Of Unreasonable Searches and Seizures: A Blueprint for a Constitutional Challenge to the Security of Canada Information Sharing Act

by

Reem Zaia

A thesis submitted in conformity with the requirements for the degree of Master of Laws (LL.M.)

Faculty of Law
University of Toronto

© Copyright by Reem Zaia 2017
Abstract

This thesis scrutinizes the Security of Canada Information Sharing Act ["SoCIS"] through the lens of section 8 of the Charter of Rights and Freedoms. Drawing an epistemological link between search and seizure principles and the domestic exchange of information, I argue that the SoCIS falls short of the safeguards demanded by section 8. By permitting the unremitting disclosure of information, the regime casts too wide a net, and risks the exchange of information about innocent Canadians – not unlike the cases of Maher Arar, Ahmad Elmaati, Muayyed Nureddin, and Abdullaah Almalki. When measured against jurisprudential standards and lessons from commissions of inquiry involving porous information-sharing dynamics, the absence of oversight or accountability in the SoCIS proves disproportionate to its overarching objective. Thus, it cannot be saved by section 1 of the Charter, and should be declared of no force or effect.
ACKNOWLEDGMENTS

This thesis is dedicated to my mother whose love has no bounds. I am indebted to her for her continued encouragement of my academic career. As a single mother, she took extraordinary leaps to secure my professional success. She instilled in me the value of perseverance, dedication and hard work. She is my beacon of light.

To my brother - whose brilliant philosophical ideas inspired me to think outside the box when scrutinizing surveillance at the metaphysical level. I admire you.

To my grandmother – whose former career as a teacher in Iraq is an inspiration to the women in our family.

To my better half, Michael Purcell – thank you for unconditional love and patience with my academic career. I am grateful for your unparalleled support of my scholarship. Without you, this achievement would not have been possible.

To my mentor – Brian Manarin – thank you for your sage wisdom. You are my pillar of support. I admire your dedication to the practice of law and the academy. In the words of the learned, when faced with writer’s block, “just write.”

To my LL.M. colleagues – particularly Nicholas, Jean-Paul, and Stephane - thank you for enriching my LL.M. experience. I will miss our theoretical musings at Falconer Hall.

Finally, to my thesis supervisor – Kent Roach. Your contributions to criminal and national security law are unmatched. Thank you for your patience with me in the writing process. Your humility and dedication to your graduate students is a paradigmatic example for the academy.
# TABLE OF CONTENTS

**CHAPTER I: THE SoCIS, REASONABLE EXPECTATIONS, AND SECTION 8 OF THE CHARTER** .............................................................................................................................. 4

(i) *The Information-Sharing Provisions in the SoCIS* ................................................. 4

(a) *The Import of the Words “Subject to any provision of any other Act of Parliament”* ................................................................................................................................. 5

(b) *What is the threshold for disclosure?* ................................................................. 9

(c) *What are these activities?* .................................................................................. 12

(ii) *Reasonable Expectations and Informational Privacy: The “Epistemological” Nexus Between the SoCIS and Section 8* ....................................................... 14

(a) *The Case for a Reasonable Expectation of Privacy* ........................................ 15

(b) *Applying the Spencer Factors* ...................................................................... 17

(c) *The Case for a Search or Seizure* ................................................................. 20

**CHAPTER II: SAFEGUARDS AND ACCOUNTABILITY MEASURES IN INFORMATION-SHARING REGIMES** ........................................................................... 23

(i) *Safeguards, Accountability and the Reasonableness of Legislation through a Jurisprudential Lens* ..................................................................................... 23

(a) *Air India Flight 182: Major Report* ............................................................... 30

(b) *Maher Arar: The O’Connor Report* ............................................................. 32

(ii) *Accountability, Safeguards and Oversight: Reasons that the SoCIS is an Unreasonable Law* ......................................................................................... 36

(a) *The SoCIS Cannot Borrow its Lawfulness from Other Acts* ......................... 36

(b) *The Manner Information is Shared and Stored* ............................................ 37

(c) *The Absence of Training, Designated Staff, and Related Unknown Regulations* .............................................................................................................. 42
CHAPTER III: THE SoCIS CANNOT BE JUSTIFIED BY SECTION 1 OF THE CHARTER........................................................................................................45

(i) Does the SoCIS have a pressing and substantial objective? ........................................45

(ii) Are the measures in the SoCIS reasonable and demonstrably justified in a free and democratic society? ........................................................................................................47

(ii) Rational Connection........................................................................................................48

(iii) Minimal Impairment........................................................................................................49

(iv) Overall Proportionality: Salutary versus Deleterious Effects .................................53

CONCLUSION .........................................................................................................................57
“While a preliminary view of the data suggests a limited use of [the SoCIS] … the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them.”

