McGill Law Journal
Revue de droit de McGill

Interjurisdictional Information Sharing and National Security: A Constitutional and Legislative Analysis

Jacques J.M. Shore, Brian A. Crane and John J. Wilson

Volume 62, Number 1, September 2016

URI: https://id.erudit.org/iderudit/1038712ar
DOI: https://doi.org/10.7202/1038712ar

See table of contents

Publisher(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (print)
1920-6356 (digital)

Explore this journal

Cite this article

Shore, J. J., Crane, B. A. & Wilson, J. J. (2016). Interjurisdictional Information Sharing and National Security: A Constitutional and Legislative Analysis. *McGill Law Journal / Revue de droit de McGill*, *62*(1), 207–239. https://doi.org/10.7202/1038712ar

Article abstract

This article analyzes whether there are constitutional arguments that help or hinder the flow of information between the different levels of government in Canada. The duty to share information is acutely important to the protection of Canadian citizens and the maintenance of public order, responsibilities that often overlap the federal and provincial competencies. This article concludes that the Canadian constitution and its unwritten principles, such as co-operative federalism, demonstrate support for interjurisdictional information sharing. The true weakness in information sharing can largely be found in institutional and cultural impediments. It is critical for federal and provincial government agencies to work past these impediments to share information, thus fulfilling their obligations to protect the public and maintain order.

INTERJURISDICTIONAL INFORMATION SHARING AND NATIONAL SECURITY: A CONSTITUTIONAL AND LEGISLATIVE ANALYSIS

*Jacques J.M. Shore, Brian A. Crane, and John J. Wilson**

This article analyzes whether there are constitutional arguments that help or hinder the flow of information between the different levels of government in Canada. The duty to share information is acutely important to the protection of Canadian citizens and the maintenance of public order, responsibilities that often overlap the federal and provincial competencies. This article concludes that the Canadian constitution and its unwritten principles, such as cooperative federalism, demonstrate support for interjurisdictional information sharing. The true weakness in information sharing can largely be found in institutional and cultural impediments. It is critical for federal and provincial government agencies to work past these impediments to share information, thus fulfilling their obligations to protect the public and maintain order.

Cet article examine les arguments constitutionnels qui viennent en aide ou font obstacle aux échanges d'information entre les différents niveaux du gouvernement canadien. L'obligation de partage d'information est cruciale pour assurer la protection des citoyens canadiens et le maintien de l'ordre public, responsabilités qui chevauchent souvent les compétences fédérales et provinciales. Cet article conclut que la constitution canadienne et ses principes non-écrits, tel que le fédéralisme coopératif, se montrent en faveur du partage d'information. La véritable faiblesse de ce partage d'information se trouve en grande partie au sein d'obstacles institutionnels et culturels. Il est primordial pour les agences gouvernementales fédérales et provinciales de travailler à combattre ces obstacles au partage d'information, pour ainsi remplir leurs obligations de protection des citoyens et de maintien de l'ordre.

* Jacques J.M. Shore and Brian A. Crane are partners at Gowling WLG (Canada) LLP. John J. Wilson is a student-at-law at Gowling WLG (Canada) LLP. The authors wish to thank the Department of Public Safety of the Government of New Brunswick for its encouragement to publish this article, which is based on an opinion completed for the Government of New Brunswick in 2015.

Citation: (2016) 62:1 McGill LJ 207 — Référence : (2016) 62:1 RD McGill 207

Introduction

A government's obligation to protect its citizens is one of its fundamental responsibilities and a source of its political legitimacy.[1] In order for this general duty to be discharged meaningfully in today's "increasingly complex and dangerous threat environment,"[2] it is essential that government agencies share relevant information in a timely manner. Failure to do so brings disastrous consequences—this was the lesson of 9/11.[3] As the Auditor General notes, the importance of timely and accurate security intelligence "cannot be overstated".[4]

Canada's national security policy recognizes the importance of the best possible intelligence for the design, maintenance, and operation of security programs:

> Intelligence is the foundation of our ability to take effective measures to provide for the security of Canada and Canadians. To manage risk effectively, we need the best possible information about threats we face and about the intentions, capabilities and activities of those who would do us harm.[5]

The government also recognizes the need for co-operation and collaboration across jurisdictional boundaries. Indeed, following 9/11, the federal government was aware of information "stovepipes" among federal agencies and other levels of government that could prevent timely recognition of threats and hinder the effectiveness of responses.[6] As early as 2004, the Office of the Auditor General recognized that "co-operation and integration are important tools," and that government appeared to be "moving in the right direction" by making "efforts to more closely co-ordinate the collection of intelligence information and to encourage the exchange of information among analysts."[7] Unfortunately, there exist deficiencies and

---

1 See *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9 at para 1, [2007] 1 SCR 350, McLachlin CJC ("[o]ne of the most fundamental responsibilities of a government is to ensure the security of its citizens"). See also Jacques JM Shore, "An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security" (2015) 28:2 Intl J Intelligence & CounterIntelligence 236 at 237–38.

2 Privy Council Office of Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa: PCO, 2004) at iii [*Securing an Open Society*].

3 See Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008) at 434 [Forcese, *National Security Law*].

4 Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: National Security in Canada—The 2001 Anti-Terrorism Initiative*, ch 3 (Ottawa: OAG, 2004) at 14 [*National Security in Canada*].

5 *Securing an Open Society*, *supra* note 2 at 15.

6 *National Security in Canada*, *supra* note 4 at 19.

7 *Ibid* at 14.

redundancies in how intelligence is managed across the government, attributable in large part to a lack of intergovernmental coordination.[8] Indeed, government actors from various jurisdictions continue to report that the inadequate dissemination of relevant information hinders their ability to appreciate and respond to security threats. Recent events, such as the 22 October 2014 shooting on Parliament Hill, have further highlighted the importance of information sharing among provincial and federal governments generally.[9]

This article examines the constitutional, statutory, and practical constraints that influence the flow of security information in Canada. Four key findings flow from our analysis. First, despite the ostensibly sharp division of powers set out in the *Constitution Act, 1867*,[10] the judicial interpretation of these powers and the accompanying constitutional principles are compatible with the fulsome and timely sharing of security information across jurisdictions. Second, contrary to a popular sentiment held by state agencies,[11] there are no significant legislative boundaries or privacy concerns impeding such exchanges. In fact, many pieces of legislation, including the federal *Privacy Act*,[12] support the practice. The true impediments to information sharing lie in a set of nebulous institutional cultural barriers between agencies which, ultimately, share the same goals. Accordingly, we argue that government has a fundamental moral obligation to share security information across jurisdictions.

I. The Constitutional Framework

Canada does not have the advantage of being a unitary government, in which one agency (or a set of agencies) is responsible for all aspects of maintaining the country's security. This fundamental responsibility is

---

8 See *ibid* at 1.

9 See e.g. Royal Canadian Mounted Police, *External Engagement and Coordination—Parliament Hill Incident on October 22, 2014: After Action Review* (Ottawa: RCMP, 2015) at 17. The recently released RCMP review of the events characterizes the reciprocal information-sharing relationship between RCMP's National Division and the Ottawa Police Service that emerged after the events as a "[b]est [p]ractice" (*ibid*). Yet, other government reports on the event offer little insight into the way the information was managed and shared between local and federal police *before* the events took place (see e.g. Ontario Provincial Police, *Independent Investigation into the Death of Michael Zehaf-Bibeau, October 22 2014, Centre Block, Parliament Hill, Ottawa, Canada* (Ottawa: OPP, 2015); Ontario Provincial Police, *RCMP Security Posture Parliament Hill, October 22, 2014: OPP Review & Recommendations, March 2015* (Ottawa: OPP, 2015)).

10 (UK), 30 & 31 Vict, c 3, s 92(14), reprinted in RSC 1985, Appendix II, No 5.

11 See *National Security in Canada*, *supra* note 4 at 17, 22–23.

12 RSC 1985, c P-21.

shared between the federal and provincial legislatures. This Part considers the constitutional framework within which government agencies share information relevant to security threats, paying particular attention to the relevant heads of power and the principle of co-operative federalism. Ultimately, we conclude that the federal framework supports, rather than hinders, interjurisdictional information sharing.

