The Application of Section 8 of the *Canadian Charter of Rights and Freedoms* to Searches Conducted for Purposes of National Security Intelligence

by

Mylène Bouzigon

A thesis submitted in conformity with the requirements for the degree of Master of Laws

Faculty of Law
University of Toronto

© Copyright by Mylène Bouzigon (2017)
The Application of Section 8 of the *Canadian Charter of Rights and Freedoms* to Searches Conducted for Purposes of National Security Intelligence

Mylène Bouzigon  
Master of Laws  

Faculty of Law  
University of Toronto  
2017

**Abstract**

This paper proposes an approach to the interpretation and application of section 8 of the *Canadian Charter of Rights and Freedoms* where searches by the state are effected in the course of ensuring national security, more specifically in producing national security intelligence.

Having outlined the principles developed by the courts in applying section 8, it suggests that the state’s interest in national security is one of the highest order, resulting in it weighing heavily in balancing against individuals’ privacy interests. In the course of its examination, it describes national security intelligence and criminal investigations as different paradigms, justifying different treatments. It proposes that the *Hunter v Southam* standard remains available in areas where privacy stakes are the most serious, to begin to slide toward that of reasonable suspicion at earlier points than it would in criminal matters, remaining modulated by the expectation of privacy or degree of intrusion.

*Legal counsel with the Department of Justice (Canada). The views and opinion expressed herein are those of the author and do not represent in any manner those of the Department of Justice or of the Government of Canada.*
ACKNOWLEDGMENTS

I would like to thank my thesis supervisor, Professor Kent Roach, for his advice and guidance as well as his patience through a writing process that ended up taking much longer than either of us could have anticipated.
# Table of Contents

Acknowledgements

Table of Contents

Introduction

1. The *Canadian Charter of Rights and Freedoms*  
   a. Interpreting the *Charter*  
   b. Section 8 of the *Charter* in the courts

2. National security intelligence  
   a. National security and the notion of national security intelligence  
   b. The processes of national security intelligence  
   c. Distinguishing security intelligence from criminal investigations

3. The application of the section 8 analytical framework  
   a. A contextual approach  
   b. The justifiable expectation of privacy  
   c. Impact of variations in the degree of privacy and the level of intrusiveness  
   d. Searches conducted under the CSIS Act  
   e. Accountability and publicity in the *Hunter* test  
   f. Control and review mechanisms

4. A proposed approach
Introduction

There has not been much written as of yet in Canadian law regarding the legal treatment of security intelligence. This may be because not much appears to be required: intelligence is, after all, just a form of information. It is not readily apparent that it is of such importance in our legal landscape that it deserves to stand at the center of any legal discussion or debate. Another reason may be that while national security intelligence is a subject that has come of age as an area of academic interest in the field of humanities, it may have taken more time for it to have become sufficiently contoured to sustain legal commentary in Canada.

This paper aims to remedy this, at least to a small degree. The acquisition and formulation of national security intelligence are activities that will engage rights at some point almost as a matter of course since some of the information used for these purposes is likely to have been

---

1 There are not many authors who have studied and published on legal aspects of national security intelligence in Canada. Stanley A. Cohen covered some of those aspects in Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril (Markham: LexisNexis Butterworths, 2005) [Cohen]), which was written in the wake of the events of 9/11 and the adoption of the Anti-terrorism Act, SC 2001, c 4. Professor Craig Forcese wrote a basic text book in 2007 that he is updating via his blog to which he contributes on a very regular basis (Craig Forcese, National Security Law: Canadian Practice in International Perspective (Toronto: Irwin Law, 2007); Craig Forcese, National Law (blog), online: <http://craigforcese.squarespace.com/national-security-law-blog>). Both Forcese and Professor Kent Roach have been generous contributors to the field of national security law through articles and comments on specific issues and authorship of a textbook about Bill C-51 [Craig Forcese and Kent Roach, False Security: The Radicalization of Canadian Anti-terrorism (Toronto, Irwin Law, 2015)]. Some of the issues discussed here were foregrounded in remarks of Pr. Roach in a research paper for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 [Canada, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Research Papers, Volume 4, The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence (Ottawa: Public Works and Government Services, 2010) more particularly at 116-119, [Air India Research Papers].] While I aim to provide an accurate description of the field of national security intelligence in Canada, the approach taken remains based on readings available on the practice of national security intelligence in other jurisdictions; as well as by observations made on the basis of exposure I would have had as legal counsel working alongside officers in this area.

2 Michael Herman reported in 1989 having counted in Canada 107 institutions offering 130 intelligence studies courses [Michael Herman, Intelligence Power in Peace and War (Cambridge, UK: Cambridge University Press, 1996) at 2, n 7]. This summer, in Ottawa alone, both the University of Ottawa and Carleton University are offering summer courses on security intelligence (e.g. Summer Course on Intelligence and Security, Center on Public Management and Policy, University of Ottawa; The Practical Certificate in National Security Intelligence Norman School of International Affairs in cooperation with the Center for Security, Intelligence and Defence Studies, Carleton University).
obtained by the state through forms of intrusive activities. I propose to examine national security intelligence by looking at the analytical framework that has been developed by the courts for section 8 of the *Canadian Charter of Rights and Freedoms*.³

In its seminal judgment in *Hunter v Southam*,⁴ the Supreme Court of Canada laid out the approach to be followed in assessing the constitutional validity of statutory provisions authorizing search and seizure. It did note that the relevant standard to be applied may be different where the government interest at stake is state security. *Hunter* was issued over 30 years ago and short of the *Atwal* judgments that go back to the mid-eighties and little more than an acknowledgement in a recent Federal Court of Appeal judgment in *Mahjoub* (both are discussed below) there has been little commentary since discussing how this different standard may be articulated. In this paper, I explore the nature and boundaries of the exception alluded to by the Supreme Court, to then propose a theory of application of s. 8 of the *Charter* in a national security intelligence context.

In addressing this question, I posit that national security intelligence as a discipline is sufficiently defined and concrete to support such an analysis, at least within the construct I elaborate below, although I would also suggest that the question of the different formulation of an analytical framework for s. 8 of the *Charter* in such a context could be studied as a matter of theoretical interest.

I first set out the current analytical framework for the *Charter* and s. 8 of the *Charter*, focussing on factors and elements that are relevant to the proposal of a constitutional justification that would apply in the national security intelligence context. I then describe national security intelligence and related concepts for the purpose of my analysis. Throughout and at the end, I propose elements for that justification.

1. **The Canadian Charter of Rights and Freedoms**

a. Interpreting the Charter

In our legal history, the Canadian Charter of Rights and Freedoms remains the most important legislative step in incorporating rights and freedoms in the fabric of our society and providing a constitutional recognition and effect to these fundamental rights. It is the bulwark solidifying the main safeguards of our civil liberties. Section 8 of the Charter, situated among provisions on legal rights, sets out a guarantee for everyone to be free from unreasonable search and seizure effected by the state. It has to stand among those rights of the Charter that are most regularly invoked in the course of legal proceedings. This gives us a rich interpretive landscape, relevant parts of which will be reviewed below.⁵

The principles governing the interpretation of the Charter will be relevant to our discussion. In 1985, in R v Big M Drug Mart Ltd, the Supreme Court commented on principles relevant to determine the meaning of rights and freedoms guaranteed by the Charter. Dickson C. J. referred to the basic approach elaborated in Hunter: the meaning of a right and freedom guaranteed by the Charter is to be ascertained by the analysis of the purpose of the guarantee.⁶ He also elaborated on a point he had made there to the effect that the provisions of the Charter must be capable of growth and development over time to meet new social, political and historical realities.⁷ At the same time, the Court has emphasized the importance of considering the context in which a Charter right is invoked when interpreting it. This was discussed in R v Wholesale Travel, notably by referring to reasons of Wilson J. in a previous matter:

In Edmonton Journal v Alberta (Attorney General), Wilson J. stressed the importance of a contextual approach to Charter interpretation. She recognized that a particular right or freedom may have a different meaning depending upon the context in which it is asserted. She put her position this way, at pp. 1355-56:

One virtue of the contextual approach, it seems to me, is that it recognizes that a particular right or freedom may have a different value depending on the context.... The contextual approach attempts to bring into sharp relief the aspect of the right or freedom

---

⁵ The jurisprudence originating from the Supreme Court of Canada on the interpretation and application of the Charter is extensive. As a result, save for a few exceptions, all decisions referred to herein are originating from that Court and the references to “the Court” should be understood as referring to it.


⁷ Ibid at 117.
which is truly at stake in the case as well as the relevant aspects of any values in competition with it. It seems to be more sensitive to the reality of the dilemma posed by the particular facts and therefore more conducive to finding a fair and just compromise between the two competing values under s. 1.

It is my view that a right or freedom may have different meanings in different contexts.... It seems entirely probable that the value to be attached to it in different contexts for the purpose of the balancing under s. 1 might also be different. It is for this reason that I believe that the importance of the right or freedom must be assessed in context rather than in the abstract and that its purpose must be ascertained in context. This having been done, the right or freedom must then, in accordance with the dictates of this Court, be given a generous interpretation aimed at fulfilling that purpose and securing for the individual the full benefit of the guarantee. . . .

It is now clear that the Charter is to be interpreted in light of the context in which the claim arises. Context is relevant both with respect to the delineation of the meaning and scope of Charter rights, as well as to the determination of the balance to be struck between individual rights and the interests of society. [citation omitted]

In McKinlay Transport, Wilson J. comments that flexibility is also key to interpreting the Charter and that it would be wrong to apply a rigid approach to one of its particular provisions since it must be capable of application in a vast variety of legislative schemes. This was one of the early cases examining the application of section 8 of the Charter in a regulatory context. In Wholesale Travel this approach led the Court to comment that a Charter right ‘may have different scope and implications in a regulatory context than in a truly criminal one’. The Court also noted that:

Under the contextual approach, constitutional standards developed in the criminal context cannot be applied automatically to regulatory offences. Rather, the content of the Charter right must be determined only after an examination of all relevant factors and in light of the essential differences between the two classes of prohibited activity.”

I propose an application of the Charter that is premised on a specific context: state activities directed to the safeguarding of national security. As the Court noted in its decision in Charkaoui

---

10 Supra note 8 at para 150.
11 Ibid at para 151.
1. meeting national security responsibilities in no way obviate the necessity for the government to act accountably and in conformity with the Constitution: “These two propositions describe a tension that lies at the heart of modern democratic governance. It is a tension that must be resolved in a way that respects the imperatives both of security and of accountable constitutional governance.”

Within this context then, we will focus more precisely on the production of national security intelligence.

b. **Section 8 of the Charter in the courts**

Section 8 provides protection against unreasonable intrusion in privacy by the state. It establishes a fundamental right to it. At the same time, it does not set privacy as an absolute constitutional right. The possible scope of the protection granted by s. 8 is narrowed by defining the protection as applying against ‘unreasonable’ search and seizure. As set out in Edwards: “[t]here are two distinct questions which must be answered in any s. 8 challenges. The first is whether the accused had a reasonable expectation of privacy. The second is whether the search was an unreasonable intrusion on that right of privacy”.

In interpreting s. 8 since its inception, the Courts have elaborated an analytical framework that now turns, in great part, on the determination of the reasonableness of a search.

The Supreme Court of Canada first examined the application of s. 8 in 1984, in the matter of Hunter. Two days after the proclamation of the Constitution Act, 1982 incorporating the Charter, investigative officers attended the premises of the Edmonton Journal belonging to Southam Inc. They were acting under the power of an authorization to enter issued by A.W. Hunter, Director of the Investigation and Research of the Combines Investigation Branch, and certified by the Restrictive Trade Practices Commission, all as per s. 10 of the Combines Investigation Act, allowing them to examine documents and other things on the premises. Hunter arose out of a challenge to the constitutionality of s. 10 in the light of s. 8 of the Charter.

---

12 The Court was seized of questions related to procedural requirement arising out of the application of s. 7 of the Charter. Charkaoui v Canada (Citizenship and Immigration), 2007 SCC 9, [2007] 1 SCR 350 at 1 [Charkaoui I].


14 Supra note 4.
Dickson J., speaking for the Court, rapidly moved to the issue of the meaning to be given to the term “unreasonable” that frames the guarantee in s. 8, rendering it, in his words, ‘vague and open’. Deploring the frugality of the constitutional text, he remarked that “(t)here is no specificity in the section beyond the bare guarantee of freedom from “unreasonable” search and seizure; nor is there any particular historical, political or philosophic context capable of providing an obvious gloss on the meaning of the guarantee”. Examining the purpose underlying s. 8, he concluded that the protection of s. 8 goes at least as far as protecting the right of privacy.

