool after or during the

---

[105] *Supra* note 19 at 168.

[106] See generally ...

[107] See *e.g. Thomson Newspapers* (competition); *R. v. McKinlay Transport Ltd*., [1990] 1 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; Comite paritaire de l'industrie de la chemise v. Selection Milton*, [1994] 2 S.C.R. 406 at 422-23 (employment standards).

[108] See *e.g. Weatherall v. Canada (Attorney General)*, [1993] 2 S.C.R. 872 (prisons); *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393 (schools).

[109] See *e.g. R. v. Simmons*, [1988] 2 S.C.R. 495; *R. v. Monney*, [1999] 1 S.C.R. 652; *R. v. Jacques*, [1996] 3 S.C.R. 312.

[110] *Supra* note 19 at 168.

[111] *Atwal*, *supra* note 92 at 131-34. See also *Canadian Civil Liberties Assn. v. Canada (Attorney General)* (1997) 161 D.L.R. (4th) 225 at 254-57, 126 C.C.C. (3d) 257 (Ont. C.A.), leave to appeal to SCC refused [1998] S.C.C.A. No. 487 (QL) [*CCLA v. Canada*] (finding that s. 21 and other provisions of the *CSIS Act* are not facially overbroad and declining to grant public interest standing to non-profit organization challenging Act's constitutionality).

event," the court reasoned, "while the *Act* is directed primarily to gathering information in an attempt to anticipate future occurrences." Accordingly,

> [The *Act*] does not require the issuing Judge to be satisfied that an offence has been committed and that evidence thereof will be found in execution of the warrant. What the Act does authorize is the investigation of threats to the security of Canada and, *inter alia*, the collection of information respecting activities that may, on reasonable grounds, be suspected of constituting such threats. . .. [T]he Act fully satisfies, *mutatis mutandis*, the prescription of *Hunter v. Southam* as to the minimum criteria demanded by s. 8 of the legislation authorizing a search and seizure. The Judge is required to be satisfied, on reasonable and probable grounds established by sworn evidence, that a threat to the security of Canada exists and that a warrant is required to enable its investigation. In my opinion, that is an objective standard.[112]

The decision, however, was not unanimous. In his dissenting reasons, Justice Hugessen asserted that the legislation does not require CSIS to show any direct connection "between the information it is hoped to obtain from the intercepted communication and the alleged threat to the security of Canada." All that is needed, in his view, is a connection between the interception and the investigation itself. This would allow warrants targeting the communications of only innocent persons, such as the communications of intended victims of a terrorist threat or worse, those of persons who CSIS would coerce (by threatening to disclose damaging information) into become informants.[113]

Justice Hugessen's fears, in my view, are greatly exaggerated. If the words of a

---

[112] *Ibid*. The *Atwal* Court did hold, however, 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 such disclosure would be damaging to the national security interest. *Ibid*. at XX-XX. The government may also be able to assert other forms of statutory and common law privilege (such as informer or public interest privilege) to prevent disclosure. See Hubbard, Brauti and Fenton, *supra* note 16 § 12.8.1-12.8.4; *Canada Evidence Act*, R.S.C. 1985, c. C-5, ss. 37-38.16. See also *R. v. Malik [Erasure of wiretap recordings]*, 2002 BCSC 864 (negligent destruction of wiretap recording held to violate disclosure obligation under s. 7 of the *Charter*).

[113] *Ibid*.

statute can reasonably bear the construction, they must be interpreted in a way that accords with the Constitution.[114] As discussed, statutory minimization clauses are not constitutionally required, undue invasions of the privacy of non-targets may be found to violate section 8 of the *Charter*.[115] Section 8 also clothes judges with a residual discretion to refuse to issue a warrant even where the express, statutory requirements for issuance have been met.[116] In exercising this discretion, judges must strive to balance the interests of individuals in being "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."[117] In light of these principles, it stretches credulity to invalidate a warrant provision because it does not expressly forbid intrusions that would inevitably be considered to violate the *Charter*.[118]

More generally, it is difficult to imagine a warrant regime that would achieve a more sensible accommodation between privacy and security interests than the one set out in the *CSIS Act*. As the *Atwal* majority stressed, the primary function of CSIS is not to investigate and collect evidence of criminal offences. Restricting the use of search and surveillance powers to the investigation of discrete offences 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, for example, would fall within the scope of paragraph (*c*) of that definition, which would require the warrant applicant to show probable cause to believe that the intrusion is required 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."[119]

The greatest weakness of the Act is not the scope of its warrant powers, but rather its secrecy. The few reported decisions about this power suggest that

---

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

[115] S*upra* note 51.

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

[117] *Ibid*. at XXX.

[118] 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).