- Privacy Commissioner of Canada

Opining on sovereignty, Carl Schmitt once posited that emergency laws embody a “state of exception” — a phenomenon that involves the suspension of a constitutional order and the rule of law to preserve public security. One scholar describes it as a suspension of the juridical order in which the state arbitrarily decides that it is in a permanent state of emergency. Others suggest that the state of exception has become the rule, rather than the exception.

The Security of Canada Information Sharing Act [SoCIS] squarely captures the phenomenon espoused by Schmitt. It is a fitting example of how domestic information-sharing legislation perpetuates the misplaced conception that we co-exist in a persistent, unpredictable state of emergency. When measured against the constitutional order, the SoCIS does not contain the requisite safeguards required by section 8 of the Charter of Rights and Freedoms. Thus, the crux of this thesis is that the SoCIS does not strike a reasonable balance between the right to informational privacy and Canada’s interest in curtailing terrorism. On balance, it cannot be justified in law.

---

2 Carl Schmitt, Dictatorship: From the Beginning of the Modern Concept of Sovereignty to the Proletarian Class-Struggle, 7th ed (Berlin: Duncker & Humblot, 2006).
4 Ibid at pp 2 and 4.
5 Ibid at p 6.
6 SC 2015, c 20 [SoCIS].
7 Canadian Charter of Rights and Freedoms, s 8, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11 which reads: “Everyone has the right to be secure against unreasonable search or seizure” [Charter].
By way of brief introduction, the SoCIS permits over 143 “Government of Canada”⁸ institutions to disclose personal information about Canadians on their own initiative, or upon request, to 17 recipient institutions, including the RCMP and the Canadian Security Intelligence Service [“CSIS”].⁹ It does not require disclosing agencies to obtain prior judicial authorization. The threshold for sharing information is extremely low. Information need only be “relevant” to the jurisdiction of the receiving institution, and capture “activities that undermine the security of Canada”, without further direction on what relevance entails.¹⁰ The term “activities” is not exhaustively defined. It is exceptionally broad. The structural makeup of the SoCIS is at odds with commissions of inquiry on information that stress the importance of oversight, accountability and safeguards in information-sharing. In practical terms, the regime permits the warrantless exchange of personal information, generating a risk that faulty, misconstrued and/or unreliable data will crystallize into intelligence. Its breadth will inevitably capture innocuous information about innocent people. I argue that Canadians have a privacy interest in the information captured by the SoCIS, and that intra-governmental information exchanges constitute searches and seizures, which trigger the protections afforded by section 8 of the Charter.¹¹ These protections suggest that the current regime is unconstitutional.

This thesis provides a substantive blueprint for a constitutional challenge to the SoCIS using section 8 of the Charter and jurisprudence on the need for accountability and oversight measures in search and seizure legislation. Part I situates the SoCIS within the informational privacy context to demonstrate how it engages the reasonable expectation of privacy doctrine, and by implication, section 8 of the Charter. Part I also deconstructs the legislative underpinnings of the SoCIS, pointing to the improvidence of its legislative language, its practical effects on the Privacy Act¹² [“PA”], and section 8 of the Charter.

---

⁸ SoCIS, supra note 6, s 2: A Government of Canada institution in the SoCIS means: “(a) a government institution, as defined in section 3 of the Privacy Act – other than one that is listed in Schedule 1; or (b) an institution that is listed in Schedule 2.” The Privacy Act, RSC, 1985, c P-21 defines government institution as “(a) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule” [PA]. The schedule in the PA then goes on to list hundreds of agencies, many of which do not have national security mandates.
⁹ SoCIS, supra note 6 at s 5.
¹⁰ Ibid at s 2.
¹¹ By search or seizure, I adopt the following from R v Cole, 2012 SCC 53; [2012] 3 SCR 54 at para 34: “An inspection is a search, and a taking is a seizure, where a person has a reasonable privacy interest in the object or subject matter of the state action and the information to which it gives access…” [Cole].
¹² PA, supra note 8.
Part II highlights jurisprudence explaining the significance of safeguards and accountability measures that have preserved the constitutionality of search and seizure laws. It also provides a synopsis of commissions of inquiry in relation to events surrounding the Air India bombing in 1985 and the actions of Canadian officials in relation to Maher Arar. In doing so, it underscores the dangers of unfettered information-sharing through a legal and practical lens.