A. The Division of Powers

The "rules of federalism" that allocate legislative powers between the federal and provincial governments are established in sections 91 and 92 of the *Constitution Act, 1867*.[13] The principle of federalism, in turn, recognizes the autonomy of the provinces, while providing the central government with exclusive jurisdiction over matters in which the provinces have a common interest.[14]

It is well established that "national security" is predominantly a federal responsibility, flowing from either the residual "Peace, Order, and good Government" power under section 91 or the defence power under subsection 91(7).[15] Also relevant is Parliament's plenary jurisdiction to pass laws in relation to criminal law and criminal procedure under subsection 91(27).

Pursuant to these powers, the federal government has established a security intelligence agency under the *Canadian Security Intelligence Service Act*,[16] and crafted a national security policy, *Securing an Open Society*, which identifies and addresses a number of "core national security interests."[17] Under the *Security Offences Act*, the Royal Canadian Mounted Police (RCMP) has the primary responsibility to investigate, prevent, and prosecute criminal activities relating to national security.[18]

The term "national security", describes the sphere of activity in which the federal government has an overarching interest. The term has proven, however, to be somewhat nebulous, particularly because descriptions of "national security" in legislation and policy provide little direction as to its content. One commentator writes, "[T]he descriptions do little to define

---

13 Peter Hogg, *Constitutional Law of Canada*, 5th ed (Toronto: Carswell, 2007) (loose-leaf updated 2015, release 1) vol 1 at 1-3.

14 See *Reference re Secession of Quebec*, [1998] 2 SCR 217 at para 58, 161 DLR (4th) 385 [*Secession Reference*].

15 See Hogg, *supra* note 13 at 19-13.

16 RSC 1985, c C-23 [*CSIS Act*].

17 *Securing an Open Society*, *supra* note 2 at iii.

18 See *Security Offences Act*, RSC 1985, c S-7, ss 2, 6(1).

exactly when threats of the sort listed in the definitions constitute national security concerns. For example, when is a threat to the physical safety of Canadians a legitimate 'national security' concern rather than a regular policing matter?"[19]

The corresponding provincial head of power is subsection 92(14), which assigns authority over "[t]he Administration of Justice in the Province."[20] The scope of subsection 92(14) has been interpreted very broadly, encompassing a variety of responsibilities relevant to public order and security. The most relevant provincial responsibility is the power to police, investigate, and prosecute offences under the *Criminal Code*.[21]

Justice Dickson, concurring with the majority in *Di Iorio v. Warden of the Montreal Jail*[22] (*Di Iorio*), explained provincial responsibilities as follows:

> Since Confederation, the provincial departments of the Attorney General have in practice "administered justice" in the broadest sense, at great expense to the taxpayers, and irrespective of whether the laws being administered fell legislatively within the purview of provincial legislatures or the federal Parliament. This is reflected in the provision of police services and other enforcement agencies responsible to the provincial Attorneys General for the investigation, detection and control of crime within the respective provinces and in the maintenance of staffs for the prosecution of all types of infractions whether within the purview of provincial legislatures or the federal Parliament.[23]

Justice Beetz, also writing in *Di Iorio*, explained the historical basis for provincial authority:

> Before Confederation, the provinces were in charge of the administration of justice, including criminal justice. It was contemplated by s. 91(27) of the *British North America Act*, *1867*, that criminal law, substantive and procedural, would come under the exclusive legislative authority of the Parliament of Canada. But subject to this provision and to the paramountcy of federal law enacted under primary or ancillary federal jurisdiction, the provinces were to remain responsible in principle for the enforcement of criminal law and to retain such power as they had before with respect to the administration of criminal justice. They continued in fact to police their respective territories, to investigate crime, to gather and to keep records

---

19 Craig Forcese, "Through a Glass Darkly: The Role and Review of 'National Security' Concepts in Canadian Law" (2006) 43:4 Alta L Rev 963 at 967.

20 *Constitution Act, 1867*, *supra* note 10, s 92(14).

21 See Hogg, *supra* note 13 at 18-2.

22 [1978] 1 SCR 152, 73 DLR (3d) 491 [*Di Iorio* cited to SCR].

23 *Ibid* at 200.

> and informations relating to crime, to prosecute criminals and to supervise police forces, sheriffs, coroners, fire commissioners, officers of justice, the summoning of juries, recognizances in criminal cases, and the like.[24]

Since *Di Iorio*, the power to administer justice "in the broadest sense" has been interpreted to allow provinces to hold inquiries into specific criminal activities,[25] to suppress crime related to matters of provincial competence,[26] and to discipline the provincial and municipal police.[27] Thus, despite the federal government's jurisdiction over criminal law and criminal procedure, the provinces bear the primary responsibility for local criminal law investigation and enforcement, or as some commentators have put it, "local public order and morality."[28]

Of course, the local responsibility to maintain public order is also discharged by municipal governments exercising authority delegated to them under provincial legislation. New Brunswick's *Police Act*, for example, provides that every municipality is responsible for providing and maintaining adequate police services within its boundaries, and invests a chief of police with all powers necessary to do so.[29]

These broad spheres of provincial and federal jurisdiction inevitably overlap. The existence of overlap has prompted cooperative arrangements between federal and provincial agencies, rather than narrow, legalistic boundary drawing. As stated in the 1940 *Report of the Royal Commission on Dominion-Provincial Relations*, "The different aspects of life in a society are not insulated from one another in such a way as to make possible a mechanical application of the division of powers. There is nothing in human affairs which corresponds to the neat logical divisions found in the constitution."[30] Governmental responsibility for public safety and public order is no exception.

The division of powers accommodates these instances of overlap with particular arrangements between federal and provincial agencies, which draw their authority from a combination of valid federal and provincial statutes. An example of such intergovernmental arrangements is the for-

---

24 *Ibid* at 223.

25 See *Keable v Canada (AG)* (1978), [1979] 1 SCR 218 at 241, 90 DLR (3d) 161.

26 See *Arkinstall v Surrey (City of)*, 2008 BCSC 1419 at para 99, 300 DLR (4th) 232.

27 See *Hamalengwa v Bentley*, 2011 ONSC 4145 at para 30, 207 ACWS (3d) 20.

28 Guy Régimbald & Dwight Newman, *The Law of the Canadian Constitution* (Markham: Lexis Nexis, 2013) at 245.

29 See *Police Act*, SNB 1977, c P-9.2, ss 3(1), 3.1(3)(b).

30 *Report of the Royal Commission on Dominion-Provincial Relations*: *Canada, 1867–1939*, book 1 (Ottawa: King's Printer, 1940) at 31.

mation of policing contracts between the RCMP and the provinces. These contracts are authorized, on the one hand, by the *Royal Canadian Mounted Police Act*,[31] and on the other, by companion provisions in provincial police legislation.[32]

Provincial institutions have a defined and legitimate interest in the maintenance of public order and security, in particular with respect to criminal law. Inevitably, intelligence in the possession of federal institutions will be very relevant to fulfilling this provincial role.

In our view, there are compelling reasons for sharing national security information across federal and provincial agencies to the fullest extent possible, within the boundaries set by their governing legislation. Indeed, as we go on to show below, the meaningful discharge of both federal and provincial constitutional responsibilities likely requires inter-agency information sharing.[33]

B. Co-operative Federalism

In recent years, the Supreme Court of Canada has given new life to the principle of "co-operative federalism". The Court has held that co-operative federalism is a "legal principle that has been invoked to provide flexibility in separation of powers doctrines, ... used to facilitate interlocking federal and provincial legislative schemes and to avoid unnecessary constraints on provincial legislative action."[34] It is one of the recognized constitutional principles that "infuse the analysis and interpretation of the division of powers,"[35] and as such helps to delineate the "spheres of jurisdiction, the scope of rights and obligations, and the role of our political institutions."[36]

In *Canadian Western Bank v. Alberta*, the Court held that the constitution "serves as a framework for life and for political action within a federal state, in which the courts have rightly observed the importance of co-operation among government actors to ensure that federalism operates flexibly."[37] Underlying the principle of co-operative federalism is the idea that the Canadian federal state is a collaborative enterprise requiring co-

---

31 RSC 1985, c R-10, s 20.

32 See e.g. *Police Act*, *supra* note 29, s 2.

33 See *Securing an Open Society*, *supra* note 2 at 15.

34 *Quebec (AG) v Canada (AG)*, 2015 SCC 14 at para 17, [2015] 1 SCR 693 [*Quebec v Canada*].