Having concluded earlier that an assessment of the constitutionality of a search -- or statutory provision authorizing same -- must focus on its “reasonable” or “unreasonable” impact on the subject of the search (and not simply on its rationality in furthering some valid government objective), he explains:

… The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation (…) , whether it is expressed negatively as a freedom from ‘unreasonable’ search and seizure, or positively as an entitlement to a ‘reasonable’ expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public’s interest in being left alone by government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals, notably those of law enforcement.

In making that assessment:

The location of the constitutional balance between a justifiable expectation of privacy and the legitimate need of the state cannot depend on the subjective appreciation of individual adjudicators. Some objective standard must be established.

---

15 Ibid at 154.
16 “It is first necessary to specify the purpose underlying s 8: in other words to delineate the nature of the interests it is meant to protect”, as per the purposive approach set out in Big M and outlined above.
17 Supra note 4 at 158-159.
18 Ibid at 157.
19 Ibid at 159-160.
20 Ibid at 166.
As to the standard, having rejected that of holding a reasonable belief that information may be uncovered in a search (which was provided for in s. 10 of the *Combines Investigation Act*), he adopts a higher threshold, commenting in an oft quoted passage:

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. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement.

And then:

Where the state’s interest is not simply law enforcement as, for instance, where state security is involved, or where the individual’s interest is not simply his expectation of privacy as, for instance when the search threatens his bodily integrity, the relevant standard might well be a different one.21 [*emphasis added*]

Thus, Dickson J. clearly considered that the approach he had set would need to be modulated on the basis of factors related to the nature of the state interests at issue, and felt it appropriate to use state security as an example warranting a different standard, at a time where the Court’s *Charter* activism was at its height.22 He was explicitly particularizing the approach to the case before him when he summed it up by stating that the minimum standard consistent with s. 8 for authorizing a search required showing that there was reasonable and probable grounds established upon oath, that an offence was committed and that evidence would be found at the place of the search.23 As to when this would be done, the Court held that the purposes of s. 8 mandated that it be used to prevent unjustified searches before they happen, which required a system of prior authorization.24 Where it would not be reasonable to insist on prior authorization, the search would be presumed unreasonable and the onus to justify the constitutional validity of a search, on the balance of probabilities, would fall upon the state.25 In *Collins*, the Court would establish that to be shown to be reasonable, a warrantless search must be authorized by law, the law itself must be reasonable and the manner in which the search was carried out must be reasonable as well.26

---

22 This remark was inspired by a comment made by Professor Roach.
23 *Supra* note 4 at 168.
24 *Ibid* at 160.
26 *Collins, supra* note 25 at para 23.
Occasions in which the courts have sought to apply these principles in relation to intrusive powers granted to intelligence agencies remain rare. This first arose in 1987 in the matter of *Atwal* in the Federal Court and Federal Court of Appeal. As is described more fully below, the Court of Appeal transported the *Hunter* standard to the context of security intelligence, that of issuance of warrants under the *Canadian Security Intelligence Service Act*. In doing so, the Court provided a practical application of the principles set by Dickson J. The Court of Appeal recently affirmed that earlier decision in *Mahjoub*.  

2. **National Security Intelligence**

   a. National security and the notion of national security intelligence

In developing elements of an analytical framework that would apply to national security intelligence, it is necessary to explain what I mean by that expression. This will also serve to distinguish it from other contexts, principally criminal law, in which the courts have applied s. 8 of the *Charter* and built the framework over time. Also, it is not an area that is well known and one where, in my experience in interacting with other legal practitioners, erroneous assumptions abound.

National security, while often referred to, is not defined precisely. The Honourable Justice Simon Noël summed it up by stating that “‘national security’ means, at a minimum, the preservation of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms in Canada.” The security of Canada, the capacity to maintain our society and its values, to foster the environment that allows those values to flourish stands as an

---

27 *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [CSIS Act].
28 *Mahjoub v. Canada (Minister of Citizenship and Immigration)*, 2017 FCA 157, 2017 FCJ No 726 at para 175-178 [*Mahjoub*].
29 For the purpose of this paper, I am not discussing the mandate and role of the Canadian armed forces. While there is no doubt that military activities do include intelligence functions and play an important role in national security, they are governed by a set of rules and principles that depend in large part on international law and royal prerogative. How these military activities interact with the *Charter* and the issues that these activities raise are, for the most part, quite different.
30 *Attorney General v Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar*, 2007 FC 766 at para 68. This was a decision on a matter arising under s. 38 of the *Canada Evidence Act* relating to the *Arar Commission of Inquiry*. 

8
important interest; a point that Dickson J. would likely have assumed when he used it to illustrate his point in *Hunter*.

This corresponds to the conclusion of Stanley Cohen, as he wrote about ‘national security’:

> The security of the nation depends on the ability of the state to take measures to protect the national interest, conduct its national defence or in the power to enact laws to ensure the “peace, order and good government” of Canada. “National security” is arguably the most important justification that can be advanced in support of legislation, springing, as it does, from the necessity to safeguard and preserve the very existence of the state and its democratic institutions and ensure their continued survival. [footnote omitted]

In pursuing security of the country, the federal government will be preoccupied with a range of matters, some more immediate than others. In 2014, in a statement before the Standing Senate Committee on National Security and Defence, talking from his vantage point as national security advisor to the Prime Minister, Stephen Rigby, provided an illustrative description of the issues he saw as pertaining to the security of Canada:

> "National security" can no longer be considered in any narrow sense of the term in association with specific threats within Canada or even at our borders. To speak of national security today is to address a multitude of issues that are complex, interconnected and in constant evolution. Increasingly, Canada's national security interests are manifest in a broad range of foreign policy and defence imperatives…

The terrorist threat in particular has undergone noteworthy changes in recent years. (...) 

---

31 Cohen, *supra* note 1 at 155.

32 Under our constitutional system, the Prime Minister is responsible for ensuring the security of Canada, a role described as fundamental by the *Commission of Inquiry into the investigation of the Bombing of Air India flight 182*. [Canada, Commission of Inquiry into the investigation of the Bombing of Air India flight 182, *Air India Flight 182: A Canadian Tragedy*, vol 3 (Ottawa: Public Works and Government Services Canada, 2010) at 18-19 [Air India Commission, v3]. The Prime Minister discharges this mandate with the support of the National Security Advisor (NSA), a senior government official occupying a position within the Privy Council Office (PCO). The role of the NSA is to coordinate activities in government relating to national security. The NSA does not have formal powers, nor is the position described in legislation. (An exception is the mention of the Office of the National Security Advisor to the Prime Minister in the schedule to the *Security of Information Act*, RSC 1985, c O-5; the organizational chart and the functions of the NSA’s three Secretariats can be found in PCO’s website, online: <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=org&doc=text_e.htm> and <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=secretariats#XV>, respectively, retrieved on August 27, 2017.) Yet, the role is pivotal in its capacity to integrate information from diverse points within the government for the purpose of discussions at cabinet committees, and decision-making by the Prime Minister.
Changes at the geopolitical level have an impact on the threat context that Canada faces. Our security interests vary from region to region and are often multifaceted. The number and the complexity of crises around the world is challenging for Canada and its allies.

In the Asia-Pacific region, economic and security interests are increasingly intertwined for all actors. Regional instability in South Asia creates significant risks. North Korea is a specific state source of regional tension through its unpredictability and possession of weapons of mass destruction.

If we look to the Middle East, we see that regional instability threatens our friends and us. At this time, we are witnesses to an unprecedented humanitarian crisis in Syria that is only getting worse. Terrorists from other locales are moving in to use the country as a training ground, while refugees spill over into neighbouring countries that have struggled to absorb them, and the threat of regional instability grows.

Closer to home, weak governance and crime threaten Canadian interests in our hemisphere. History shows that any serious humanitarian event, natural disaster or security incident may see calls for Canadian support, especially from our military, police, correctional services and/or for asylum support, given people-to-people ties, global burden-sharing responsibilities and our strong record of ongoing engagement. (...). 33

The importance of the state’s objective to ensure and maintain national security was recognized by the Supreme Court of Canada in Charkaoui 1 where it began its decision by stating that one of the most fundamental responsibilities of a government is to ensure the security of its citizens. 34 Later on, in applying section 1 of the Charter, the Court found that the protection of Canada’s national security (and related intelligence sources) “undoubtedly constitutes a pressing and substantial objective.” 35

33 Canada, Standing Senate Committee on National Security and Defence, Proceedings of the Standing Senate Committee on National Security and Defence: Canada’s national security and defence policies, practices, circumstances and capabilities, Issue No 2 (2 February 2014) at 2:26–2:28 (Chair: Hon Daniel Lang) [Committee on National Security]; online: <https://sencanada.ca/Content/SEN/Committee/412/secd/pdf/02issue.pdf> . Includes translated portions.
34 Supra note 12 at para 1.
35 Ibid at para 68-69. The procedure that was in place then under Immigration and Refugee Protection Act’s security certificate regime was found to fail the minimal impairment test of s. 1 of the Charter.
There appears to be no doubt that national security, and ensuring it, constitutes an appropriate element for the purpose of the *Charter*’s s. 8 balancing exercise.  

National security intelligence is one of the principal tools that governments rely upon in the pursuit of discharging that responsibility. In its 1981 report, the McDonald Commission that examined certain activities of the Royal Canadian Mounted Police (RCMP)\(^{37}\) explained security intelligence as being “…essentially advance warning and advice about activities which threaten the internal security of Canada”.\(^ {38}\)

Acknowledging that there is no universal agreement on what constitutes national security intelligence, Loch Johnson, in his book on the subject, describes it summarily as being the gathering and analysis of information, information then used by government decision makers\(^ {39}\), before proposing a broader description for the American context:

> Intelligence is the umbrella term referring to the range of activities – from planning and information collection to analysis and dissemination – conducted in secret, and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner what allows for the timely implementation of a preventive

---

\(^{36}\) A view that is foregrounded by remarks of the Court in *R v Tessling*: “At the same time, social and economic life creates competing demands. The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns. Thus s. 8 of the *Charter* accepts the validity of reasonable searches and seizures. A balance must be struck…”. *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 17 [*Tessling*].


\(^{38}\) McDonald: second Report, v1, *supra* note 37 at 414, para 5 and see also 417 at para 16. In *Suresh*, the Supreme Court of Canada found that the expression “danger to the security of Canada” as found in deportation provisions of the *IRPA* was not unconstitutionally vague. (*Suresh v Canada (Minister of Citizenship and Immigration*, 2002 SCC 1, [2002] 1 SCR 3, at para 5.)

policy or strategy, including, where deemed desirable, covert activities.40

b. The processes of security intelligence

For most of us, exposure to intelligence as a form of information is very limited. National security intelligence remains secret and not available to the general public. As is the case with the formulation of legal advice, the production of intelligence starts from facts and ends with an assessment about the state of things. But there ends the similarities. The objectives sought are different from those of legal analysis and the means to attain them have evolved differently. This is not to say that security intelligence is a world devoid of rules and principles. It is not the case but like many similar fields, it does not benefit from the wisdom and discipline instilled by this great arbiter that is the judiciary and the system it serves.

The intelligence work done in Canada is broadly driven by the intelligence requirements set by Cabinet which are then conveyed to the intelligence agencies by way of ministerial directions.41 This serves to highlight another characteristic of security intelligence work: in its control and accountability, it remains squarely within the domain of the executive.42 A number of

40 Ibid at 15; Johnson’s description is also favoured by Peter Gill, see: Peter Gill & Mark Phytian, Intelligence in an Insecure World (Cambridge, UK: Polity Press, 2006) [Gill & Phytian], at 7. Scholarship on national security intelligence appears to have known a first golden age in the United States (US) and the United Kingdom (UK) in the 1970s, described as a ‘Time of Troubles’ for the intelligence community by Michael Warner, see Michael Warner, The Rise and Fall of Intelligence: An International Security History (Washington: Georgetown University Press, 2014) at 213. The 1970’s was a period that saw the Church Committee on activities of the Central Intelligence Agency (CIA) on American soil, Watergate, British publications about defectors to the then U.S.S.R. and revelations about powers used during World War II (WWII) and then underwent a revival following the 9/11 attacks and the Iraq and Gulf wars, a point also illustrated by comments and examples by Johnson in the preface to his book, see Johnson. Indeed, most of the authors whose work I consulted for this paper had been practitioners in the field or were directly involved in management, oversight or review activities in relation to these events.
41 In testimony given on February 3, 2017 before the Committee on national security, Stephen Rigby explained: “The minister's involvement typically is focused on intelligence priorities that are established by cabinet. Cabinet meets and establishes the priorities. Those are given out individually to the security agencies in government. They are converted into ministerial directives, so they are disaggregated from a broad-brush direction for something, and you can probably guess what one or two of them might be. From there, those directives are then placed into the work plans of the individual organizations, and that is the link that would occur in terms of the minister giving direction to CSEC to pursue something.” Canada, Standing Senate Committee on National Security and Defence, Proceedings of the Standing Senate Committee on National Security and Defence: Canada's national security and defence policies, practices, circumstances and capabilities, (3 February 2014) (Chair: Hon Daniel Lang) online: <http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51162-e.HTM>.
42 Indeed, the McDonald Commission referred to the notion of ‘responsible government’ in the report that resulted in the creation of CSIS and set out the purpose security has in securing democracy: “…there must be effective procedures for ensuring that those who carry out security investigations and other security measures are accountable to Ministers of the Crown, who in turn are responsible to Parliament. Security activities of necessity involved a
departments and agencies are engaged in the production of intelligence of various types in support of the delivery of their mandates and while some will rely on national security intelligence in elaborating policy as well as in making decisions, they are not typically engaged in intrusive activities to do so. There is little information available about intelligence assessments provided to the Government of Canada although there are indications that the intelligence community is broadly distributed. Security intelligence, even if based on open sources of information is normally considered to be sensitive information. While also noting that it raises issues of morality, legality and accountability, authors agree that secrecy is an essential facet of intelligence. As will be discussed later, secrecy, of course, has an impact where we are examining intelligence from a rights perspective.