Finally, Part III explains why the SoCIS cannot be justified under section 1 of the Charter. While the SoCIS presents a pressing and substantial objective, the measures used to obtain the objective are disproportionate to the limitations on the right to be free from unreasonable search and seizure. By undertaking this exercise, I hope to dispel the misguided notion that the security of a nation and the preservation of privacy are mutually exclusive concepts.
CHAPTER I

THE SoCIS, REASONABLE EXPECTATIONS, AND SECTION 8 OF THE CHARTER

This part explains why Canadians have a reasonable expectation of privacy in the information captured by the SoCIS, and why it triggers section 8 of the Charter. The argument is divided into two sections. Section one canvasses the information-sharing provisions of the SoCIS, detailing the scope and effect of the most contentious provisions. Section two establishes a nexus between informational privacy and the SoCIS, explaining why the information captured by the SoCIS attracts a reasonable expectation of privacy [“REP”]. This entire Part constitutes the foundation for the constitutional challenge proposed in Part III of the paper by outlining the REP argument.

Throughout this part, and the remainder of this thesis, I make intermittent references to a hypothetical fact scenario to assist the reader in understanding the reach of the SoCIS. The hypothetical is as follows:

A Canadian citizen, X, has been a member of a prominent Islamic mosque in Toronto for decades. He recently made a sizeable donation to the mosque. He reported the donation to the Canada Revenue Agency (CRA) on his annual tax return as an eligible credit. The CRA identified the donation as an “activity” that “undermines the security of Canada.” The CRA then disclosed information about X to CSIS. As a result, CSIS and the RCMP are now surveilling X.

(i) The Information-Sharing Provisions in the SoCIS

Arguably, the most contentious provisions of the ten in the SoCIS are sections 5 and 6 which authorize the disclosure of information between federal government institutions. They provide a wide discretionary authority for institutions to exchange what they deem relevant in the national security context. Sections 5 and 6 read:

5. (1) Subject to any provision of any other Act of Parliament, or of any regulation made under such an Act, that prohibits or restricts the disclosure of information, a Government of Canada institution may on its own initiative or request, disclose information to the head of a recipient Government of Canada institution, whose title is listed in Schedule 3, or their delegate, if the information is relevant to the recipient institution’s jurisdiction or responsibilities under an Act of Parliament or another lawful

---

13 Schedule 3 of the PA, supra note 8 encompasses the 143 institutions I describe above.
authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.

5. (2) Information received under subsection (1) may be further disclosed under that subsection.

6. For greater certainty, the use and further disclosure, other than under this Act, of information that is disclosed under subsection 5(1) are neither authorized nor prohibited by this Act, but must be done in accordance with the law, including any legal requirements, restrictions and prohibitions.14

Section 5 is essentially divided into three parts. The first engages the import of other legislation on the SoCIS; the second details which government entities are authorized to disclose and receive information and under what circumstances; and the third touches on what type of information is authorized for exchange. Section 6 enhances the scope of section 5 by allowing the use and further disclosure of the information already shared. In the following sections, I analyze three central features engaged by the main disclosure provision in section 5.

(a) The Import of the Words “Subject to any provision of any other Act of Parliament”

The opening language of section 5 provides that information-sharing is “subject to”, which engages questions about whether the SoCIS ought to be employed harmoniously with other acts. This is particularly salient in respect of the PA, which merits further analysis.

The PA protects personal information in the possession of the government by prohibiting its disclosure absent the consent of the individual to whom it relates, and subject to several exceptions.15 Information includes but is not limited to that which identifies an individual in relation to their race, national or ethnic origin, colour, religion, age, marital status, fingerprints, blood type, address, education, criminal, medical or employment history.16 Meanwhile, these

---

14 SoCIS, supra note 6 at ss 5 and 6.
15 Section 7 of the PA protects “personal information under the control of a government institution” which institutions “shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2). Section 8(2) then lists a series of exceptions under which information can be disclosed without consent. For our purposes, section 8(2)(e) and 8(2)(m) are salient. The former permits disclosures for investigative purposes and the latter for public interest reasons.
16 PA, supra note 8 at s 3.
exceptions are also “subject to any other Act of Parliament”, suggesting that both the SoCIS and the PA defer to one another.