35 *Ibid* at para 144.

36 *Secession Reference*, *supra* note 14 at para 52.

37 *Canadian Western Bank v Alberta*, 2007 SCC 22 at para 42, [2007] 2 SCR 3.

operative and flexible arrangements between levels of government, a notion that tends to inform the Supreme Court's analysis of division of powers questions. For instance, when applied to the doctrine of interjurisdictional immunity, the principle of co-operative federalism has been used as a justification to relax a strict "watertight compartments" view of the division of powers, where doing so would avoid imposing unnecessary constraints on the legislative powers of one level of government.[38]

The principle of co-operative federalism was considered in 2015 in *Quebec (Attorney General) v. Canada (Attorney General)*,[39] where Quebec challenged section 29 of the *Act to amend the Criminal Code and the Firearms Act*,[40] an aspect of federal legislation that ordered the dismantling of the federal long-gun registry. Quebec argued that the principle of co-operative federalism prevented the federal government from acting or legislating in a way that would hinder ongoing co-operative arrangements between governments, especially in areas of concurrent jurisdiction. The majority of the Supreme Court disagreed, finding that "[n]either th[e] Court's jurisprudence nor the text of the *Constitution Act, 1867* supports using that principle to limit the scope of legislative authority or to impose a positive obligation to facilitate cooperation where the constitutional division of powers authorizes unilateral action."[41] There is no question, however, that the principle applies to situations involving overlapping federal and provincial jurisdictions. As demonstrated in the division of powers analysis above, governmental responsibility for public safety and order is one such overlapping jurisdiction. It follows, therefore, that the principle supports ongoing cooperation between federal and provincial governments in matters of national security.

Co-operation between the federal and provincial governments in the administration of justice has occurred with great success in areas relevant to our present concern. Of particular note is the provinces' use of RCMP officers through an arrangement whereby the federal government confers on provincial officials the power and responsibility to apply federal laws[42]—what Professor Lederman calls the "administrative type of intergovernmental delegation."[43] Such arrangements, through which eight of

---

38 See *ibid* at paras 36–37.

39 *Supra* note 34.

40 RSC 2012, c 6.

41 *Quebec v Canada*, *supra* note 34 at para 20. See also *Rogers Communications Inc v Châteauguay (City of)*, 2016 SCC 23 at para 39, 117 LCR 215.

42 See e.g. *Police Act*, RSA 2000, c P-17, s 21(1).

43 WR Lederman, *Continuing Canadian Constitutional Dilemmas* (Toronto: Butterworths, 1981) at 321–22, 327.

the ten provinces employ the RCMP to enforce both provincial and federal laws, point to one instance of delegation that "has brought valuable and indispensable elements of flexibility to our federal system."[44] This type of flexibility is increasingly needed as the nature and complexity of security threats change and expand beyond borders.

C. Conclusions on the Constitutional Framework

Our analysis shows that Canada's constitutional framework and constitutional doctrine do not impose significant impediments on, but rather support information sharing.

Both the provincial and federal levels of government have equally well-established constitutional interests in maintaining public safety and security, in support of government's larger, more general obligation to protect its citizens. Moreover, because of the vital importance of information in the apprehension, prevention, and response to security threats, the meaningful discharge of both federal and provincial interests may require timely and comprehensive information sharing. Events such as the Air India bombing and 9/11 provide painful reminders of the consequences that may follow from the inadequate dissemination of intelligence.

Similarly, the doctrine of co-operative federalism supports enhanced collaboration between different levels of government and government agencies. Such collaboration, in matters of security, includes meaningful and timely information sharing, especially in light of the dangers of withholding critical intelligence.

II. Potential Impediments to Information Sharing

We now examine impediments to information sharing across government agencies. It should be noted that the analysis below proceeds on the assumption that the persons receiving and using the information through inter-agency disclosure are persons with the appropriate security clearance.

A. Legislation

Following 9/11, a series of reforms increased legislative protection for information that could be injurious to national security. For example, section 38 of the *Canada Evidence Act* was amended to include a scheme to limit the disclosure of broadly defined "sensitive" or "potentially injurious"

---

[44] *Ibid* at 327.

information.[45] Similarly, under the security certificate process set out in the *Immigration and Refugee Protection Act*, a judge can prohibit the disclosure of evidence in deportation proceedings if that evidence is deemed "injurious to national security."[46] Finally, the federal *Privacy Act* allows for the denial of access to information where the information requested was obtained in the course of an investigation into "threats to the security of Canada,"[47] defined in the *Canadian Security Intelligence Service Act* (*CSIS Act*).[48]

These statutes work to limit the public disclosure of information where that information is relevant to national security concerns. We must, however, avoid conflating limits on public disclosure with limits on intergovernmental information sharing. A review of these statutes demonstrates that necessary limits on public disclosure do not include limits on intergovernmental disclosure of information.

1. Federal Statutes Explicitly Encouraging Information Sharing

Two statutes expressly require collaboration and information sharing in the context of public safety. The first is the *Department of Public Safety*

---

45 *Canada Evidence Act*, RSC 1985, c C-5, s 38. The *Act* defines "sensitive information" as information "in the possession of the Government of Canada" that relates to international relations, national defence, or national security (*ibid*, s 38, *sub verbo* "sensitive information"). "Potentially injurious information" is more broadly defined as "information of the type that, if it were disclosed to the public, could injure international relations or national defence or national security" (*ibid*, s 38, *sub verbo* "potentially injurious information").

46 *Immigration and Refugee Protection Act*, SC 2001, c 27, s 83(1)(c).

47 *Privacy Act*, *supra* note 12, s 22(1)(a)(iii).

48 The *CSIS Act*, *supra* note 16, s 2 defines "threats to the security of Canada" 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).

and Emergency Preparedness Act (*DPSEPA*),[49] which establishes a Department of Public Safety and Emergency Preparedness, and outlines the various functions of that minister:

> 6(1) In exercising his or her powers and in performing his or her duties and functions and *with due regard to the powers conferred on the provinces and territories*, the Minister may
>
> (a) *initiate, recommend, coordinate, implement or promote* policies, programs or projects relating to public safety and emergency preparedness;
>
> (b) *cooperate with any province*, foreign state, international organization or any other entity;
>
> (c) make grants or contributions; and
>
> (d) *facilitate the sharing of information*, where authorized, to promote public safety objectives.[50]

We make several observations about subsection 6(1).

First, the minister, in carrying out his or her duties, is to have "due regard" to the powers of the provinces and territories. That is, the minister is to be cognizant of the content of the roles assigned to the minister's provincial and territorial counterparts. Second, the minister has the express discretion to co-operate with any province, consistent with the spirit of co-operative federalism outlined above. Third, the provision contemplates that the minister will take active steps to facilitate information sharing, where such sharing is authorized. The language of "facilitation" is important, as it both recognizes the value of information sharing as something to be fostered and suggests that the federal minister has a responsibility to encourage such practices. While this section of the *DPSEPA* stands as a strong example of federal legislation that both recognizes the value of and encourages collaboration and information sharing across and within levels of government, this provision appears to have received no judicial consideration to date.

The second example of legislated intergovernmental co-operation and discretion to facilitate information sharing is found in the *Emergency Management Act*.[51] Under this statute, the minister of Public Safety and Emergency Preparedness "is responsible for exercising leadership relating to emergency management in Canada by coordinating, among government institutions and in cooperation with the provinces and other enti-

---

[49] SC 2005, c 10.

[50] *Ibid*, s 6(1) [emphasis added].

[51] SC 2007, c 15.

ties, emergency management activities."[52] This co-operative mandate is further developed in the section outlining the minister's responsibilities, which include "facilitating the authorized sharing of information in order to enhance emergency management."[53] Similarly, this provision has not attracted any judicial consideration thus far.

The above provisions of both the *DPSEPA* and the *Emergency Management Act* provide evidence of the parliamentary intent to encourage information sharing in the context of public safety, and, importantly, invest the federal government with the responsibility to actively promote the exchange of information. The lack of judicial consideration of these provisions, although curious, allows for the possibility of such active information sharing.