National security intelligence is the product of processes that are specific to the discipline. And where intrusive activities are carried out, in Canada they will be done under the authority of a statute. This supports a view that legal standards that should apply to the collection of information for purposes of security intelligence are applicable with respect to defined activities and purposes, done within generally accepted principles and functions.

great deal of secrecy… but it does not follow that they cannot be an open book to responsible Ministers. [McDonald: Second Report, v1, supra note 37 at 44]. In setting out the reasons supporting the establishments of a civilian service, separate from the RCMP, the McDonald Commission linked it to the implementation of structures and processes that would enable the government to direct and control the security service. At the same time, the Commission recognized the need for the new agency to be able to resist improper directions. Ibid at 794.

43 One source of assessments is the Integrated Terrorism Assessment Center (“ITAC”), a ‘fusion center’ located at CSIS. The last detailed reference to ITAC activities in the CSIS annual report, which is in the Annual Report 2007-2008, is indicative of the level of work done at that location: “ITAC issued 348 threat assessments and redistributed over 1,300 others produced by allied fusion centres. ITAC also published Media Watch each business day for distribution to clients. Further, ITAC provided over 120 briefings to its domestic clients … During the period under review, ITAC assumed responsibility for the Threat Assessment Unit, which provides time-sensitive evaluations of potential threats to Canadians and Canadian interests in Canada or abroad, or to foreign interests or nationals in Canada…” Canadian Security Intelligence Service Annual Report 2007-2008, online: <https://www.publicsafety.gc.ca/lbrr/archives/cn24357-2007-2008-eng.pdf>, retrieved August 27, 2017.


45 The term “intelligence” itself is susceptible to different uses. For instance, Lowenthal, supra note 44, uses the term “intelligence” to refer to processes, to products and to organizations, indicating he uses them all in his scholarship, at 9. In this paper, however, the term “intelligence” is used to refer to the end product.
Intelligence analysis can be either short term in outlook and precise in content or strategic, providing longer term assessments or covering broader territory. As described by David Omand in his book ‘Securing the State’: “Good intelligence assessment has explanatory value in helping deepen real understanding of how a situation has arisen, the dynamics between the parties and what the motivations of the actors are likely to be.” Omand goes on to state that “[it] has an operational purpose to help government secure its objectives, it has to tell governments what they do not know, and perhaps what they would rather not have to know, about approaching threats.” As was also descriptively stated: “It is the role of intelligence to extract certainty from uncertainty and to facilitate coherent decision in an incoherent environment.”

Perhaps one of the most distinctive characteristics of intelligence is that it admits of failure. While assessments of reliability are required, accuracy is not the ultimate objective. This is well illustrated in a statement by General Michael Hayden, then head of National Security

---

46 They are distinguished as follows in a description of intelligence provided to the Government of Canada that was contained in the 2011-2013 CSIS Annual Report: “Raw intelligence reporting is disseminated in order to provide a snapshot of a threat-related issue. This is different from a threat assessment, which typically offers a synopsis of the immediate situation. Both raw intelligence reporting and threat assessments are designed to answer short-term questions. There is, however, a need for in-depth assessments that contextualize the issue and tell the reader why it is significant for Canada. These are strategic intelligence assessments, which draw upon CSIS reporting, foreign agency information and open-source material and serve to provide government officials with a holistic picture of the threat and its potential consequences for Canada. Strategic intelligence assessments not only answer questions about what happened yesterday but they also throw light on what might happen in the coming weeks or months – and what that might mean for Canada’s national security. Strategic intelligence assessments play a key role in identifying emerging trends and, in some cases, linking those trends or actors to recent events in Canada or abroad. …”. Canadian Security Intelligence Service Annual Report 2011-2013, online: <https://www.csis-scrs.gc.ca/pblctns/nlrprt/2011-2013/index-en.php?=undefined&wbdisable=true>, retrieved August 27, 2017.
47 Supra note 44 at 25.
48 Ibid at 24-27. Omand explains that at the operational level, the demand is for timely all-source analysis to support operational decision-making by providing a level of detail that will supplement knowledge of recipients. He provides examples, which could be similar to decisions to be made in Canada, including decisions on allocation of security and intelligence resources in face of conflicting demands, what advice to provide to travellers overseas, how to respond to a terrorist threat to an embassy overseas, implications of high tech weaponry reaching a country of concern, whether a particular export should be permitted, additional protective measures taken at a big public event or what passengers should be allowed to board an airplane. He also provides examples of use at the tactical level: tactical decisions being made within policy frameworks by front line security, law enforcement, military forces where the raw information may be used by intelligence specialists.
50 Lowenthal, supra note 44 at 158-159. He also addresses the question of what defines good intelligence by setting out what qualities it should bear: timely, tailored, digestible, clear regarding the known and the unknown and overall, objective, which he describes as overtaking all others. At 157, 158.
Administration: “If it were a fact, it would not be intelligence”\textsuperscript{51}. The point is also made by Joshua Rovner in his book devoted to the analysis phase of the intelligence cycle when he describes intelligence assessments by citing an (unnamed) long time CIA official:

\begin{quote}
Unlike economic and statistical data derived from hard fact, intelligence materials are based on reports of varying levels of certainty and reliability. Some reports will bear no more than the weight of a wispy guess, others can support an army tank or a national policy. Only someone who works with this material every day has the knowledge to see this clearly and use the data wisely.\textsuperscript{52}
\end{quote}

Intelligence then, for our purposes, is information generated about and in support of national security and it is an essential tool to ensure and maintain security of Canadians. It is produced to guide policy, select courses of action and make decisions. The information is derived from facts that undergo processing and exploitation, combined with observations, opinions and experience. Security intelligence is also security-based which brings it within the description proposed by Johnson: “knowledge, ideally, foreknowledge, sought by nations in response to external threats and to protect their vital interests, especially the well-being of their people”\textsuperscript{53}. And, in order to produce intelligence, governments will sometimes have recourse to intrusive methods.

If we except the RCMP and enforcement arms of a number of agencies that devote their activities primarily to investigations of crimes for purposes of prosecution, there are two main organisations that hold mandates and powers to engage in intrusive activities for the purpose of providing national security intelligence to the Government of Canada: the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS or the Service).\textsuperscript{54}

\textsuperscript{51} General Michael Hayden, then head of National Security Administration, cited in Robert Jervis, \textit{Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War} (Ithaca: Cornell University Press, 2010) at 1. Not that intelligence practitioners are not intent to reduce the incidence of failures: not having prevented the 9/11 attacks and the faulty Iraq WMD intelligence being prime instances where colossal efforts were devoted to soul searching and post mortem analysis. But the point made by Richard Betts, a scholar in the field, and reiterated by others is that due to intrinsic and systemic aspects of how intelligence is generated, intelligence failures are inevitable. [Betts, \textit{supra} note 49, at 19.]

\textsuperscript{52} Joshua Rovner, \textit{Fixing the facts: National Security and the Politics of Intelligence} (Ithaca: Cornell University, 2011) at 22.

\textsuperscript{53} Johnson, \textit{supra} note 39 at 365, cited in Gill & Phytian, \textit{supra} note 40 at 6.

\textsuperscript{54} The PCO website contains an archived document, dating back to 2001, that describes the functions of the security and intelligence community within the Canadian government, see PCO, \textit{The Canadian Security and Intelligence Community: Helping Keep Canada and Canadians Safe and Secure}, online: <http://www.pco>.
The remits of CSIS and CSE are set out in statutes. They are each focussing on different facets of national security intelligence. With proper authorizations in place, both CSIS and CSE may carry out interceptions of communications and searches. We will focus here mainly on CSIS’ principal investigative powers since the fact that CSE is prohibited from directing any of its activities to Canadians or persons in the country would create other limitations to the application of section 8. CSIS offers a good backdrop against which to study these issues.

c. Distinguishing security intelligence from criminal investigations

National security intelligence functions, in our system, are not law enforcement activities. It is necessary to distinguish intelligence and intelligence investigations from criminal investigations for a number of reasons. First, as explained in more detail below, criminal prosecutions set the high watermark in terms of s. 8 Charter standards. This will also be relevant because the bulk of legal developments and judicial pronouncements concerning the protection conferred by s. 8 of the Charter occurred in the course of criminal prosecutions. Finally, the tack adopted by the courts, practitioners and academia in examining issues of privacy in the national security intelligence context has frequently been to revert to criminal law, using it as the frame of reference against which the constitutional validity of actions taken by the government is assessed. Within these exercises, deviations from criminal law processes have often been seen as aberrations that needed to be made to fit within the mold or to be found deficient rather than as a manifestation that a change of paradigm may be required, which is what I am proposing here.

For instance, in the reasons issued in the matter of Harkat, the Supreme Court of Canada based its finding that police informer class privilege should not be extended to CSIS intelligence human
sources by looking at the matter mainly from a criminal law lens (and then finding that CSIS fell short.)

In its work, the McDonald Commission started from terms of reference focussed on investigative practices and activities involving members of the RCMP that were not authorized or provided for by law. It concluded that separating law enforcement from the collection of information about threats to the security of Canada was the best approach. This was at the origin of the split of functions between the RCMP and CSIS.

The Commission of inquiry into the Investigation of the Bombing of Air India Flight 182 commissioned a number of research papers prepared under the leadership of Professor Kent Roach. A study by Bruce Hoffman includes an examination of the role of intelligence and law enforcement in preventing terrorism. In it, he highlights some of the same fundamental differences between information gathering for intelligence and that for solving a case.

---

58 Canada (Citizenship and Immigration) v Harkat, 2014 SCC 37, [2014] 2 SCR 33. The Chief Justice’s findings and reasons on this point are primarily set out in paragraph 85. The Chief Justice briefly compares police and intelligence investigations by referring to their different purposes (collection of evidence for purposes of a trial vs global scale investigation geared towards prospectively preventing risks), adds that intelligence may be used in proceedings with varying evidentiary standards (while police evidence is used in criminal trials that incorporate significant evidentiary standards) and notes that CSIS is not constrained in using informers by the requirement to waive privilege if their information is such that they would be called as witnesses. He concludes that “the differences between traditional policing and modern intelligence gathering preclude automatically applying traditional police informer privileges to CSIS human sources”. Assuming privilege would aim to protect the informer as well as exist in recognition of the importance of preserving access to human sources for national security intelligence investigations, his conclusion suggests that by not being fully integrated within the criminal law system, national security intelligence investigations do not acquire the types of characteristics that would make them worthy of being able to sustain a privilege of the same nature and scope as that of police informer. The reasons of Abella and Cromwell JJ., dissenting on this point, are more fully articulated.

59 McDonald: Second Report, v1, supra note 37. In 1966, Prime Minister Pearson established a Royal Commission of Inquiry on Security, with a mandate “… to make a full and confidential inquiry into and report upon the operations of Canadian security methods and procedures. The McKenzie Commission, as it came to be known, recommended that a civilian security intelligence service be created outside of the RCMP. In rejecting that recommendation, the Prime Minister, by then Mr. Trudeau, declared his agreement with the conclusion that there is a fundamental distinction between law enforcement and security (and the government’s preference to address it organizationally from within the RCMP. At page 70. The McKenzie Commission is at: Canada. Report of the Royal Commission on security (Abridged) (Ottawa: Minister of Supply and Services Canada, 1969).