[119] *CSIS Act*, s. 2(c) [emphasis added]. Motive problem Roach at 295-96.

authorizing judges take their supervisory role seriously.[120] But as the Act contains no notice requirement, and as investigations rarely lead to criminal proceedings, it is difficult to know whether the process is functioning as it should.[121]

To help alleviate this problem, while at the same time accommodating the need for secrecy inevitably attaching to national security surveillance, the Act establishes two independent oversight mechanisms: an "Inspector General" and the Security Intelligence Review Committee (SIRC).[122] The constitution and functioning of these bodies is beyond the scope of this article. But as part of its responsibilities, SIRC investigates and reports on the use of warrant powers.[123] While suggestions have been made to subject CSIS to a greater degree of Parliamentary oversight,[124] the consensus of commentators is that SIRC does a reasonable job in making CSIS accountable.[125] The combination of this accountability and the Act's commitment to prior authorization on reasonable grounds, in my view, renders it compatible with section 8 of the *Charter*.[126]

CSEC SURVEILLANCE POWERS

---

[120] In addition to the cases cited *supra*, 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).

[121] See Hubbard, Brauti and Fenton, *supra* note 16 § 12.3-12.4.

[122] *CSIS Act*, ss. 29-55.

[123] 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 at http://www.sirc-csars.gc.ca/anrran/index-eng.html. See *e.g.* 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*, 52-3 (noting that 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).

[124] See Whitaker, *supra* note 123 at 144-45; Jean-Paul Brodeur, "The Invention of Outsiders: The Relationship between Operatives and Civilian Experts" in Joseph F. Fletcher, ed., *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999) 150 at 163-64.

[125] See Whitaker, *supra* note 123; Hubbard, Brauti and Fenton, *supra* note 16 § 12.4.

[126] See generally *CCLA v. Canada*, *supra* note 111 at paras. 14, 73 (taking note of SIRC's role in suggesting that the Act's warrant powers likely do not violate s. 8).

Context and legislation

The Communications Security Establishment Canada is the agency charged with collecting what was traditionally called "foreign signals intelligence." This entails the capture of electronic communications from outside Canada for the purpose of advancing the nation's interests in defence, security, and international relations. Created during World War II to capture and decode enemy communications, from its inception the CSEC has worked closely and shared intelligence with sister agencies in the United States, the United Kingdom, Australia, and New Zealand.[127] CSEC's activities were clothed in secrecy for many decades. It operated without any statutory mandate, and the government did not formally acknowledge its existence until 1983.[128] Though the issue is not free of doubt, during this period the agency was not authorized to intercept private communications within Canada.[129]

The enactment of the *Anti-terrorism Act* in 2001 changed much of this.[130] First, CSEC was given a statutory home in a new part of the *National Defence Act*.[131] Second, Parliament delineated the agency's mandate, which includes the acquisition and use of "information from the global information infrastructure[132] for the purpose of providing "foreign intelligence."[133] The legislation specifies,

---

[127] This highly secretive alliance, which grew out of an agreement (the UKUSA Agreement) signed between the participating nations in 1948, is sometimes referred to as ECHELON. The names of the participating agencies are the United States' National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB). See Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance" in Hayden B. Peake and Samuel Halpern, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (X: NIBC Press, 1994) 95-109; European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), Final A5-0264/2001 PAR 1, July 11, 2001.

[128] See Nomi Morris, "Inside Canada's Most Secret Agency" *Maclean's* 109:36 (9 February 1996) 32.

[129] Former CSE agents have alleged that before 2001, the agency often intercepted private communications in Canada. See Morris, *supra* note 128.

[130] See *Anti-Terrorism Act*, S.C. 2001, c. 41, s. 102.

[131] R.S.C. 1985, c. N-5, Part V.1.

[132] 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."

[133] Section 273.61 of the *National Defence Act* defines "foreign intelligence" to mean

however, that these activities "shall not be directed at Canadians or any person in Canada" and "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information."[134] Third, the agency was for the first time authorized to intercept private communications in Canada, but only as a by-product of intercepts directed at entities outside Canada.[135] Specifically, the Minister of National Defence[136] may authorize such intercepts in the following circumstances:

1. the "sole purpose" of the interception must be to obtain foreign intelligence; and
2. the Minister must be 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

---

"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." The 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." *Ibid*., s. 273.64. To help fulfill the former mandate, the Act also gives CSEC powers to intercept private communications in order to investigate threats to government computer systems. *Ibid*., s. 273.65(3)-(4). Discussion of these powers is beyond the scope of this article. See Hubbard, Brauti and Fenton, *supra* note 16 § 17.2.

Notably, the 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." *Ibid*., s. 273.64(1)(*c*). CSEC's role in this context is consequently limited to providing technical support to the police and CSIS in exercising their investigative powers. See Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008) at 453-54.

[134] *National Defence Act*, s. 273.64(2).

[135] No authorization is required, however, if there is no capture of communications made in Canada. 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*. *National Defence Act*, s. 273.61. See also Canada, Communications Security Establishment Commissioner, *Annual Report: 2003-2004* (Ottawa: Office of the Communications Security Establishment Commissioner, 2006) at 6.

[136] "Minister" is defined to mean "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*, s. 273.61.

> 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.[137]

Such authorizations may persist for up to one year and are renewable for further one year periods.[138] As with CSIS warrants, there is no notification requirement.