2. Federal Privacy Legislation and Information Sharing

The picture surrounding information disclosure becomes more complex when statutes deal expressly with individual privacy rights, which are both well-established and closely guarded by Canadian common law.[54]

As Justice La Forest noted in *R. v. Dyment*, the recognition and protection of information privacy is set out in the *Privacy Act*,[55] federal legislation that the Supreme Court describes as "a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society."[56] As such, the *Privacy Act* regulates the public disclosure of what it broadly defines as "personal information" in the possession of a government institution.[57]

The formal structure of the *Privacy Act* reflects the high value of the informational privacy it aims to protect. Subsection 8(1) begins with a general prohibition on the disclosure of personal information under the control of a government institution without the consent of the individual to whom it relates.

The strong sentiment in favour of non-disclosure carried by this section of the *Privacy Act*, as well as more general concerns surrounding the

---

52 *Ibid*, s 3.

53 *Ibid*, s 4(1)(r).

54 See *Ruby v Canada (SG)*, [2000] 3 FC 589 at para 166 (CA), 187 DLR (4th) 675, where the Court explains that the law recognizes and protects "three distinct 'zones' of privacy"—the territorial, the corporeal, and, of particular interest here, the informational.

55 See *R v Dyment*, [1988] 2 SCR 417 at 429–30, 55 DLR (4th) 503.

56 *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 at para 25, [2002] 2 SCR 773.

57 See *Privacy Act*, *supra* note 12, s 3, *sub verbo* "personal information".

infringement on privacy rights at large, has been cited as a reason for the non-disclosure of information across intergovernmental or inter-agency lines. The *Privacy Act* and analogous legislation, however, do not provide a legitimate legal justification for withholding security information.

The third chapter of the Auditor General's March 2004 report, "National Security in Canada: The 2001 Anti-Terrorism Initiative," provides a similar view. As a result of the frequency with which "privacy concerns" were provided by government actors as a justification for not sharing information, the 2004 report considered the merits of the justification, ultimately rejecting it:

> We noted that privacy concerns were often cited as the reasons why agencies could not exchange information. However, officials were not able to show us any legal opinions, specific references to legislation, or judgments as a basis for that position. ...
>
> We found that in some situations, departmental officials would not share or examine the possibility of sharing information, based on the assumption that it would contravene the principles of the *Privacy Act*. However, the *Privacy Act* accommodates the sharing of information among federal government agencies in a variety of situations, including for reasons of national security. We believe that some decisions not to share information were made without a proper examination of potential security concerns.[58]

As the Auditor General notes, the *Privacy Act* does not, in fact, preclude information sharing across government agencies. Rather, the general prohibition is immediately qualified by a set of exceptions, four of which expressly provide for disclosure across departmental lines in particular situations. In *Re Privacy Act (Canada)*, the Federal Court of Appeal noted that the wide range of these exceptions "unquestionably attests to the intention of Parliament to allow disclosure of personal information to persons who have no connection whatsoever with the disclosing institution and for purposes other than those for which the information was collected."[59]

The first of these exceptions, set out in paragraph 8(2)(a), is referred to as the "consistent use" exception to the *Privacy Act*'s general prohibition of personal information disclosure.[60] On this exception, personal information may be disclosed "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that

---

[58] *National Security in Canada*, *supra* note 4 at 17, 23.

[59] *Re Privacy Act (Canada)*, [2000] 3 FC 82 at para 14, 210 DLR (4th) 279 [*Re Privacy Act*].

[60] See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) at 115 [*Arar Inquiry*].

purpose."[61] For example, where personal information is gathered for one law enforcement purpose, it may be released for another such purpose, including law enforcement in other jurisdictions.[62]

The second exception in paragraph 8(2)(b) authorizes disclosure where another act or regulation of Parliament authorizes that disclosure. Where disclosure would be authorized by the more specific statute, paragraph 8(2)(b) provides that the *Privacy Act*'s general prohibition does not apply.[63] The Federal Court of Appeal, in discussing the second exception, recognized that the *Privacy Act* makes a distinction between "the collection of information, which can only be for purposes related to the activity of the institution," and "the disclosure of information, which, in most cases, is for purposes other than those for which it was collected and for purposes related to the activity of the requesting institution."[64] As such, the Court recognized that

> paragraph 8(2)(b) cannot but be interpreted as being a provision that enables Parliament to confer on any Minister (for example) through a given statute a wide discretion, both as to form and substance, with respect to the disclosure of information his department has collected, such discretion, of course, to be exercised in conformity with the purpose of the *Privacy Act*.[65]

The third exception, set out in paragraph 8(2)(e), is directly relevant to national security. Here, personal information can be disclosed to an investigative body specified in the regulations[66] "for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation,"

---

61 *Privacy Act*, *supra* note 12, s 8(2)(a).

62 See Forcese, *National Security Law*, *supra* note 3 at 441; *Arar Inquiry*, *supra* note 60 at 115.

63 Retired Commodore Eric Lehre provides the following illustrative example, citing paragraph 107(4)(h) of the *Customs Act*, RSC 1985, c 1 (2nd Supp). He states,

> Para[graph] 8(2)(b) [of the *Privacy Act*] authorizes transfer if another act, say the *Customs Act*, authorizes information release to other government bodies. The *Customs Act* does so, authorizing other institutions "access" to customs data if, for example, it "is reasonably regarded by the official to be information relating to the national security or defence of Canada" (Canadian Defence & Foreign Affairs Institute, "'Connecting the Dots' and the Canadian Counter-terrorism Effort: Steady Progress or Technical, Bureaucratic, Legal and Political Failure?" by Eric Lehre (Cmdre ret'd) (Calgary: CDFAI, March 2009) at 9 [Lehre, "Connecting the Dots"]).

64 *Re Privacy Act*, *supra* note 59 at para 17.

65 *Ibid* at para 18.

66 For a list of "investigative bodies", see *Privacy Regulations*, SOR/83-508, Schedule III. These bodies include, *inter alia*, CSIS, Canadian Forces Military Police, the RCMP, and the Canadian Forces National Counter-Intelligence Unit.

where that body provides a written request that "specifies the purpose and describes the information to be disclosed."[67]

Under the fourth exception pursuant to paragraph 8(2)(f), personal information may be disclosed under "agreements" or "arrangements" with the provinces, "for the purpose of administering or enforcing any law or carrying out a lawful investigation."[68] The breadth of this exception provides an opportunity for the disclosure of information across levels of government. Indeed, provided there is some pre-existing arrangement in place, it seems difficult to imagine instances where the *Privacy Act* would preclude the disclosure of personal information in the possession of one of the government institutions. Furthermore, in light of the breadth of what is captured by the *Privacy Act*'s definition of "personal information," the content of what can be exchanged is appreciably wide in scope.[69] For these reasons, paragraph 8(2)(f) is a tool whereby security information might be shared between governments. As such, it would be difficult for a federal official to claim that information cannot be released where such an agreement or arrangement exists.

In addition to these four exceptions, the *Privacy Act* includes a discretionary provision, paragraph 8(2)(m), which allows for disclosure where, "in the opinion of the head of the institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates."[70] The first branch of this catch-all provision is particularly applicable to the argument at hand, which relies on government's shared obligation to one aspect of the public interest—namely, the safety and security of Canadian citizens. Nothing in paragraph 8(2)(m) precludes the sharing of information to institutions beyond federal departments and agencies, such as relevant departments of provincial governments.

Taken together, these exceptions significantly reduce the legitimacy of an agency's reliance on *Privacy Act* concerns to justify non-disclosure of relevant security information. Seen in this light, the federal *Privacy Act*

---

67 *Privacy Act*, *supra* note 12, s 8(2)(e).

68 *Ibid*, s 8(2)(f).

69 See *ibid*, s 3, which defines personal information as meaning "information about an identifiable individual that is recorded in any form," including, *inter alia*: information relating to personal characteristics; medical, criminal, or employment history; address, fingerprints, or blood type; confidential and private correspondence with the government. This list is meant to be illustrative and non-exhaustive.

70 *Ibid*, s 8(2)(m).

represents a tool for information sharing between federal and provincial governments, rather than a justification for withholding information.