60 The separation between law enforcement and security intelligence functions is not unique to Canada. Elsewhere, it may be attributed to a preoccupation to avoid combining the functions within a single too powerful entity. Most countries also have separate organizations working domestically and on foreign soil. The latter will also often be empowered to carry out offensive operations, e.g. DGSE in France, CIA in the United States, MI6 in the UK, ASIS in Australia (from personal discussions).

61 Bruce Hoffman, “Study of International Terrorism” in Air India Research Papers, supra note 1, Volume 1, 17 at 46-47. Looking at the issue from a strategic perspective in discussing instrument choice, Peter M. Archambault argues, in the same series, for preserving the different mandates and objectives as a mean to maintain effectiveness.
The comparative description between law enforcement and intelligence investigations that was made by the Special Senate Committee that examined the *CSIS Act* as it was first introduced in Parliament remains apposite today. It contrasted the two systems in relation to the stances taken (proactive vs reactive), the publicity (open vs secret), the outcome types (result oriented vs information oriented) and the modes (closed system vs open ended):

The differences [between investigations] are considerable. Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law.

Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy.

Law enforcement is resulted oriented, emphasizing apprehension and adjudication, and the players in the system, police, prosecutors, defence counsel, and the judiciary operate with a high degree of autonomy. Security intelligence is, in contrast, information-oriented. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital.

Finally, law enforcement is a virtually enclosed system with finite limits, commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis and the formulation of intelligence. [text re-formatted][62]

Comments illustrating the same effect were made by the Federal Court of Appeal in the matter of *Atwal*,[63] and cited in *R v Alizadeh* in 2014[64]:

The [Criminal] Code contemplates interception as an investigative tool after or during the event while the [CSIS] Act is directed primarily to gathering information in an attempt to anticipate future occurrences. The distinction was recognized by the United States Supreme Court in *U.S. v U.S. District Court*, (1972) 407 U.S. 292 at 322.

---

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime". The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.\textsuperscript{65}

Referring to the same passage, Cohen contrasts security intelligence work to the balancing that takes places in criminal investigations by citing \textit{Brown v Durham Regional Police Force}:

\begin{quote}
In the criminal law context, police and individual interests typically interest after the alleged commission of a crime. The police power to interfere with individual liberty or security is tied to their ability to link the individual to the event or events under investigation. This societal harm done by the commission of a crime and the suspect’s connexion to the event provide the justification for state action which interferes with individual freedoms.

According to this paradigm, the police conduct is reactive and, in so far as it interferes with individual liberty of security, is circumscribed by the police ability to meet pre-established standards which are said to forge a sufficiently strong connection between the past event and the individual to warrant interference with constitutional right. [\textit{passage omitted}] It is self-evident that assessments of what has happened and an individual’s involvement in those past event are much more likely to be reliable than are assessments of what may happen in the future and the involvement that an individual may have in those events should they occur.\textsuperscript{66}
\end{quote}

While there are distinctions, there are also clearly some overlaps. In \textit{Charkaoui} \textsuperscript{2}\textsuperscript{67}, the Court remarked that while it is clear that CSIS is not a police force, “it must be acknowledged that the

\begin{footnotes}
\textsuperscript{65} \textit{Ibid} at 12-13.
\textsuperscript{66} Cited in Cohen, \textit{supra} note 1 at 53-44. The difference between the two types of work is also illustrated by available data. Public Safety Canada’s 2016 \textit{Public Report On The Terrorist Threat To Canada} posted in August 2016, reports that over the previous 14 years (since 2002), 20 individuals had been convicted of terrorism offences under the \textit{Criminal Code} and that another 21 had been charged with terrorism-related offences (including 16 since January 2015) and were either awaiting trial or had warrants outstanding for their arrest. Even if we are to assume for the sake of this paper that CSIS will have provided early information to the RCMP in some cases (the Supreme Court referred to this occurring occasionally) but taking into account that some instances may involve more than one individual at a time, this still stand in sharp contrast to numbers revealed in the annual reports of the Security Intelligence Review Committee. The most recent of these indicates that in 2015-16, under its section 12 mandate, CSIS was investigating approximately 550 persons or groups engaged in activities suspected of posing threats to the security of Canada (which to be noted, covers more than terrorism). Online: \textcolor{blue}{https://www.publicsafety.gc.ca/cnt/rsrcs/phletns/2016-pblc-rpr-trrrst-thrt/index-en.aspx\%3E}, retrieved August 27, 2017.
\textsuperscript{67} \textit{Charkaoui v. Canada (Citizenship and Immigration)}, 2008 SCC 38, [2008] 2 SCR 326 [\textit{Charkaoui 2}].
\end{footnotes}
activities of the RCMP and those of CSIS have in some respects been converging as they, and the country, have become increasingly concerned about domestic and international terrorism. The division of work between CSIS and the RCMP in the investigation of terrorist activities is tending to become less clear than the authors of the report seem to have originally envisioned. (…) For example, CSIS occasionally discloses information to the RCMP”. This passage that has often been quoted but seldom commented upon, would likely refer to an increase in the number of situations where the work of the two organizations overlap. This is bound to happen, particularly in terrorism matters where the scope and nature of criminal and administrative offences has broadened continuously since September 2011, primarily as a result of Canada’s complying with its international obligations.

Instances of such overlaps have since been made public as part of at least three prosecutions: R v Ahmad (as part of the “Toronto 18”)

68, R v Jaser69 and Alizadeh70. In all three, the courts concluded that the two types of investigations, law enforcement and national security intelligence, were kept separate and parallel. In these cases, ‘occasional disclosures’, to use the same words as the Supreme Court in Charkaoui, were not sufficient for the courts to conclude that CSIS was acting as part of the Crown for disclosure purposes.

On occasion, normally when assessing privacy in the context of regulatory searches and when distinguishing the search from those done as part of law enforcement activities, the Court described the absence of public stigma as a factor that would remove some weight to the privacy part of the equation. It did so in Thomson71. Here, the secrecy surrounding national security intelligence also has an impact: for reasons entirely different from those that operate in the context of regulatory searches or presence at borders, there will not be any public knowledge that a person’s name has come up in relation to matters about which national security intelligence is being developed. Thus, while secrecy does represent challenges from a number of perspectives,

70 Alizadeh, supra note 64 at para 26.
individuals do not necessarily suffer public stigma from the only fact of having had their identity secretly associated with security intelligence information.72

Where then does security intelligence information and investigations stand in relation to law enforcement investigations? In my view they are and remain very distinct types of state activities. Their governance and accountability modes are very different. They serve different state purposes and arrive at vastly different types of outcomes. They each obey to their own discipline and rules. They are conducted very differently although they may use similar tools. These differences are such as to render imprudent, and likely inappropriate in most situations, the application of a criminal law lens to examine security intelligence activities. Thus, while the values set out by s. 8 are universal, it would be most prudent to ensure that these distinctions are considered at the time jurisprudence is developed, as they should be considered relevant to the analysis. As will be seen below, I am arguing that the distinction needs to be carried over, at least when it comes to principles governing the application of section 8 of the Charter.

3. The application of the section section 8 analytical framework
   a. A contextual approach

After Hunter, the courts have examined how s. 8 should be applied in a variety of circumstances.73 In this, context became a particularly important factor as the Court did adapt the Hunter standards to different legislative schemes.

In 1990, in Thomson Newspapers Ltd74, the Court was divided over whether s. 8 was engaged when the appellants were served with orders to appear before the Restrictive Trade Practices

---

72 The impact of the presence or absence of stigma was more often discussed in classifying legislative scheme, in determining if they are criminal nature. This was the case for example in Wholesale Travel, supra note 8, mainly at para 30 et seq. or in Dehgnani v Canada (Minister of Employment and Immigration) [1993] 1 SCR 1053; [1993] SCJ No 38 [Dehghani] at para 38. This matter was about whether examination at port of entry by immigration officer amounted to detention for purposes of s. 7 of the Charter.

73 This paper refers to ‘searches’ throughout rather than to ‘searches and seizure’. This is done for convenience purposes and the discussion should generally apply in respect of both but it also reflects the fact that in the field of security intelligence, where collections and investigations are generally done covertly and will remain unacknowledged, it is much less common to have recourse to seizures.

74 Thomson, supra note 71. This pertained to ss. 8 and 17 of the Combines Investigation Act that allowed the issuance of subpoena, to administer oath and to question a witness.
Commission and to produce documents. Commenting about the application of the Hunter standard, La Forest, L’Heureux-Dubé and then Wilson JJ (dissenting), all found here also that the purpose for which the information was sought by the state was relevant on how s. 8 would apply. Wilson J. wrote:

Not all seizures violate s. 8 of the Charter; only unreasonable ones. Put another way, an individual is accorded only a reasonable expectation of privacy. At some point the individual’s interest in privacy must give way to the broader state interest in having the information or document disclosed. However, the state interest only becomes paramount when care is taken to infringe the privacy interest of the individual as little as possible. … I would agree, however, that [the Hunter] criteria are not hard and fast rules which must be adhered to in all cases under all forms of legislation. What may be reasonable in the regulatory or civil context may not be reasonable in a criminal or quasi-criminal context. What is important is not so much that the strict criteria be mechanically applied in every case but that the legislation respond in a meaningful way to the concerns identified by Dickson J. in Hunter.75

Two years earlier, in R v Simmons,76 the Court had looked at the validity of a search conducted at the border, Dickson C.J., speaking for the majority first took care to reaffirm the primacy of the Hunter standards.77 He then accepted the position presented by the Crown and inspired from American jurisprudence on the Fourth Amendment, that a sovereign state’s interest in national self-protection, amounting to a significant government interest in preventing the entry of contraband and enforcing custom laws, is an important component of the calculus in establishing reasonableness.78 He insisted on the importance of preventing unjustified searches, remarking that departures from the Hunter standard that would be considered reasonable will be exceedingly rare but concluded that the application of the standard, and its elements, were not

---

75 Ibid at 95. L’Heureux-Dubé J. agreed with Wilson J. that reasonableness will differ with context, be it regulatory or civil versus criminal or quasi-criminal and commented that since (in her view) the impugned legislation was regulatory, the reasonableness of the subpoena issued under its authority should be assessed by taking into account a number of factors, including the importance of the underlying purpose, the necessity of impairing privacy interests and the absence of other, less onerous, alternatives. At 279.
77 Ibid at para 47.
78 Ibid, at para 48. He concluded that the relevant provisions of the Customs Act, authorizing searches on a standard of ‘reasonable cause to suppose’ with the possibility for the person to ask to be taken before a magistrate, were not inconsistent with s. 8 when combined with a lower expectation of privacy at customs and the type of search (searches of the person conducted in private not being so highly invasive as to be considered unreasonable) (at 5para 50 et seq.).
required there, this premised on the goal pursued as well as on the degree of intrusiveness of the searches.  

The Court went on to affirm and apply that principle in a rather consistent fashion in a series of judgements where it examined the importance of the state interest at issue by not looking only at the weight it has in the balance but also at how it informs the determination of the standard itself.

In 1994, in *R v Colarusso* 80, an interesting case for our discussion, the Court was examining a warrantless seizure of blood by a coroner in the light of s. 8. La Forest remarked that “in *Thomson*… I alluded to the fact that the *Hunter* criteria may be more flexible in non-criminal situations.” 81 and then “having regard to the fact that a coroner’s inquest fulfils an important non-criminal function, and some measures of investigatory powers is necessary to enable the coroner to fulfill his or her duties adequately, I am prepared to accept that a lower standard that the *Hunter* requirement of prior judicial authorization may be acceptable for seizures undertaken by a coroner for valid purposes”. 82

In *British Columbia Securities Commission v Branch*, 83 the Court, commenting on expectation of privacy of individuals engaged in securities market, noted that the “greater the departure from the realm of criminal law, the more flexible will be the approach to the standard of reasonableness. The application of a less strenuous approach to regulatory or administrative searches or seizures is consistent with a purposive approach to the elaboration of s. 8.” 84

---

79 *Ibid*, at para 47, 50. In this case, questioning, search of luggage, frisk and pat searches, removal in private or articles of clothing to permit investigations of suspicious bodily bulges. The *Customs Act* provided then a standard of ‘reasonable cause to suppose’ and a right to require an officer to take him before a decision maker who could discharge the person if he or she found no reasonable cause.

80 [1994] 1 SCR 20, 110 DLR (4th) 297 [*Colarusso*]

81 *Ibid* at para 95 (for the majority).

82 *Ibid* at para 95. He did caution against authorities using a lower standard to piggy-back towards use in criminal proceedings and other improper reliance, at para 97-98. The minority reiterated that the *Hunter* criteria are flexible and that the reasonableness of a power is to be assessed in light of the particular context in which it operates. At para 33-34.