Constitutionality

As yet there are no decisions interpreting or discussing the constitutionality of these provisions. The *Charter* is unlikely to be engaged by purely foreign surveillance. Intercepts with a domestic nexus are a different matter. By definition, such intercepts invade a reasonable expectation of privacy and trigger constitutional protection. On the face of it, it is difficult to imagine that the scheme could be considered reasonable under section 8. Though it contains a number of measures designed to mitigate intrusions on Canadians' privacy, including minimization[139] and investigative necessity[140] requirements, two of the most critical elements of reasonableness outlined in the jurisprudence are missing: judicial authorization on the standard of reasonable and probable grounds. Ministerial authorization, of course, is not the equivalent of judicial authorization. As Justice Dickson explained in *Hunter v. Southam Inc.*:

> 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

---

[137] *National Defence Act*, s. 273.65. 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). It should also be noted that unlike *Criminal Code* and *CSIS Act* warrants, which must relate to particular investigations, *National Defence Act* authorizations may relate to "an activity or class of activities specified in the authorization." *Ibid*. ss. 273.65(1) and 273.65(3).

[138] *National Defence Act*, s. 273.68.

[139] See *National Defence Act*, s. 273.65(2)(*d*).

[140] See *National Defence Act*, s. 273.65(2)(*b*). See also Hubbard, Brauti and Fenton, *supra* note 16 § 17.2.

> 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.[141]

The person deciding whether to allow the intrusion, in other words, must be independent of the state's investigative machinery. The Minister of the Government, especially one responsible for the operations of the investigative agency, cannot possibly fulfill this role.[142]

To overcome this objection, the government would have to show that judicial authorization would hamper CSEC's ability to collect vital national security intelligence.[143] It is difficult to envisage how such an argument could succeed. There are good reasons to think that foreign intelligence intercepts (especially those designed to prevent catastrophic terrorist attacks) should operate under a different set of rules than criminal wiretaps. Advances in digital communications

---

[141] *Supra* note 18 at para. 32.

[142] The operations of the CSE are overseen by an independent Commissioner, who must be a former superior court judge. *Ibid*., s. 273.63. The Commissioner is obligated, *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." *Ibid*., s. 273.65(8). The current commissioner is former Supreme Court of Canada puisne justice Charles Gonthier, who was appointed in August, 2006 to replace Antonio Lamer, the former Chief Justice of Canada. In 2005-2006, the Commissioner conducted six reviews of activities carried out under ministerial authorizations: one on foreign intelligence collection and five on network security. He reported no illegal conduct, but noted that these findings were based on the Justice Department's interpretations of the governing legislation and that these interpretations are contentious. He also noted that there was a general "lack of clarity" in the documentation supporting authorization requests. See "CSE Commissioner's Report, 2005-06," *supra* note cse2006 at 9-11.

It should also be noted that the Commissioner's reviews are conducted *ex post*, *i.e.* after the expiry of the authorizations in question. See Communications Security Establishment Commissioner, *Annual Report: 2004-2005* (Ottawa: Office of the Communications Security Establishment Commissioner, 2006) at 7 ("CSE Commissioner's Report, 2004-05") <http://csec-ccst.gc.ca/ann-rpt/2004-2005/ann-rpt_e.pdf>.

[143] This was part of the argument, for example, advanced by the United States President in the aftermath of 9/11 to justify his evasion of statutory judicial warrant requirements for foreign intelligence intercepts with a domestic nexus. See James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times* (16 December, 2005) A1.

technologies, for example, may require a shift in focus from target-centred investigations to data-mining and pattern recognition-based surveillance.[144] It may be perfectly legitimate, therefore, for CSEC warrants to be granted for "an activity or class of activities specified in the authorization" as opposed to a discrete, target-centered investigation.[145] It may also be reasonable to define these activities in broad and flexible terms, so as to allow CSEC to respond quickly to changing events and collect information about potentially imminent threats. What is not reasonable, however, is to permit potentially massive invasions of Canadians' communications privacy without any degree of independent, *ex ante* oversight. As a consequence, the courts should rule that the CSEC provision in the *National Defence Act* violate section 8 of the *Charter*.[146]

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 rational analysis of risks and a commitment to preserving as many of our liberties as are compatible with our need for genuine 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

---

[144] See Orin S. Kerr, "Updating the *Foreign Intelligence Surveillance Act*" U. Chi. L. Rev. [forthcoming 2008], available at http://ssrn.com/abstract=1000398.

[145] *National Defence Act*, s. 273.65(1).

[146] See Hubbard, Brauti and Fenton, *supra* note 16 § 17.3; Forsese, *supra* note 133 at 457-58; Irwin Cotler, "Terrorism, Security and Rights: The Dilemma of Democracies" (2002-2003) 14 N.J.C.L. 13 at 45. For contrary views, see Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, Ont.: LexisNexis Butterworths, 2005) at 228-31; Canada, Communications Security Establishment Commissioner, *Annual Report: 2004-2005* (Ottawa: Office of the Communications Security Establishment Commissioner, 2005) at 9.

of a comprehensive, independent, and scholarly review of the RCMP's national security operations? To ask the question is to answer it.