3. The *CSIS Act*

The *CSIS Act* establishes the Canadian Security Intelligence Service (CSIS), a security intelligence agency whose mandate does not include law enforcement. Rather, CSIS' central function is to collect, analyze, and retain information and intelligence on "threats to the security of Canada."[71] To this end, the *CSIS Act* provides for a judicial warrant system that authorizes CSIS to invade individual privacy where, *inter alia*, it "believes, on reasonable grounds, that a warrant ... is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada."[72] As a result, CSIS' information-gathering powers are substantial. Warrants issued under this system authorize the collection of a wide variety of information and evidence, as persons to whom the warrant is directed are authorized to

> intercept any communication or obtain any information, record, document or thing and, for that purpose,
>
> (a) to enter any place or open or obtain access to any thing;
>
> (b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
>
> (c) to install, maintain or remove any thing.[73]

Our immediate interest lies in the ways in which intelligence gathered by CSIS may be disclosed to other agencies and governments for the purpose of discharging the state's general, shared obligation to the safety of its citizens. To this end, several provisions of the *CSIS Act* are relevant. The first is section 17, which provides, *inter alia*, that the Service can enter into co-operative arrangements with any federal or provincial government department or any provincial police force:

> 17(1) For the purpose of performing its duties and functions under this Act, the Service may,
>
> (a) with the approval of the Minister, *enter into an arrangement or otherwise cooperate with*
>
> (i) *any department of the Government of Canada or the government of a province or any department thereof*, or

---

71 *CSIS Act*, *supra* note 16, s 12(1).

72 *Ibid*, s 21(1).

73 *Ibid* at s 21(3).

> (ii) *any police force in a province, with the approval of the Minister responsible for policing in the province*; or
>
> (b) with the approval of the Minister after consultation by the Minister with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.[74]

Clearly, this provision of the *CSIS Act*, like paragraph 8(2)(f) of the *Privacy Act*, can operate as a means of structuring co-operative relationships and facilitating information sharing. Indeed, a number of such channels have been developed. The Security Intelligence Review Committee reported that, as of 31 March 2006, CSIS had established twenty-nine memoranda of understanding with domestic partners to facilitate information exchange, ten of which were with provincial and municipal entities, including police forces.[75] In this context, subparagraph 17(1)(a)(ii) of the *CSIS Act* creates an inherent ambiguity as to whether federal and provincial ministers are obliged to share information. More specifically, there are no exact details that identify how approval for information-sharing agreements can be granted by both federal and provincial ministers. These types of ambiguities can result in either the expansion or restriction of the powers to facilitate information sharing, depending on how they are interpreted by federal security officials.

The content of the information that can flow through these co-operative arrangements is limited by subsequent sections of the *CSIS Act*. The first of these is section 18, which provides:

> 18(1) Subject to subsection (2), no person shall knowingly disclose any information that they obtained or to which they had access in the course of the performance of their duties and functions under this Act or their participation in the administration or enforcement of this Act and from which could be inferred the identity of an employee who was, is or is likely to become engaged in covert operational activities of the Service or the identity of a person who was an employee engaged in such activities.
>
> (2) A person may disclose information referred to in subsection (1) for the purposes of the performance of duties and functions under this Act or any other Act of Parliament or the administration or enforcement of this Act or as required

---

74 *Ibid*, s 17(1) [emphasis added].

75 See Security Intelligence Review Committee, *SIRC Annual Report, 2005–2006: An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2006) at 34. Presumably, this number has increased since 2006.

> by any other law or in the circumstances described in any of paragraphs 19(2)(a) to (d).[76]

Subsection 18(1) of the *CSIS Act* is a general prohibition to stop any person from disclosing information obtained or accessed under the *CSIS Act* which may lead to the identification and compromising of human intelligence sources. This provision "reflects the continued emphasis on secrecy that carried over from the RCMP Security Service to CSIS."[77] Subsection 18(2), however, states that CSIS information may be disclosed for a variety of purposes, such as the enforcement of the *CSIS Act* itself, if required by any other law, and, in particular, in the circumstances described in the paragraphs of 19(2).

Subsection 19(2) of the *CSIS Act* contemplates exceptions, not unlike those set out in subsection 8(2) of the federal *Privacy Act*, through which meaningful information sharing is made possible. After a general prohibition on disclosure in subsection 19(1), subsection 19(2) vests the Service with the discretion to disclose information in four situations:

> (a) where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province ... ;
>
> (b) where the information relates to the conduct of the international affairs of Canada ... ;
>
> (c) where the information is relevant to the defence of Canada ... ;
>
> (d) where, in the opinion of the Minister, disclosure of the information ... is essential in the public interest.[78]

Two of these exceptions merit our attention. First, paragraph 19(2)(a) provides for the disclosure of CSIS information to a peace officer of the applicable jurisdiction in an instance where, in the Service's discretion (signalled by the use of the word "may" in subsection 19(2)), the information can be used to investigate or prosecute an alleged contravention of any law in Canada or a province. The boundaries of the exception are drawn broadly and generally allow for disclosure to provincial institutions in a wide variety of instances relevant to security concerns.

The more pressing and ultimate question under paragraph 19(2)(a) is to what degree CSIS is willing to exercise its residual discretion to dis-

---

[76] *CSIS Act*, *supra* note 16, s 18.

[77] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (Ottawa: Public Works and Government Services Canada, 2010) vol 2, part 1 at 243 [*Air India Report*]. It should be noted that one of the present authors, Jacques J.M. Shore, acted as co-lead counsel for the Air India Victims Family Association during the Commission's inquiry.

[78] *CSIS Act*, *supra* note 16, s 19(2) [emphasis added].

close information. Commissioner John Major, citing testimony given before the Air India inquiry, describes CSIS' decision-making process under 19(2) as a "CSIS-only analysis of '... when it is appropriate to pass information of that nature, in what circumstances,'" and whether there are policy or operations reasons for doing so.[79]

The shared general duty to protect public order and the safety of citizens discussed above may provide an additional policy reason favouring disclosure under subsection 19(2). If our analysis is correct and the provinces and federal government are partners in discharging this duty, then relevant CSIS-held information that may aid in the maintenance of public order and safety should be disclosed to the relevant peace officers in accordance with paragraph 19(2)(a).

Aside from subsection 19(2), the *CSIS Act* provides a further mechanism through which security information sharing can occur. Similar in form to paragraph 8(2)(m) of the *Privacy Act*, paragraph 19(2)(d) vests the minister with discretion to disclose information "to any minister of the Crown or person in the federal public administration." Such discretion would arise where disclosure is essential to the public interest and in the minister's opinion "that interest clearly outweighs any invasion of privacy that could result from the disclosure, to that minister or person."[80] The *CSIS Act* is silent as to whether "minister of the Crown" refers exclusively to federal ministers, and as such, the section may contemplate disclosure between federal and provincial agencies.[81] A possible impediment to information disclosure under paragraph 19(2)(d) is subsection 19(3) of the *CSIS Act*, which requires that all disclosures made under 19(2)(d) be reported to the Review Committee. Indeed, with the added pressure of review for each disclosure, subsection 19(3) may ultimately be a functional deterrent to disclosure for certain federal security officials. That is, CSIS officials, knowing that review is required for each instance of disclosure, may tend to err on the side of non-disclosure, further limiting the flow of information.

In summary, the federal legislation surveyed does not impede information sharing across levels of government, but rather provides statutory mechanisms by which meaningful information exchange may occur. The legislation provides the federal government with the tools and opportunities to choose to co-operate for our shared purposes. As retired Commo-

---

79 *Air India Report*, vol 2, part 1, *supra* note 77 at 244.

80 *CSIS Act*, *supra* note 16, s 19(2)(d).

81 The *CSIS Act* does not define the expression "minister of the Crown", nor does the federal *Interpretation Act*, RSC 1985, c I-21. The meaning of this terminology depends on the context (see Hogg, *supra* note 13 at 10-19).

dore Eric Lehre notes, the solution to coordination and data-sharing problems "lies in using the laws already available."[82] Yet, even with laws that support information sharing, government agencies such as CSIS can still interpret the law in a manner that could limit information sharing in practice. This narrow reading of the law is, in our view, inherently a problem of interpretation, culture, and institutional impediments, as discussed below. The statutory framework should not bear the blame for a lack of timely and effective information sharing.