83 [1995] 2 SCR 3; [1995] SCJ No 32 [*Branch*].

84 *Ibid* at 52.
The matter of *R v Jacques*\(^{85}\) concerned expectation of privacy at borders, in relation to the stop and search of vehicle. Gonthier J. referred here also to the state having a pressing interest in protecting its borders, which justified a lower standard (“not stringent but not illusory”) of reasonable suspicion under the *Customs Act*.\(^{86}\) In this, he referred to the Court’s decision in *Dehghani*\(^{87}\) noting that both matters highlight the need for a contextual approach (well established at that point), which recognizes the significance of the border situation.\(^{88}\) He also referred to the balancing exercise: interests of highway safety and compliance on one hand and sovereignty in the other, being interests that are relevant in the constitutional calculus, as was found by the Court in two other cases it considered, *R v Ladouceur* and *R v Husky*.\(^{89}\)

More recently, in *Chehill*,\(^{90}\) the Court reiterated the validity of the two-pronged approach, referring also to its decisions in *Kang-Brown*\(^ {91}\) and *A.M.*\(^ {92}\) that balanced the society’s interest in routine crime prevention against individuals’ interest in their own privacy.

Finally, *Wakeling* offered another occasion for members of the Court to examine state interests as part of applying s. 8:

> The assessment of this balance must be connected to the underlying purposes of s. 8 itself. Just as the expectation of privacy analysis asks what we, as a society, should be able to expect will be kept private … the assessment of whether a law provides reasonable authority for a search involves asking what level of privacy protection we are entitled to expect, given the state’s objective in seeking the information.\(^ {93}\) (Citations omitted)

---

\(^{85}\) [1996] 3 SCR 312; [1996] SCJ No 88 [*Jacques*].

\(^{86}\) *Ibid* at para 15, 17.

\(^{87}\) *Dehghani*, supra note 72.

\(^{88}\) *Jacques*, supra note 85 at para 19-20.

\(^{89}\) *Ibid* at para 21, *R v Ladouceur* [1990] 1 SCR 1257, [1990] SCJ No 53; *R v Hufsky* [1988] 1 SCR 621, [1988] SCJ No 30. These cases, however, were mainly about the constitutionality of random stops under s. 9 of the *Charter*. The case of *R v Monney*, [1999] 1 SCR 652, 171 DLR (4th) 1 [*Monney*] was heard at the end of 1998 and is another matter about the application of s. 8 to a search by custom officers. Iacobucci J. relied on *Simmons* and *Hunter* to remind that the standard of reasonableness is subject to change along with the state interest at issue (at para 34-35).

\(^{90}\) *R v Chehil*, 2013 SCC 49, [2013] 3 SCR 220 [*Chehil*].


\(^{92}\) *R v A.M.*, 2008 SCC 19, [2008] 1 SCR 569 [*A.M.*].

\(^{93}\) *Wakeling v United States of America*, 2014 SCC 72, [2014] 3 SCR 549 at 111 (Karakatsanis J., dissenting on whether s. 8 was engaged) [*Wakeling*].
Ensuring and maintaining national security has to stand amongst our society’s highest purposes, one that is linked to the ability of the state to ensure its continuity, to remain the “free and democratic society” which section 1 of the Charter holds as our standard. This is coherent with the Supreme Court’s statement in Charkaoui that ensuring the security of its citizen stands as one of the most fundamental responsibilities of a government. As such then, national security and taking measures to preserve it represent an objective that will play a predominant role in the balancing exercise mandated by section 8. Thus, in assessing the validity of provisions authorizing the intrusive intelligence gathering activities found in the CSIS Act (or, for CSE, the National Defence Act) or government actions undertaken pursuant to them, that objective will also be considered in determining what would be an appropriate standard as per the invitation made in Hunter.

b. The justifiable expectation of privacy

The other side of the equation is represented by the justifiable expectation of privacy. First, of course, the information at issue must be of such a nature that it attracts the protection of s. 8. As explained in Tessling: “… only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitutes a ‘search’ within the meaning of s. 8”.94 Or as set out by the Court in the matter of Cole in discussing whether an expectation of privacy was objectively reasonable:

The closer the subject matter of the alleged search lies to the biological core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.95

There is certainly no room to suggest that the same principle does not hold when considering the reasonableness of an expectation of privacy for purposes of national security, a conclusion dictated by the normative nature of s. 8.

c. Impact of variations in the level of privacy and the degree of intrusiveness

The Court has also held that the degree of intrusion of an activity or the level of the expectation of privacy will be relevant in applying s. 8. Variations in the level of privacy and the degree of intrusiveness of the search will have an impact in the definition of the applicable standard as well as in the balancing of the interests at play.

The degree of privacy that one can reasonably expect in information that could be relevant to matters under investigation or examination by the state can vary significantly. In \textit{R v M (M.R.)}, Cory J. commented that the analysis of s. 8 and the consideration of what constitutes a search and seizure for that purpose will be affected where a reasonable expectation exists in circumstances where it would be diminished. Indeed it could go as far as rendering the \textit{Hunter} criteria inapplicable. Such a finding was made in \textit{Thomson}, where La Forest J. found that the limited privacy interest in the records at stake was a factor that made the \textit{Hunter} criteria inappropriate for determination. He then pointed out that for the Court, the degree of intrusion into personal privacy and bodily integrity correlates with an increasing threshold of constitutional justification. In other words, the more intrusive the search, the greater the degree of constitutional protection required in terms of the standard of suspicion or belief which must be met.

Lower expectations of privacy were found to exist by the courts in a variety of circumstances, illustrating the point made by L’Heureux-Dubé J. that context matters in that regard as well too. These include regulatory customs searches of luggages at airport and vehicles at border, searches by school principal on school premises, use of rudimentary

\footnotesize

\begin{itemize}
\item\footnote{96} This point was discussed by La Forest J. in \textit{Thomson, supra} note 71 at para 122.
\item\footnote{97} \textit{R. v. M. (M.R.)}, [1998] 3 SCR 393, 166 DLR (4th) 261 at para 33 [M.R.]. Cory J. referred to \textit{Simmons}, and being of the view that it was “because of this lesser expectation of privacy [at the border], that a customs search did not have to meet the standards in Hunter … in order to be reasonable”.
\item\footnote{98} \textit{Thomson, supra} note 71 at para 149.
\item\footnote{99} \textit{Ibid.}
\item\footnote{100} Quoting from \textit{R v Bernshaw}, [1995] 1 SCR 254, at pp. 304-6, as quoted by Gonthier J. in \textit{Jacques, supra} note 85 (at para 20).
\item\footnote{101} \textit{Jacques, supra} note 85 at 324.
\item\footnote{102} \textit{Simmons, supra} note 76 at 528.
\item\footnote{103} \textit{M.R., supra} note 97 at para 33.
\end{itemize}

26
location tracker by the police and regulatory search of sleeping area of a truck cab which is also a place of work.

In the case of *McKenzie*, the lower expectation of privacy resulted in a lower standard being found to be applicable in terms of expectation of evidence that would be yielded by the search. The same outcome occurred where a lower expectation of privacy was found to exist in bus terminals and schools and in relation to use of sniffer dogs for drug detection, in motor vehicle on public highways, luggage at airport, in digital electricity consumption meter on a power line and search of a student on school premises.

The outcome is not always that a search is reasonable however. A finding that the highest standard applies in circumstances where an expectation of privacy is diminished is likely to be the result in those still very few circumstances where the courts has found that the higher degrees of constitutional protection are warranted. This would be coherent with remarks of Binnie J. in *Gomboc*, referring back to *Branch* and *Nolet*, matters involving regulatory searches, where he noted that while legislation was a factor to be considered when determining whether an expectation of privacy was objectively reasonable, ‘it may be insufficient to negate an expectation of privacy that is otherwise particularly compelling.’ I would propose that this principle extends for example to interception of communications, searches of personal

108  *Chehil, supra* note 90.
110  *M.R., supra* note 97, where it was found that a search of a student will be properly instituted where the teacher or principal conducting the search has reasonable grounds to believe that a school rule has been violated and the evidence of the breach will be found on the student (at para 50).
111  In *Cole, supra* note 95, for instance, while the Court found that the expectation of privacy that Cole had in the content of the computer he was using was lowered, consideration of the totality of circumstances on balance, supported a finding of objective reasonableness of Cole’s subjective expectation of privacy. In *Wakeling, supra* note 93, it was indicated that: “As this Court held in *Tessling*, a diminished subjective expectation of privacy does not necessarily result in reduced constitutional protections: the “[e]xpectation of privacy is a normative rather than a descriptive standard” (dissenting judge, at para 42).
112  *Gomboc, supra* note 109 at para 115.
computer or intelligent phone\textsuperscript{114}, seizure and searches of bodily samples\textsuperscript{115} and, in terms of territorial privacy, searches of residences of the person challenging the search.\textsuperscript{116}

The Court made similar pronouncements regarding the impact of the degree of intrusion of a particular search on its reasonableness. The relevance of the degree of intrusiveness of a search was discussed in \textit{Simmons} where Dickson C.J. set out three types of searches conducted at border, each carrying different degree of intrusion. He commented that it was obvious that the greater the intrusion, the greater must be the justification and the greater the degree of constitutional protection.\textsuperscript{117} For instance, the warrantless use of sniffer dogs has been described by the Court as not being highly intrusive in the circumstances of \textit{Chehil} where the Court explained that they could be used without judicial authorization as “they are minimally intrusive, narrowly targeted and highly accurate”.\textsuperscript{118}

Indeed, in \textit{Thomson}, La Forest J. clearly linked the application of the \textit{Hunter} criteria to the greater intrusiveness of the investigative power that were challenged in that matter.\textsuperscript{119} In \textit{Monney}, Iacobucci J. acknowledged that the degree of intrusion into personal privacy and bodily integrity correlated there with an increasing threshold of constitutional justification, commenting that the greater the degree of constitutional protection is then required in terms of the standard of suspicion or belief which must be met.\textsuperscript{120}

Thus, while it is clear that the balancing exercise mandated by \textit{Hunter} will be triggered by the existence of a reasonable expectation of privacy in the information sought by the state, the

\textsuperscript{114} See for example \textit{Cole, supra} note 95, \textit{R v Morelli}, 2010 CSC 8, [2010] 1 RCS 253.
\textsuperscript{116} For example of a recent judgment on the search of private residence, see \textit{R v Paterson}, 2017 SCC 15 where the Court confirmed that it benefits from substantial protection. Also \textit{R v Grant}, [1993] 3 SCR 223 and \textit{R v Plant} [1993] 3 SCR 281, [1993] SCJ No 97.
\textsuperscript{117} \textit{Simmons, supra} note 76 at 517. As noted above in \textit{McKinlay Transport, supra} note 9, Wilson J. argued for flexibility in interpreting the \textit{Charter}, noting that expectations of privacy may vary among and she commented that the greater the intrusion into the privacy interests of an individual, the more likely it will be that safeguards akin to those in \textit{Hunter} will be required individuals (at para 26).
\textsuperscript{118} \textit{Chehil, supra} note 90 at para 1.
\textsuperscript{119} \textit{Thomson, supra} note 71 at para 149.
\textsuperscript{120} \textit{Monney, supra} note 89 at para 38. One example of similar conclusions being reached arises in \textit{Tessling, supra} note 36 at para 50, Binnie J.
weight to be given to that expectation will be affected by both the degree of intrusion and the level of expectation of privacy. The standard that will be used to assess the reasonableness of the search is also susceptible to adapt accordingly. An illustration of this is offered by the remarks of Deschamps J. in Kang-Brown: “Consequently, a reasonable suspicion standard may be sufficient where the investigative technique is relatively non-intrusive and the expectation of privacy is not high.”121

d. Searches carried under the CSIS Act

Turning now to the backdrop provided by the CSIS Act, the largest proportion of CSIS activities would be devoted to what is often presented as its main mandate: the investigation of threats to the security of Canada to obtain information and intelligence for the purpose of reporting to, and advising, the Government of Canada under s. 12 of the Act. The threats that are defined in section 2 of the CSIS Act correspond basically to espionage, sabotage, clandestine foreign-influenced activities and terrorism, whenever these relate to Canada.122

Section 12 of the CSIS Act gives CSIS the mandate to collect information and intelligence for the purpose of advising the Government of Canada on these threats to the security of the country. The collection, and retention, of information and intelligence under s. 12 of the CSIS Act are subject to the requirement that these only be done to the extent strictly necessary and upon having formed reasonable grounds to suspect that the activities at issue constitute threats to

---

121 Kang-Brown, supra note 91 at para 168.
122 CSIS Act, supra note 27, s 12. The definition of “threats to the security of Canada” at section 2 provides as follows: (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). Like CSE, CSIS has the authority to collect information or intelligence on the capabilities, intentions or activities of foreign individuals, corporations or states as they relate to international affairs, defence or security (terrorism being dealt with separately in the CSIS Act). But this mandate is circumscribed quite precisely in ways that makes it unsuitable for our analysis: CSIS can only collect this information within Canada and cannot target Canadian citizens or entities [CSIS Act, section 16]. CSIS may only exercise this authority upon a personal request from the Minister of Foreign Affairs or the Minister of National Defence.
security. The mandate of CSIS to investigate these threats and to collect information in this regard is not limited geographically, as was made clear by an amendment to s. 12 (and a similar one to s. 21) adopted in 2015.