4. Provincial Privacy and Policing Legislation

In this section, we consider as examples the privacy statutes of Alberta, Ontario, and New Brunswick, and New Brunswick's policing statute. We have limited our legislative review to these provinces due to our familiarity with these statutes through our work. We encourage further research and analysis of other provincial legislation.

Alberta's *Freedom of Information and Protection of Privacy Act*[83] is similar in form and spirit to the federal *Privacy Act*, in that it limits public disclosure of personal information held by government institutions. Importantly, like the federal *Privacy Act*, the Alberta *Privacy Act* includes a general prohibition of public disclosure, subject to a number of exceptions for intergovernmental disclosure. Several of the exceptions in subsection 40(1) of the provincial legislation, mirror those set out in the *Privacy Act*.[84] As such, the *Freedom of Information and Protection of Privacy Act* provides for widespread information sharing between government agencies.

Similarly, the *Police Act*[85] of New Brunswick constitutes a good example of legislated collaboration aimed at fulfilling the government's shared and more general obligation to public safety. Subsection 1.1(1) of the *Police Act* provides:

> 1.1(1) The Minister shall
>
> (a) promote the preservation of peace, the prevention of crime, the efficiency of police services and the development of effective policing, and

---

82 Lehre, "Connecting the Dots", *supra* note 63 at 12.

83 RSA 2000, c F-25.

84 See e.g. *ibid*, s 40(1)(e), which allows disclosure "for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada."

85 *Supra* note 29.

> (b) co-ordinate the work and efforts of police forces and the Royal Canadian Mounted Police within the Province.[86]

This opening provision at once recognizes the province's role in the preservation of peace and the prevention of crime under subsection 92(14) of the *Constitution Act, 1867*, and contemplates a co-operative scheme between the RCMP and the province. Subsequent provisions provide that the minister may, for the purposes of subsection 1.1(1), *inter alia*, consult with and advise the RCMP on matters relating to policing, and provide the RCMP with "information and advice respecting the management and operation of police forces."[87] Furthermore, under subsection 1.1(3), the minister may issue guidelines and directives to any police force within the province for the purposes set out in 1.1(1). In our view, nothing in the *Police Act* would impede the flow of information from the RCMP to the province. Rather, the *Act* appears to contemplate a structure of co-operation.

Similar to the federal *Privacy Act* and the Alberta *Freedom of Information and Protection of Privacy Act*, the New Brunswick *Right to Information and Protection of Privacy Act*[88] provides a right of access to information in records under the control of the province, while still recognizing the need for mandatory and discretionary exceptions to disclosure and protecting the privacy of New Brunswick residents with respect to their personal information held by government institutions.[89]

The Ontario *Freedom of Information and Protection of Privacy Act*[90] and *Municipal Freedom of Information and Privacy Act*[91] provide a right of access to information in records under the control of the provincial and municipal governments, while recognizing the need for exceptions to the right of access, in addition to protecting the privacy of Ontarians with respect to their personal information held by government institutions.[92]

---

86 *Ibid*, s 1.1(1).

87 *Ibid*, s 1.1(2).

88 SNB 2009, c R-10.6.

89 See e.g. *ibid*, ss 7, 37(1). See also *Energy and Utilities Board Act*, SNB 2006, c E-9.18, s 34; *Mining Act*, SNB 1985, c M-14.1, s 18 (which contain confidentiality clauses recognizing the possibility of divulging confidential information in the public interest).

90 RSO 1990, c F.31 [*Ontario Privacy Act*].

91 RSO 1990, c M.56.

92 See e.g. *ibid*, ss 4(1), 14(1), 28, 31–32; *Ontario Privacy Act*, *supra* note 90, ss 10(1), 21(1), 38(2), 39(1).

B. Extra-Legal Impediments: Institutional and Cultural Barriers

The foregoing discussion supports the conclusion that there are no insurmountable legal barriers or prohibitions to the comprehensive and timely sharing of security information across federal and provincial levels of government. In fact, the legislation reviewed is capable of supporting such exchanges and practices.

Why, then, do weaknesses in information sharing continue to plague government institutions?

In our view, the reluctance to share intelligence is likely attributable to a set of more nebulous, extra-legal impediments that structure the interpersonal and inter-agency relations between state actors. Put simply, the timeliness and comprehensiveness of information exchange ultimately depends on how people and organizations relate to one another in practice.[93] In the *Air India Report*, Commissioner Major expresses as much when describing the relationship between CSIS and the RCMP:

> At present, to manage the information flow between them, the two agencies are left to devise non-statutory and non-binding mechanisms that do not interfere with their very different functions. The success of these mechanisms turns largely on the personalities of the employees in the two agencies.[94]

Commissioner Major's emphasis on the importance of human, cultural factors echoes the earlier findings of those investigating the events of 11 September 2001. As the 9/11 National Commission on Terrorist Attacks upon the United States noted, "[t]he biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information."[95]

This Part examines a set of non-legal impediments responsible for information-sharing failures, drawn from our review of several government reports and commissions of inquiry, from both Canada and the United States. We can usefully classify these impediments as "institutional" and "cultural" impediments. For the purposes of our description, institutional impediments are those which emanate from the internal organization of a government agency and its understanding of how that structure relates to

---

93 For a survey-based investigation of some of the problems plaguing joint force operations, see Stephen Schneider & Christine Hurst, "Obstacles to an Integrated, Joint Forces Approach to Organized Crime Enforcement: A Canadian Case Study" (2008) 31:3 Policing: International J Police Strategies & Management 359.

94 *Air India Report*, vol 3, *supra* note 77 at 22.

95 US, National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, by Philip Zelikow et al (New York: WW Norton, 2004) at 416 [*9/11 Commission Report*].

other agencies. "Cultural" impediments, by contrast, find their source in the principles and attitudes that make up an organization's culture or ethos.

1. The Air India Inquiry

Commissioner Major's report on the Air India inquiry is particularly relevant to our present discussion. Commissioner Major's discussion of the relationship between CSIS and the RCMP is a cautionary tale with a terrible ending. Its tragic conclusion illustrates the value of co-operation and the necessity of timely and comprehensive information sharing:

> The undeniable conclusion from the foregoing is that had information been efficiently shared among agencies rather than being retained in various silos, CSIS would have been able to assemble enough of the "mosaic" to provide a well-informed threat assessment to the RCMP. This might have been useful in a criminal investigation context, and might have prevented the destruction of Air India Flight 182 and the murder of 329 people.[96]

Here, Commissioner Major makes reference to the "mosaic effect," a concept prevalent in the intelligence and security communities. The concept recognizes that information is only ever valuable in context;[97] that is, the meaning of one piece of information is often contingent on it being appreciated alongside other seemingly unrelated or innocuous pieces of information. The mosaic effect is often invoked as a justification to withhold information. For instance, in its opening statement to the commission, the Attorney General of Canada warned that an informed reader with designs on harming national security interests could use otherwise innocuous pieces of disclosed information to build a more comprehensive picture to aid in those designs.[98] As Commissioner Major notes above, however, this property of information can also be used to argue for disclosure, so that intelligence and law enforcement can better protect those same national security interests. As will be seen below, the mosaic effect plays a prominent role in decisions surrounding information disclosure.

In the course of his review, Commissioner Major makes a series of observations about impediments to the exchange of information between CSIS and the RCMP that are still generally relevant to the institutional relationship across government agencies today, in spite of efforts to improve the situation. To the extent that these impediments still persist in institutional relations and shape decisions about information disclosure,

---

96 *Air India Report*, vol 2 part 1, *supra* note 77 at 440.

97 See *ibid* at 427.

98 See *ibid*.

they provide an explanation of why information-sharing issues persist despite a legal framework which is open to and encourages these exchanges.

2. Impediments Flowing from Overlapping Mandates

The first two institutional impediments arise from a common source: the overlap in mandates between CSIS and the RCMP. CSIS has a mandate to collect intelligence to inform the government about threats to the security of Canada,[99] whereas the RCMP has the primary responsibility to prevent and investigate crimes that constitute a threat to the security of Canada.[100] As a result of these overlapping mandates, CSIS and the RCMP are both involved in investigating the same set of activities, the number of which, as Commissioner Major explains, has increased with new legislation, including the *Anti-Terrorism Act*[101] of 2001. The *Anti-Terrorism Act* created offences for "the planning of, and the provision of assistance for, terrorist acts, whether or not the acts occur," thereby increasing the role of the RCMP in the investigation of terrorism matters previously addressed by CSIS.[102]

A review of the commission's findings discloses two institutional responses to this overlapping mandate, both of which restricted the flow of information. The first can be characterized as an overemphasis on the fulfillment of each agency's independent interests. When requests for information disclosure were submitted, strident assertions of the necessity of disclosure or non-disclosure followed from both sides. What resulted was a lack of possible dialogue, where ultimately no information was passed, and both investigation and intelligence collection suffered. Commissioner Major explains:

> Each agency had a tendency to exaggerate the public interest that corresponded to its particular interests in any given situation. Hence, the RCMP generally claimed that every piece of information was essential to the investigation/prosecution, while CSIS often took the initial position that disclosing the requested information was too dangerous to its operations, without any real analysis having yet been conducted on either side. Not surprisingly, the agencies came to have little respect for each other's broad claims and assertions, creating a context where they could hardly have the type of dialogue that would have been necessary to balance fairly the interests in-

---

99 See *CSIS Act*, *supra* note 16, s 12(1).

100 See *Security Offences Act*, *supra* note 18, ss 2, 6.

101 SC 2001, c 41.

102 *Air India Report*, vol 3, *supra* note 77 at 12 [footnotes omitted]. See e.g. s 83.18(1) *Anti-terrorism Act*, *supra* note 101.

> volved. To this day, the sharing and use of CSIS information in the criminal process remains a complex problem.[103]

What is particularly startling is that both agencies took extreme, self-interested stances as their initial, default positions, before conducting any meaningful analysis. If such polarized positions were and continue to be the norm, it is not difficult to understand why the flow of information is intermittent.

The commission's findings suggest a second, related institutional impediment. When CSIS disclosure analysis is conducted in earnest, it always involves legal counsel and a strict interpretation of the *CSIS Act*. Ultimately, Commissioner Major characterizes the analysis as being too technical and legalistic too much of the time, to the detriment of the overall, collective interests that both parties were attempting to serve.[104]

Of note for our purposes is Commissioner Major's recognition that the ultimate decisions concerning information disclosure could not simply be based on narrow legal interpretations or on the fulfillment of some mandate. Rather, such decisions must look to "broad public interest considerations."[105] Of course, the point here is not to jettison or even minimize the importance of the legal channels through which such information must be passed, but rather to avoid a narrow focus on these channels, which has the effect of obscuring more fundamental, shared goals.

3. The Need-to-Know Principle

The next set of information-disclosure impediments flow from a more general cultural impediment, namely, the widespread adoption of the "need to know" principle. Stated as a general proposition, the need-to-know principle holds that, for reasons of security, sensitive or confidential information should only be disclosed to parties who have a demonstrable, mandated work-related need for that information—in other words "*need* to know." Commissioner Major notes that this axiom was a prevailing principle for the RCMP security service (and subsequently CSIS), present both internally within their own institutions and externally in their relationships with other agencies.[106]

As a general matter, the need-to-know principle has the immediate effect of limiting the practice of information sharing.[107] In light of the mosa-

---

[103] *Air India Report*, vol 2 part 2, *supra* note 77 at 420.

[104] See *ibid* at 416–17.

[105] *Ibid* at 416.

[106] See *Air India Report*, vol 2 part 1, *supra* note 77 at 340–41.

[107] See *ibid*.

ic effect sketched above, this decreased quantity of information moving across and within agencies means that those responsible for collecting and interpreting the data will, out of necessity, produce intelligence of decreased quality, and, in some cases fail to appreciate or apprehend certain pieces of information as having any utility all.

Reliance on the need-to-know principle has led to two further structural impediments to information sharing, both flagged by Commissioner Major. The first is compartmentalization of duties and the creation of silos or stovepipes around certain kinds of information. The dangers associated with compartmentalization are observed by Commissioner Major in his discussion of a telex sent by Air India on 1 June 1985. This telex, sent to all Air India offices worldwide, indicated the likelihood of an attack and called for meticulous implementation of "counter-sabotage measures for flights at all airports."[108] Although the document came into the RCMP's possession, it was never forwarded to CSIS. The officer in charge of the decision to disclose the information to CSIS testified that "he saw 'no need' to share the information with CSIS".[109] As a result, CSIS's assessment was, in Commissioner Major's words, "both incomplete and misleading," and the agency itself was therefore "completely unaware of this threat and the extreme security measures called for in response."[110] As such, Commissioner Major reports that the failures to handle the telex from 1 June 1985 appropriately "illustrate the dangers of compartmentalization of duties and the need for shared responsibility in aviation security."[111] We agree.

A second institutional impediment resulting from the use of the need-to-know principle is top-down centralization and delay in disclosure decisions. As Commissioner Major explains, the ultimate decisions regarding information disclosure were made by CSIS headquarters—those who always possess a "need to know".[112] In cases where information that was disclosed might be used in a criminal investigation, additional layers of analysis were included, resulting in delay:

> CSIS policy generally required that if there was a possibility that information to be shared would lead to, or become relevant to, a criminal investigation, the exchange of information had to be precleared with CSIS HQ, which was where the decisions about information sharing with the RCMP were made. Where authorization was sought by the RCMP to use CSIS information in the judicial

---

[108] *Ibid* at 505.

[109] *Ibid* at 436.

[110] *Ibid* at 507.

[111] *Ibid* at 21.

[112] See *Air India Report*, vol 2 part 2, *supra* note 77 at 414.

> process, CSIS HQ also insisted on being advised and on making the decision, in light of the risk that its information would be disclosed to the defence.[113]

The foregoing suggests that the internalization of the need-to-know principle, consistent with the polarized positions that the agencies took during disclosure requests, further delayed and frustrated the timely and comprehensive sharing of information.

Compounding the above impediments is Commissioner Major's observation that, as a general rule, the two agencies had little knowledge about what the other ultimately valued or prioritized. Without this knowledge, preliminary assessments of whether some information might be valuable were hampered. Commissioner Major referred to Professor Martin Rudner's testimony on this point:

> Each agency collects information in a silo without a sufficiently detailed awareness of the priorities of the other agencies. No one agency has the capacity to "connect the dots" to see the complete picture created by the intelligence collected by the various agencies and to link together all the activities required for an all-of-government approach to intervening in the terrorism cycle.[114]

Here, we can see the mosaic effect operating on an institutional level. Agencies lacking knowledge of one another's mandates and operations are unable to meaningfully appreciate whether some information may be valuable to another institution. As such, the pieces remain separate, and no one group or groups can meaningfully "connect the dots", appreciably increasing the risk that some credible threat may materialize.

4. Lessons from Air India

In our view, several conclusions can be drawn from the cultural and institutional impediments identified by Commissioner Major.

First, it seems clear that widespread internalization of the need-to-know principle should be avoided, especially in instances where all parties operate under similar degrees of confidentiality. There is some support for this proposition in the American context. Following 9/11, there have been calls to replace the need-to-know paradigm with a "need-to-share" paradigm. For instance, the National Commission on Terrorist Attacks upon the United States argues that the culture of agencies feeling that they own the information gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to share the

---

[113] *Ibid.*

[114] *Air India Report*, vol 2 part 1, *supra* note 77 at 428–29 [footnotes omitted].

information—to repay the taxpayers' investment by making that information available.[115] While it may seem somewhat odd to describe information sharing as a "taxpayer investment", we can at least appreciate the suggestion that there is some duty to disclose owed. In particular, government agencies owe an obligation to share information when it is necessary to discharge their duty to the general safety of the public.