In investigating threats to security, CSIS may obtain judicial authorizations to use measures that may engage s. 8 of the Charter or would otherwise be unlawful.

The conditions that must be met by applications for warrants as well as the manner in which judges may exercise their discretion are set out in s. 21 of the CSIS Act. Section 21 was clearly modelled on the Criminal Code wiretap provisions as they stood then; it contains many similar elements and follow the same structure as what was then section 178.1.

The investigative necessity provision incorporates an additional element to those that would normally be found in such regimes: that without warrant, it is likely that information of importance with respect to the threat would not be obtained. The issuing judge can issue these warrant for up to one year and can accompany them of any terms and conditions as he considers advisable in the public interest.

In Mahjoub, the Federal court of Appeal stated its agreement with a passage from Alizadeh that commented on the propriety of that element as a distinct, legitimate and necessary ground upon which a judge can issue a warrant, this taking into account the practical and complex realities required for CSIS to fulfil its mandate to investigate.

---

123 Section 12; see also the recent judgment of the Federal Court in Canadian Security Intelligence Act (Can.) (Re), 2016 FC 1105, [2016] FCJ No 1193 [Associated Data].
124 Protection of Canada from Terrorists Act, SC 2015 c 9, s 3; s. 12(2) of the CSIS Act reads as follows: “For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada”, see CSIS Act, supra note 55, CSIS Act, supra note 27, s 12(2). The mandate of the Service is somewhat unusual among those of other countries with which it is often compared.
125 As adopted by the Protection of Privacy Act, 1973-74 (Can.), c. 50 and discussed in Wiretap Reference (1984) 2 SCR 697, 14 DLR (4th) 546. In relation to threats to security, s. 21 provides that an application may be presented to a designated judge of the Federal Court on the basis of a belief, formed on reasonable grounds, that a warrant is required to enable CSIS to investigate a threat to the security of Canada. The application must set out the facts justifying that belief and the type of communications to be intercepted or information records documents or things proposed to be obtained and the ancillary powers proposed to be exercises. It must also identify the person(s) whose communications would be intercepted or in possession of the information records etc. proposed to be obtained, a general description of the places where it will be executed, where known and any previous application in relation to the same person(s).
126 CSIS Act, supra note 27, s 21. Warrants to investigate subversive activities may only be issued for 60 days.
threats while noting as well that it contains internal limitations that must be interpreted in a meaningful way so as to protect privacy interests of Canadian citizens and residents.\textsuperscript{127}

The matters of \textit{Atwal}\textsuperscript{128}, \textit{Ahmad}\textsuperscript{129} and \textit{Alizadeh}\textsuperscript{130} offered the courts the occasion to comment on the constitutional validity of the warrant scheme set out by the CSIS Act. These were all criminal prosecutions arising out of the investigations of subjects who had also come under CSIS’ scrutiny and where the courts was given occasion to comment on the CSIS warrants. In all instances, it was found that the warrant regime met the test set in \textit{Hunter}.

As noted above, its constitutionality was first addressed in the decisions of the Federal Court and Federal Court of Appeal in \textit{Atwal}. Mr. Atwal was attacking a warrant obtained by CSIS and seeking to rescind an affidavit that was presented as part of the application for the warrant. One of the grounds for his attack was that the warrant and affidavit failed to comply with the minimum constitutional standards for a reasonable search and seizure pursuant to s. 8. Atwal conceded that the requirements of prior authorization, by a persona capable of acting judicially, made on the basis of sworn evidence, were met. However, he argued that the last element of the \textit{Hunter} test, \textit{i.e.} that the objective standard must include reasonable and probable grounds to believe that the offence has been committed and that evidence of it would be found, was not met. Referring back to some of the same passages of \textit{Hunter} as quoted above, Mahoney J. A. discussed how that fourth branch of the \textit{Hunter} test should be applied in the context of s. 21. He first noted that the objectives pursued differed from those of criminal law, and that it is then entirely to be expected that s. 21 would not require the issuing judge to be satisfied of the same elements that would be relevant in the criminal context. He interpreted the provisions of the \textit{Act} as providing that the judge is required to be satisfied, on reasonable and probable grounds established on some evidence, that a threat to the security of Canada exist and that a warrant is required to enable its investigation, concluding that in his opinion, this was an objective standard. The Federal Court of Appeal found that these provisions met the \textit{Hunter} requirements.\textsuperscript{131}

\textsuperscript{127} \textit{Mahjoub}, supra note 28, at para 269-271.
\textsuperscript{128} \textit{Atwal}, supra note 63.
\textsuperscript{129} Discussed peripherically in \textit{Ruling no. 20 in R v Ahmad}, [2009] OJ No 6159 2009, 2009 CarswellOnt 9307 (ONSC), see also note 68.
\textsuperscript{130} \textit{Supra} note 64 at para 27.
\textsuperscript{131} \textit{Atwal}, supra note 63.
When considered in 2017, the Court of Appeal decision does not appear to represent a notable departure from the standard that was found to be applicable in criminal matters as per Hunter. Setting a standard that would require that factors specific to law enforcement activities be established would have been artificial and ineffective when applied to a security intelligence organization. The outcome in Atwal is partly the result of a pragmatic exercise: it simply did not make sense to use language and concepts applicable to law enforcement for a body that does not perform law enforcement functions. The Court used the language of s. 21 injecting an additional element, the requirement to establish that a threat to the security of Canada exists, and to do so on a ‘reasonable grounds to believe’ standard that was already provided for the other elements to establish. Still, at the time it represented an early application of the principles that had been set by Dickson J. Short of a recognition that different realities are involved where national security is at issue, the decision does not venture into any detailed discussions of the appropriate standard. 132

In Mahjoub, the Court of Appeal also confirmed that its decision in Atwal remains sound law; it refers to it as the benchmark to follow in the course of finding that s. 21, and its ‘reasonable ground to believe’ standard is constitutional. 133

CSIS (as does CSE) benefit from statutory authorities when it collects information. In 2013, in the Mahjoub immigration security certificate file, Blanchard J. addressed a question on whether minimally intrusive techniques used pursuant to section 12 of the CSIS Act resulted in an unreasonable search or seizure, section 12 setting a ‘reasonable ground to suspect’ standard for the collection of information by CSIS. 134 In rejecting the challenge, the judge acknowledged a heightened public interest in the Service investigating threats to the security of Canada. He concluded that section 12 provided an appropriate basis for the use of such techniques on the grounds that it “requires the Service to have an objective, particularized basis for the use of any minimally intrusive investigative techniques and strikes the appropriate balance between the

132 In Atwal, ibid and referred to in Alizadeh, supra note 64 at para 27.
133 Mahjoub, supra note 28 at para 175-178.
134 Mahjoub (Re) 2013 FC 1096, 457 FTR 1 at 26 et seq. Appeal was dismissed, Mahjoub supra note 28.
public interest in investigating threats to the security of Canada and the individual target's privacy rights.”\textsuperscript{135}

Further down, he explains\textsuperscript{136}:

I am satisfied, on a review of the techniques enumerated in the Service policies above, that they are minimally intrusive, if they engage a reasonable expectation of privacy at all. The "reasonable suspicion" standard must be satisfied in order to employ these techniques. Further, the policies contemplate obtaining Federal Court warrants, governed by sections 21 to 24, for more intrusive techniques. In my view, section 12 of the \textit{CSIS Act}, as interpreted by the Service, requires the Service to have an objective, particularized basis for the use of any minimally intrusive investigative techniques and strikes the appropriate balance between the public interest in investigating threats to the security of Canada and the individual target's privacy rights.\textsuperscript{137}

On July 19, 2017, the Federal Court of Appeal issued judgment on the appeal of Blanchard J.’s decision.\textsuperscript{138} Stratas J. agreed with the reasons of the Federal Court finding that s. 12 was constitutional and declined to find that the Court had erred in assessing the constitutionality of s. 12 and 21. In relation to s. 12, he found that the ‘reasonable grounds to suspect’ standard complies with s. 8, when applied to the minimally intrusive search at issue there, thereby providing another example of the application of Hunter in a context where national security intelligence has been used.

e. Accountability and publicity in the Hunter test

In the matter of \textit{Atwal},\textsuperscript{1} the Federal Court of Appeal had commented on the relevance of publicity mechanism as a factor in assessing the validity of the warrant provisions at s. 21 of the \textit{CSIS Act} which sets out the procedure that CSIS must follow to obtain warrants. It referred to comments made by Dickson J. about search warrants being issued \textit{in camera} that it felt were particularly apt: “In short, what should be sought is maximum accountability and accessibility.

\footnotesize\textsuperscript{135} \textit{Ibid} at 35. The reasoning of Blanchard J. on this point, is not always clear. He did indicate that Mr Mahjoub and the Special Advocates had not argued that any particular means of investigation had failed to respect the balance between public and privacy interests, nor the constitutional validity of section 12 itself. At 40-41.

\footnotesize\textsuperscript{136} \textit{Ibid} at 33.

\footnotesize\textsuperscript{137} \textit{Ibid} at 35.

\footnotesize\textsuperscript{138} \textit{Mahjoub supra} note 28.
but not to the extent of harming the innocent or of impairing the efficiency of the search warrant as a weapon in society's never-ending fight against crime” to conclude that what must be sought for the intelligence gathering system is the maximum accountability and accessibility of the judicial presence in the intelligence gathering system but not to the extent of impairing the investigation of genuine threats to national security.  

The themes of accountability and publicity as elements of s. 8 were explored in the judgement of the Court in Tse.  

It was argued before the Court that the provisions of the Criminal Code governing a form of warrantless interception contravened s. 8 since they lacked accountability measures as well as additional conditions or limitations that would be required under s. 8. In particular, the relevant provisions (s. 184.4 of the Criminal Code) did not contain any after-the-fact notice. The Court described accountability as a mean for targeted persons to become aware of the interception, linking it back to the comment of Dickson J. in Hunter that an unreviewable power would be inconsistent with s. 8. In the context of Part VI of the Code, then, accountability would be achieved by after-the-fact notice and reporting. Notice requirements, noted the Court, are practical in these circumstances as providing an additional layer of transparency and serving as a further check against abuse.  

In the end, the provisions at issue fell on the absence of any mechanism to permit oversight of the use of the power. The Court did consider however that other effective means may be available to correct this deficiency. In commenting on other arguments presented, the Court did give some other indications of its thinking on these questions. For instance, it stated that requiring record-
keeping could be another measure ensuring accountability, where practical.\(^{145}\)

The views of the Court on these points are interesting for our purposes since CSIS will exercise its authority to collect information, whether with or without warrants, without any notice of it being given to the persons to whom the information relates. As explained below, opportunities to seize the courts of questions concerning the validity of a CSIS searches are rare.

Some of these questions were revisited in *Wakeling\(^{146}\)* that concerned the constitutional validity of provisions authorizing the disclosure of communications intercepted under the *Criminal Code* to a foreign state.\(^{147}\) The Court confirmed that accountability forms part of the reasonableness analysis under s. 8.\(^{148}\) Moldaver J., for the majority, distinguished *Tse* on the basis that it concerned warrantless interceptions. In *Wakeling*, a judge was involved in balancing the interests at issue at the time the authorization was issued and that process would have provided sufficient safeguards.\(^{149}\) He also commented that rather than seize on individual provisions of the wiretap scheme in assessing constitutional validity, the courts should look at provisions and safeguards contained in the scheme overall.\(^{150}\)

It is clear that the role of the courts in calling the government to account for its actions is a fundamental element of our constitutional democracy. Yet, it is equally clear that national

---

\(^{145}\) *Ibid* at para 92. It also found that other measures such as making a report to Parliament and imposing statutory restrictions on the use that can be made of the interception were not constitutional imperatives (at para 89, 93).

\(^{146}\) *Wakeling, supra* note 93.

\(^{147}\) Section 192(2)(e).

\(^{148}\) *Wakeling, supra* note 93 at para 52, Moldaver J., other plurality judges agreed, McLachlin C.J., dissenting, did not opine on this point.

\(^{149}\) *Ibid* at para 65-66.