A second lesson from our survey of these non-legal impediments is that agencies ought to avoid the institutional myopia that hinders and frustrates the free flow of information. Taken together, these institutional impediments point to the need for agencies to appreciate their position in their larger context as against other agencies. This may require a meaningful appreciation of the mandates, priorities, and to some extent, the operations of other institutions. Agencies and the actors that comprise them are, of course, expected to operate within the four corners of their mandates. To be sure, these mandates must be well understood and followed. In our respectful view, however, an appreciation of one's mandate is not enough. While fulfilling their mandates, government actors must also see their institutional roles for what they are: part of a larger, integrated system aimed at a set of shared goals—the most fundamental of which is the protection of Canadians. When viewed from this larger, cooperative perspective, and with an appreciation of the seriousness of potential consequences, the mere discharge of an agency's black-letter mandate seems inadequate, if not irresponsible. As Commissioner Major concludes:

> The overriding theme is the need to establish clear responsibility and accountability for decisions in national security matters. What must be avoided is a diffusion of responsibilities, where each agency and each official acts properly but where they fail collectively to achieve the ultimate goal: protecting the security of Canadians to the greatest extent possible.[116]

With this, then, we are back where we began: recognition of the government's fundamental responsibility to protect its citizens. We must not let narrow institutional interests, or the legalistic discharge of individual mandates, frustrate the ultimate goal of our shared enterprise.

III. Information Sharing: A Moral Imperative?

In this final section, we offer an additional argument in favour of sharing security information, grounded in both the nature of intelligence itself, and the consequences that follow from the failure to share it. This argu-

---

[115] See *9/11 Commission Report*, *supra* note 95 at 416–18.

[116] *Air India Report*, vol 3, *supra* note 77 at 15–16.

ment is intended to buttress the existing legal reasons to promote information exchange, and hopefully, to help mitigate the impact of the institutional and cultural impediments that frustrate such exchanges.

A. The Mosaic Effect and Preventing Harm

We begin with the nature of intelligence itself. Recall the basic premise of the mosaic effect: information is only valuable in context. That is, the meaning, and ultimately, the utility of any one piece of information as intelligence emerges only when placed alongside other ostensibly unrelated pieces of information. The Air India inquiry includes many examples of this phenomenon, including the "Duncan Blast" heard by two CSIS officers following a suspected Sikh extremist, whom they believed was involved in an assassination plot.[117] As noted by one of the agents himself, if he had been in possession of the telex from 1 June 1985 and known that a bombing was perhaps being planned, he may have interpreted the loud blast not as a rifle report confirming the assassination theory, but as a bomb blast consistent with the content of the telex.[118] An appreciation of this possibility may have materially altered the course of their investigation.

Grasping the mosaic effect allows for a recognition of the value of information sharing generally. If the utility of information as intelligence is directly connected to the context in which it is appreciated, then the comprehensive and timely exchange of information increases that utility and helps structure investigative efforts and other threat responses. Doing so helps prevent the kind of criminal acts or terrorist-motivated activities with which we are all too familiar in today's world.

B. The Moral Imperative

The timely and comprehensive sharing of information may materially reduce the risk of significant harm to the Canadian public. In our view, government's opportunity and resources to prevent this harm grounds a moral obligation to take active steps to do so.

This basic moral intuition—to prevent harm where possible—appears to influence much of the law of negligence. Elsewhere, one of the present authors has argued that in light of recent case law, an action in negligence may lie against government for a failure to warn citizens about

---

[117] The "Duncan Blast" refers to the explosion heard by two CSIS officers near Duncan, British Columbia in June of 1985. For a discussion of the "Duncan Blast", see *Air India Report*, vol 2 part 1, *supra* note 77 at 39ff.

[118] See *ibid* at 52.

credible security threats.[119] For instance, in *Fullowka v. Royal Oak Ventures Inc.*[120] (*Fullowka*), the Court of Appeal for the Northwest Territories contemplated the following hypothetical situation in which such a duty might arise:

> Another type of threat is a specific warning about an immediate and localized danger. An example would be an anonymous warning that a bomb had been placed in a building. The issue is whether those in charge of the building would have any duty in tort to respond, for example by evacuating the building for a short time. It is likely that a combination of knowledge of the threat, proximity to the potential victims, and responsibility for safety would give rise to a duty.[121]

Interestingly, the features capable of raising a novel duty of care identified by the Court of Appeal in *Fullowka* could conceivably be applied to a Canadian agency withholding information from another agency, such that the latter is unable to meaningfully appreciate and respond to a credible threat.

Even if the common law does not expand the tort of negligence to include such failures, however, the underlying moral consideration remains. That is, that positive steps which may appreciably prevent harm should be taken where possible. Indeed, one of the present authors has argued for this moral obligation in the context of cyber-security threats:

> Action is imperative. While strong evidence suggests the existence of a legal duty to act, a moral imperative lies with the government to take the necessary steps to protect its citizens from the threats of the digital age and the potentially tragic consequences of a sinister cyber attack. Political accountability to the public demands nothing less.[122]

In our view, that same underlying moral intuition holds with equal—if not greater—strength in the context of sharing information relevant to the security of Canadians for two reasons. First, as demonstrated above, there are no legal prohibitions or justifications barring such action. In fact, Canada's constitutional and legislative structure support and encourage government to act co-operatively to further security and achieve what Commissioner Major called "the ultimate goal".[123] Second, our discussion has also identified that many of the problems within the current information-sharing structure stem largely from human reaction. There exists a great deal of flexibility in how these elements can be changed.

---

[119] See Shore, *supra* note 1 at 238, 241.

[120] 2008 NWTCA 4, [2008] 7 WWR 411.

[121] *Ibid* at para 85.

[122] Shore, *supra* note 1 at 248.

[123] *Air India Report*, vol 3, *supra* note 77 at 15.

Taking steps to remove these impediments does not require legislative or constitutional amendments. Rather, through the kinds of concerted, co-operative efforts outlined above, meaningful change can be made and, as a result, the risk of harm can be reduced.

Therefore, there exists within the constitutional and legislative framework a moral imperative for governments to share security information. Government is entrusted with, indeed legitimized by, its obligation to the security of its citizens. Meaningful and satisfactory discharge of that obligation requires that all agencies, where possible, share information in a comprehensive and timely manner.

Conclusions and Recommendations

Our constitutional and legislative analysis leads to the following conclusions. First, as a constitutional matter, both the federal and provincial governments have legitimate constitutional interests in public safety and security, and, in our view, are equally required to discharge government's responsibility for citizen safety. Furthermore, the doctrine of co-operative federalism recognizes that constitutional mandates may overlap and encourages co-operation and collaboration between levels of government. In matters of security, this doctrine supports the meaningful and timely exchange of critical security information. Both federal and provincial agencies would benefit from an increased flow of information in areas of mutual interest and responsibility, and ultimately, so would Canadian citizens.

Second, our review of relevant legislation discloses no significant impediments to the practice of information sharing between federal and provincial agencies. As we have shown, arguments citing privacy concerns or public disclosure fail to provide a legal justification for non-disclosure. In fact, in most cases, the instruments cited include express exceptions to non-disclosure, and in some instances, contemplate the creation of collaborative interjurisdictional arrangements which actively encourage such disclosure. Such arrangements do exist and should act as models for other institutional relationships dealing with national security and public safety.

Third, institutional and cultural impediments are largely to blame for the recognized weaknesses in information sharing. National commissions of inquiry, both in Canada and in the United States, stress the impact of non-legal barriers and impart lessons regarding how best to reduce them. Because of the multi-jurisdictional nature of growing security threats, the process of addressing and eliminating these barriers should be a priority, focusing on collaborative and deliberative efforts, involving a variety of parties, perhaps through some sort of forum between federal and provincial agencies. A full and frank discussion among political and senior officials of federal and provincial governments may go some distance toward

reducing institutional barriers and allowing more comprehensive information flow to reduce the risks or "blind spots", which currently exist as a result of a less than full flow of critical information relevant to national security. Such an ongoing discussion would openly address larger institutional issues, as well as more discrete logistical concerns, such as security clearance policies and practices, and protecting shared foreign intelligence.

Canada's constitutional framework should not be used as an excuse to justify the current, less than optimal flow of interjurisdictional information sharing. In fact, as outlined above, our constitution provides a platform to motivate the federal and provincial governments to share information in a meaningful and timely manner to protect citizens as best as possible.

Finally, we have argued that there exists a principled reason to encourage information sharing based on the prevention of harm and the government's accountability to the public. Even in the absence of constitutional and legislative requirements, the severity of the consequences attending a failure to share critical information place an obligation on government to do so.