\(^{150}\) *Ibid* at para 67. In the course of his reasons, Moldaver J. concluded that the absence of the following measures did not render the provisions at issue unconstitutional, even though some of them may represent good practices: record-keeping requirements, obligation to give notice of disclosure of communications to foreign authorities, reporting such instances of disclosure to Parliament, requirements that would constrain the foreign state’s use of the information and adherence to international protocols and the use of caveats or information-sharing agreements (at para 66, 70, 71, 73-74). On the last item, Moldaver J. commented at para 74-75 that such indicators may be relevant in assessing whether disclosure was genuinely intended to advance the interests of the administration of justice, a criteria in section 193(2)(e) and will also impact on whether the manner of disclosure is found to be reasonable. Karakatsanis J, writing for the three dissenting judges, disagreed with these conclusions, finding that failing to require that the disclosing party to impose conditions on how foreign officials can use the information they receive by way of caveats or agreements and to set accountability measures, such as record-keeping and notice, applicable to the subsequent use of the intercepted information to deter inappropriate disclosure and permit oversight, rendered the provisions at issue unconstitutional.
security intelligence is an area where opportunities for the courts to do so are more limited, due to a combination of the factors discussed herein. As will be shown in the next section, there exists in this area strong mechanisms of control and review.

f. Control and review mechanisms

The Canadian legal framework for national security intelligence incorporates safeguards in the form of mechanisms to control and review national security activities.

The Security Intelligence Review Committee (SIRC or the Committee), is given a number of functions related to the review of CSIS activities.\(^{151}\) It is composed of members of the Privy Council.\(^ {152}\) The Committee has a general mandate to review the performance by CSIS of its duties and functions.\(^ {153}\) The *CSIS Act* specifies certain areas that must form part of activities examined by the Committee.\(^ {154}\)

The Committee also assesses whether CSIS conducted its activities in accordance with the *CSIS Act* and any direction issued by the Minister of Public Safety (see below) or if they involved an unreasonable or unnecessary exercise of its powers. It then informs the Minister of Public Safety and the Director of its findings. It also applies this lens to its review of the report on CSIS’ operational activities that the Director provides annually to the Minister of Public Safety pursuant to the *CSIS Act*.\(^ {155}\) In discharging its duties, the Committee initiates and conducts reviews itself or may ask that the Service does so and then report back.\(^ {156}\)

---

\(^{151}\) SIRC is set out under Part III of the *CSIS Act*.

\(^{152}\) *CSIS Act, supra* note 27, s 34. They are appointed by the Prime Minister after consultation with leaders of the Opposition and recognized parties in the House of Commons.

\(^{153}\) *Ibid*, s 38.

\(^{154}\) This includes, for instance, arrangements with foreign agencies and provision of information and intelligence pursuant thereto, reports to the Minister of Public Safety by the Director of the Service (the Director) that an unlawful act may have been committed in the purported performance of the Service’s duties and functions or the monitoring of requests for assistance made to CSIS under section 16 of the *CSIS Act* as described above. (s 38)

\(^{155}\) *Ibid*, s 6(4), s 38(2). In 2012, the function of Inspector General was abolished and the duties simply amalgamated with those of the Committee. As a result, the provisions setting out the duties and functions of the Committee may appear convoluted.

\(^{156}\) *Ibid*, s 40(2).
The Committee may receive complaints and carry out investigations. In discharging its duties, SIRC has access to all information in possession of CSIS, including legal advice, with the exception of Cabinet confidences. Committee members enjoy security of tenure, act independently, and can receive and investigate complaints. Finally, annual reports on the activities of CSIS are submitted to the Minister of Public Safety; the Minister is then required to table the report in Parliament within the next 15 sitting days.

That capacity will be augmented with the new National Security and Intelligence Committee of Parliamentarians. The Committee is given a review mandate cutting across organizational boundaries within the government and extending to any activity that relates to national security or intelligence. An exclusion arises where a Minister determines that the review is about an ongoing activity and that carrying it out at that time would be injurious to national security. The Committee is also to review the frameworks within which national security and intelligence activities are conducted as well as any other matter referred to it by a minister. The Committee will also have access to a vast range of information under the control of departments, subject to narrowly crafted exceptions that include Cabinet confidence an information that would identify intelligence human sources and protected witnesses. While it will be composed of parliamentarians (but not Ministers), the National Security Committee will report its findings and recommendations to the Prime Minister who must then table a copy of the report (or revised version if it contains sensitive information) before each House of Parliament. The appropriate Parliamentary committees are then considered to be seized with the report. The various review bodies are expect to work together to ensure a certain level of coordination. The legislation creating the Committee has received royal assent but at the time of writing, has yet to be proclaimed into force.

157 CSIS Act, supra note 55, s 41.
158 CSIS Act, supra note 55, s 39.
159 CSIS Act, supra note 55, s 53.
160 Ibid, s 8.
161 Ibid.
162 Ibid s 13, see also ss 14 and 16.
163 Ibid, ss 4, 21.
164 On June 22, 2017, the National Security and Intelligence Committee of Parliamentarians Act, SC 2017 c 15, received royal assent.
The Privacy Commissioner may also carry out investigations in respect of personal information under the control of the intelligence agencies to ensure that they comply with provisions of the *Privacy Act* pertaining to collection, retention, use and disclosure of personal information. Acting as an officer of Parliament, the Commissioner reports to it directly at least annually and may comment on any matter within the scope of his powers, duties and functions. His reports must be referred to the appropriate Parliamentary committee.

The Minister of Public Safety also receives duties and functions bringing him to play a role in reviewing and controlling activities of CSIS that goes beyond what is normally the case for ministers in relation to departments or agencies for which they are accountable.

First, the Minister of Public Safety retains direction of CSIS under s. 6 of the *CSIS Act*. In doing so, he may issue written directions, copies of which will be provided to SIRC. As indicated above, the Director must also present to the Minister of Public Safety an annual report about the Service’s operational activities for the year. This is then provided to SIRC for it to consider and advise the Minister of Public Safety. The Director of the Service must report to the Minister of Public Safety situations where he is of the opinion that an employee may have acted unlawfully in the purported performance of his duties. The Minister of Public Safety then provides it to the Attorney General of Canada, along with any comment he deems appropriate, and sends a copy of it to SIRC. Agreements between CSIS and other departments and governments, law enforcement agencies and foreign agencies must be approved by the Minister of Public Safety. Finally, any application to the Federal Court for warrants must be approved by the Minister of Public Safety.

---

165 *Privacy Act*, RSC 1985 c P-21, s 37.
167 *CSIS Act*, supra note 27 s 6(2).
171 *Ibid*., ss 21(1), 21.1(1). The Minister of Public Safety also designates the employee who may present the application and the *CSIS Act* also specifies that the Deputy Minister of Public Safety must be consulted.
The review framework is robust and is likely to become more so via an eventual adoption of bill C-59, An Act respecting national security matters, which was introduced in Parliament on June 20, 2017.\footnote{Bill C-59 supra note 55, makes important changes in this area. It would eliminate the position of CSE Commissioner to replace it with an intelligence commissioner that is clothed with attributes that would render it capable of acting judicially, and who is given an authorizing role similar to the one which is currently played by the Minister. It also approves certain matters for CSIS. The Commissioner’s review functions are given to a revamped security intelligence committee, starting with the mandate from the existing SIRC, augmented in terms scope and subject matters. While I am focussing here mainly on those applicable to CSIS, such safeguards also exist in relation to CSE. The Commissioner of CSE is appointed for good behaviour for a maximum period of 5 years, and must be a supernumerary or former superior court judge. He is charged with reviewing CSE’s activities to ensure they comply with the law. Where he believes they may not, he is required to inform the Minister of National Defence and the Attorney General of Canada. NDA, supra note 56, s 273.63 The NDA also specifies that the CSE’s Commissioner must review activities carried out pursuant to a ministerial authorization to ensure they are authorized and report annually to the Minister of National Defence on his findings. At s 273.65 (8).}

In my thesis, the presence of effective review and control mechanisms constitutes a factor to consider in defining and applying the elements that would meet the scriptures of the reasoning underlying the test set in Hunter. More particularly, they should be seen as providing a form of accountability.\footnote{Independent review may not be a sufficient measure to ensure accountability in all cases. Thus, the CSIS Act does encompass a regime of judicial authorizations and there is an emerging view that the Federal Court is being called upon to play a certain supervisory role for matters related to warrants issued under these provisions. On the role of the Court, see comment of Noël J. in Associated Data, supra note 122. The Department of Justice and CSIS have also commissioned Mr. Murray Segal to provide a report on the duty of candour that applies in the context of ex parte national security proceedings. Mr. Segal’s findings suggests that the Court plays an expanded role in that context. The report is available under ‘Review of CSIS Warrant Practice’ via the Department of Justice, online: http://www.justice.gc.ca/eng/rp-pr/cj-jp/antiter/doc-odl/p3.html (retrieved August 27, 2017, copy of the report with the author). In the case of CSE, as explained above, the National Defence Act sets out the Commissioner as a person capable of acting in a judicial capacity to approve ministerial authorizations that may lead to collection of information in which Canadians may have an expectation of privacy.}

4. A proposed approach

Ensuring and maintaining national security has to stand amongst our society’s highest purposes, one that is linked to the ability of the state to ensure its continuity, to remain the “free and democratic society” which s. 1 of the Charter holds as our standard. This is coherent with the Supreme Court’s statement in Charkaoui that ensuring the security of its citizen stands as one of the most fundamental responsibilities of a government.
Terrorism, which aims to seed terror among populations, illegal production or use of chemical or mass weapons, attacks against important elements of infrastructure such as energy plants or covert acquisition of information that is valuable to the interests – economic or other -- of Canada are all examples of activities that put at risk the integrity of the fabric of our society and our values, which include our guaranteed rights and freedoms. The government would also want to preserve its ability to conduct national and international affairs to the benefit of all Canadians.

In considering matters brought before it, the Supreme Court has described the criminal law system, as represented by the machinery of criminal justice, as standing at the apex of the purposive part of the equation for purposes of section 8. In my view, ensuring national security has to be given a similar place, attracting corresponding weight in applying the Charter.

The collection, analysis and dissemination of security intelligence is one of the main tools held by a democratic government to ensure maintenance of its security. This may involve the conduct of searches that would engage section 8.

In Hunter, the Supreme Court set out a standard to adopt in determining whether an intrusion by the state done for purposes of law enforcement was reasonable under section 8. It also set out elements to use in assessing whether that standard was met. While it has not deviated from the core principle it set out early on, the Court has had occasions to expand on the rationale underlying the standard and to explain how it and the elements that would support it, should adapt when the underlying state purpose varies. The Court thus provided the beginning of a map we can use in seizing the invitation offered by Dickson J. to adapt the standard he did set in Hunter to the context of national security.

What then is the guidance offered by the Court on these questions over the following 30 years? It turns out that the Court has seldom detoured from a few lanes that have become well-travelled.

---

174 To which should be added democratic use of armed forces and effective law enforcement regimes.
The first few years saw the Court explore different contexts. Coming one right after the other, the judgments of *Thomson Newspapers*, *McKinlay Transport*, and *Wholesale Travel* the Court examined the propriety of using the *Hunter* standard and its underlying elements in the context of regulatory compliance (and contrasted it with enforcement). There, the Court reinforced its statements regarding the relevance of the context in which a right or freedom is being asserted. It is to be used first in determining the meaning and content of the right, something that should not be done in the abstract (as per the Court’s prescriptions in *Edmonton Journal*). At the same time as it found that state interests in regulating the activities in question were compelling, the Court adopted much lower standards than first set out in *Hunter*, premised on the fact that by engaging in the regulated activities, individuals (and entities) would knowingly and publicly become subject to the compliance aspect of the regime. Any expectation of privacy was reduced or eliminated and none of the public stigma or negative consequences that would attach to criminal proceedings would ensue.

Since national security intelligence is normally collected and generated without the knowledge of subjects of investigation, these decisions would not find any direct application here. On the other hand, without wanting in any way to trivialize the issues and risks posed by a state being able to collect secretly information on its citizens, it might be of some relevance to note that since national security intelligence investigations and collection of information for these purposes are done in secret, they do not by themselves attract “the opprobrium of society”, public stigma or expressions of moral reprimand, which were described as relevant features of criminal law regimes in examining searches for purposes of section 8.

A second series of cases pertained to border searches and, from the outset, relied on the principle that sovereign states have the right to control both who and what enters their boundaries. While it may be topical when applied to specific facts, the approach does not make this line of jurisprudence particularly useful in setting out principles for our discussion.\(^{175}\)

\(^{175}\) It could perhaps provide an argument in support of different standards to govern the application of section 8 to activities of CSE and those undertaken by CSIS under section 16 as well possibly as security advice on immigration and citizenship matters under sections 14 and 15 of the *CSIS Act*. In relation to other CSIS activities, if the same principles were to apply, they could conceivably only do in very circumscribed factual circumstances where a subject is at a border point. These are not questions that are explored in any depth in this paper.
This said, these categories did provide helpful illustrations of the adaptiveness of the Hunter approach (see the above reference to Branch for instance.)

Thus, in the course of applying the Charter, the Court also had to look at what determines the essence of criminal law,\(^{176}\) the Hunter criteria having been said to apply with full vigor when a search takes place as part of an investigation into a crime.\(^{177}\) There does not appear to be any reason that would require that the regime and principles applicable to criminal investigation be applied to searches conducted for purposes of security intelligence investigations, provided of course that the two type of investigations do not become intermingled.\(^{178}\) Under the CSIS Act, the information collected for national security intelligence purpose generates intelligence used in advising and informing the Government of Canada. While the agencies and departments in receipt of that information or intelligence may then rely on it to make decisions that would affect person and entities in different ways, as have been seen from time to time from reported cases and judgments referring to CSIS intelligence, these should be examined separately on the basis that they represent distinct decisions and processes made under a distinct statutory framework that those governing the security intelligence agency.\(^{179}\)

\(^{176}\) The question of the principles to apply in seeking to determine if the Court is faced with criminal matters was the focus of comments in Wholesale Travel (then looking at section 7 of the Charter), where Lamer C.J. and Sopinka J. added a nuance in considering the application of section 7 to provisions permitting imprisonment for strict liability offences:

> Much has been made in this case of the fact that the Competition Act is aimed at economic regulation. … A person whose liberty has been restricted by way of imprisonment has lost no less liberty because he or she is being punished for the commission of a regulatory offence as opposed to a criminal offence. Jail is jail, whatever the reason for it. In my view, it is the fact that the state has resorted to the restriction of liberty through imprisonment for enforcement purposes which is determinative of the principles of fundamental justice. …. Indeed, while I agree that this offence can be characterized as "regulatory", the label loses much of its relevance when one considers that an accused faces up to five years' imprisonment upon conviction. (At para 42.)

\(^{177}\) In Thomson, supra note 71 at 95: “What is important is not so much that the strict criteria be mechanically applied in every case but that the legislation respond in a meaningful way to the concerns identified by Dickson J. in Hunter. This having been said, however, it would be my view that the more akin to traditional criminal law the legislation is, the less likely it is that departures from the Hunter criteria will be countenanced. This seems to be what Dickson… had in mind when he said in R v Simmons (1988) … that departures from the Hunter criteria will be exceedingly rare”.

\(^{178}\) One of the main feature of criminal law is that it carries the risk for an accused to be deprived of liberty. Indefinite detention under security certificate provisions of the Immigration and Refugee Protection Act as they stood then was one factor that led the Court to conclude that principles of fundamental justice were breached in the matter of Charkaoui 1 supra note 12.

\(^{179}\) The question of the standard applicable at the time information from CSIS or from CSE is received and used is also interesting and could be the subject of a thesis of its own right, with decisions of the Court in Wakeling, supra note 93 and R v Jarvis, 2002 SCC 73, [2002] 3 SCR 757 offering interesting possibilities.
It appears clear that national security intelligence represents a unique construct for purposes of section 8. Its particularities have been described in this paper, and also contrasted with those of law enforcement. How would they influence the nature and scope of the standard that would apply under section 8? As noted above, strict adherence to the Hunter standard is not what is required; what is necessary is to give life to the principles underlying section 8.

Security intelligence is developed for the purpose of advising the government, assisting in deciding orientations and developing policies and as a predictive and forewarning instrument. These are not areas that would generally lead to matters that would be brought before the courts. In addition, at the time the information is collected, which is where section 8 is most likely to be engaged, the ultimate and exact use(s) that recipient government institutions may make of the information is unknown. Contrary to what is the case in a usual police investigation, for example, where information is collected for purpose of investigating a known crime and laying charges, the national security investigation is open ended and has for objective to generate a more advanced form of information.

Indeed, the matters that led the courts to consider questions related to national security intelligence are almost all related to decisions made by departments and agencies such as the RCMP, Immigration and Citizenship Canada or the Canadian Border Service Agency (or their responsible ministers) acting upon their own constitutive statute and where the information they relied upon originated, in parts small or large, from advice provided by national security agencies. Where it not for such reliance, therefore, there would be little opportunities for the courts to become involved. In Mahjoub, the Federal Court of Appeal remarked that the fact that a matter (there, a warrant issued under s. 21) may be hard to challenge in some context does not logically lead to the conclusions it should be subject to a different test for purposes of challenging the validity of the warrant under Garofoli. In Hunter, the Court also distinguished between a matter not being reviewable (which would have been problematic) and not being reviewed.

---

180 Mahjoub, supra note 28 at para 267.
181 Hunter, supra note 4 at 166.
Even when security intelligence advice could provide such a basis for government action, it may not be relied upon to make decisions in administrative context or a prosecution may not proceed for a number of reasons. This is linked in large part to the requirements to ensure that sensitive information be protected from disclosure. In his report concerning the events relating to Maher Arar, the Honourable Dennis O’Connor illustrates this point when, in discussing the role of the RCMP, cited the need to protect Canada’s foreign relations, the security of sources of information or sharing protocols with other countries as underlying decisions not to lay charges.\(^{182}\)

More generally, the secrecy that constitutes feature of investigations, collection and retention of information would not allow for the main forms of accountability discussed in *Tse* and *Wakeling*.

Finally, while it obeys to certain principles that were developed to suit its intended uses, security intelligence is certainly not developed to serve as formal evidence and some of its characteristics and conditions attached to its use renders it unsuitable for it.

As Justice O’Connor also noted after his own examination, factors that would make it less likely that a Court would be called upon to play a judicial control role also lead to a risk that rights and freedoms be eroded more easily.\(^{183}\) That risk can certainly not be ignored. But the answer to this cannot then be to automatically conclude to a breach of section 8. The Court in *Hunter* was aware that the exact element of the test it established could not always be used. This was also recognized, in relation to section 7 of the Charter, in the matter of *Charkaoui 1* where the Court acknowledges that the exigencies of the security context may dictate different procedural requirements relevant to fundamental justice with the caveat that they cannot be permitted to erode the essence of s. 7 “to the point where they cease to provide the protection of due process that lies at the heart of s. 7 of the *Charter*”.\(^{184}\)


\(^{183}\) *Ibid* at 440.

\(^{184}\) The Court added the precision: “The protection may not be as complete as in a case where national security constraints do not operate. But to satisfy s. 7, meaningful and substantial protection there must be.” *Charkaoui 1*, *supra* note 12 at 27.
And, as with the standard itself, the applicability of the four elements of *Hunter* is to be informed by the context and purpose of the s. 8 search. Where, as here, that context and purpose are such that the application of the standard and its elements would not realistically result in support for the guarantee, other approaches may be explored. As noted above, the Court certainly considered this a possibility in the matters of *Tse* and *Wakeling*, where the Court referred to forms of record-keeping and to the need to consider an entire scheme rather than specific individual provisions when assessing accountability.

In my view, the presence of robust review mechanisms may palliate, at least to a large extent, the limited opportunities for prior, or post, judicial approval. Indeed, in discussing that point in his report Justice O’Connor commented that due to the nature of national security investigations, the reduced level of judicial oversight acts as further justification for independent review.

This brings us to the principles set in *Hunter* that the purposes of s. 8 would not be served by a determination of the balance of competing interests that is made after a search was conducted. As a result, a system of prior authorization by an officer capable of acting judicially rather than one of subsequent validation would be required, with warrantless searches presumed unreasonable.\(^{185}\) CSIS already operates under a system of judicial authorizations for some of its activities. Section 21 of the *CSIS Act* sets out a warrant scheme that meets the *Hunter* requirements, as was found in *Atwal* and *Mahjoub*. CSIS may also conducts searches without judicial authorizations. Section 12 of the *CSIS Act* for its part, enables CSIS to collect information as is strictly necessary to investigate activities that there are reasonable grounds to suspect constitute threats to the security of Canada.

In *Mahjoub*, the Federal Court of Appeal agreed that section 12 was constitutional in light of the “minimally intrusive” nature of the searches at issue there. In using section 12, as in all of its other activities, CSIS is subject to review and oversight mechanisms that will be augmented by the coming into force of the legislation creating the National Security and Intelligence Committee of Parliamentarians and, if bill C-59 was to be adopted by Parliament, by an expanded review function for a revamped SIRC and the arrival on the scene of another review

---

\(^{185}\) *Hunter*, supra note 4 at 160.
and oversight body, the Intelligence Commissioner. Further to Tse and Wakeling, I am proposing that in the area of national security intelligence, the existence of solid review and oversight mechanisms as described above can play a role that would compensate to a degree an absence of prior judicial oversight. These would be strengthened even more by the establishment of the new Committee of Parliamentarians, and possibly eventually the adoption of review and oversight schemes as set out in bill C-59 or similar to them.

In another series of decisions germane to the application of section 8, the Court examined searches carried out in a variety of situations where prior approvals were not obtained (often organizing its findings around the Collins criteria). The Court’s analysis has tended to focus on the degree of intrusion of the investigative or collection methods used or the level of the expectation of privacy as modulated by the context a quo. Generally in contexts that were non criminal, the Court often followed a finding that it was on a low end by a conclusion that the searches were valid. This accorded with the instruction provided in Thomson where La Forest J. linked the threshold of constitutional justification to the degree of intrusion. The above noted finding of the Court of Appeal in Mahjoub illustrates a similar conclusion in relation to CSIS. How far along on the spectrum could the reasoning apply?

At the upper end, a limit would arise where the circumstances of the expectation of privacy or of the intrusion creates a ‘particularly compelling’ situation, as referred to above where I provided as examples interceptions of communications, searches of residences or searches of computers. While the Federal Court of Appeal did not refer to the Charter in that regard, it may have had this concept in mind in the matter of X (Re) that concerned of situations where CSIS seeks the assistance of foreign agencies by asking them to intercept communications of Canadians abroad, under their own mandates and authorities. The Court of Appeal found that a judicial authorization was required to make such a request, due to the intrusiveness of the measure.186

As was seen above, in many cases, the lower expectation of privacy or lesser intrusion resulted in the court accepting that a ‘reasonable ground to suspect’ standard could apply with regard to elements that the government needed to establish. If we continue to use CSIS as an example,

---

section 12 sets out a statutory requirement whereby there must be reasonable grounds to suspect that activities constitute a threat to the security of Canada before CSIS can collect information under its authority. It also requires that information be only collected, and retained, to the extent strictly necessary. The provision sets clear limits to the power. As reiterated more recently in *Chehil*:

Both the impact on privacy interest and the importance of law enforcement objective play a role in determining the level of justification required for the state to intrude upon the privacy interest in question. In *Hunter*, this Court also recognized that this balancing of interest can justify searches on a lower standard where privacy interests are reduced, or where state objectives of public importance are predominant.\(^{187}\)

What I am proposing therefore for national security intelligence is an approach *sui generis* that would result in the point of equilibrium between the state’s interests and privacy, as represented by the reasonableness of a search, residing a different plane than for other types of searches considered by the courts. That approach would meet the principles underlying *Hunter* in a way and manner that are compatible and adapted to the particular context of national security intelligence. In this context, the state interest would be at its highest, on par with that of maintaining the criminal law system.

Assessing reasonableness would be done by considering the degree of intrusion and the level of the expectation of privacy and then adopting a standard to assess intrusive intelligence activities having regard to the statutory provisions regulating the collection (which would not necessarily always weight equally in favour of the validity of the search, depending on the provision) as per the well-established requirement to consider the totality of circumstances. This would be examined along with the framework to which they relate and having regard also to the safeguards provided by the nature and scope of the review and oversight mechanisms. That would also accord with the approach taken in matters such as *Colarusso*, where the Court commented positively on the seizure of blood by a coroner having regard the important non-criminal function performed by a coroner and the necessity to use investigatory powers to that effect. This balancing exercise may result in searches being found to be reasonable in this context that would not be found so in a law enforcement context. I would expect that the standard may begin to slide

\(^{187}\) *Chehil*, supra note 90 at para 23.
toward a threshold of reasonable suspicion at earlier points than it would in criminal matters, becoming closer to those applicable to regulatory enforcement, this being modulated by the degree of intrusion or the level of the expectation of privacy. Review and control mechanisms would play a pivotal role in helping ensure that rights guaranteed by the Charter continue to be upheld whenever they may become engaged in the course of national security intelligence activities.