This interplay poses an obvious conflict for public servants required to determine which act governs before disclosing information. It is unclear whether Parliament intended the SoCIS to supersede the information-sharing protections in the PA. In 2016, the federal government addressed this issue in its Green Paper on national security, writing that the SoCIS “…is an Act of Parliament that authorizes disclosure” and satisfies “the lawful authority exception under the Privacy Act.”

The lawful authority provision in the PA allows investigative bodies to request the disclosure of information for the “purpose of enforcing any law of Canada or a province carrying out a lawful investigation”, which would encompass essentially anything within the four corners of law enforcement. The Green Paper then goes on to suggest that the SoCIS “cannot be used to bypass other laws prohibiting or limiting disclosure” and that “[i]f another law restricts use or sharing of information, these restrictions continue to apply and must be respected.”

On this basis alone, the SoCIS is bound by the limitations on disclosure in the PA, subject to the exceptions listed. This makes little sense because it would render the SoCIS effectively toothless. Professors Kent Roach and Craig Forcese echo this concern in their response to the government on the Green Paper, writing that

They [the government] say that because the SoCIS “authorizes disclosure”, it satisfies the “lawful authority” exception to the Privacy Act, effectively trumping it. This statement is hard to understand, given that the SoCIS Act itself says it is subject to other Acts that “prohibit or restrict” the disclosure of information (And that would include the Privacy Act). At the same time, the Paper acknowledges (correctly in our view) that the SoCIS Act “cannot be used to bypass other laws prohibiting or limiting disclosure.”

18 PA, supra note 8 at s 8(2)(e).
19 Green Paper Backgrounder, supra note 17 at p 30 [emphasis added].
In keeping with the rules of statutory interpretation, introductory statutory language such as “subject to X” denotes that a separate piece of legislation should be interpreted as paramount.21 If that is the case, then the SoCIS cannot be paramount to the PA, contrary to what the Government suggests in the Green Paper. If the PA is paramount, this interpretation would accord with the fact that the PA is a quasi-constitutional document,22 warranting special treatment. Where quasi-constitutional legislation conflicts with another act, it is paramount.23 It seems that if this were the case, the government could justify disclosures under the SoCIS under the public interest exception, as provided in section 8(2)(m) of the PA. Section 8(2)(m) permits the disclosure of personal information without the consent of the subject:

(m) for any purpose 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 disclosure; or (ii) disclosure would clearly benefit the individual to whom the information relates.

It is difficult to argue that “activities that undermine the security of Canada” does not constitute information that is relevant to the public interest. Problematically, the use of the public interest exception in the PA risks capturing bulk data. Roach and Forcense echo these concerns, noting that “the inevitable fallback for the government will be generous sharing permissions in the PA.”25

If the exchange of information is subject to the PA, then it is not clear why the SoCIS was a necessary legislative enactment in the first place, since personal information could have been disclosed under the lawful authority or public interest exceptions. While the Green Paper vaguely sheds light on the application of the PA, it fails to explain how the SoCIS was intended to fill existing legislative gaps. In 2016, the Privacy Commissioner of Canada pointed to this issue in a press conference about the Act and more broadly, Bill C-51, stating that there was no evidentiary basis to justify why a broader mandate for information-sharing powers was required. Meanwhile,

21 Ruth Sullivan, Statutory Interpretation, 2nd ed (Toronto: Irwin Law, 2007) at pp 304 and 305.
24 PA, supra note 8 at s 8(2)(m).
upon introducing Bill C-51, then Public Safety Minister, Stephen Blaney, was adamant that the Act was intended to eradicate barriers and information silos in existing information-sharing structures, without explaining why “previous law[s] created impediments to information sharing operationally required for national security purposes.” The divergence between the comments of the Minister and the Privacy Commissioner suggests that we ought to be circumspect about legislation which lacks evidence-based foundations. In this regard, I question whether the SoCIS purposely circumvents the safeguards inherent in prior judicial authorization schemes in favour of a quicker, more accessible way of exchanging information.

Some have argued that the permissions in the PA are so ambiguous that courts might disagree that the Act meets the “authorized by law” requirement under section 8 of the Charter. This argument is partially attributable to the SoCIS’s opaque language, which attracts inconsistent interpretation, particularly among public servants responsible for sharing information. Unfortunately, the PA does little to mitigate this problem, providing no assistance in terms of “what federal departments do with their information, with whom they share it, and why.” That only some disclosures will be subject to post facto review further frustrates the purpose of section 8 of the Charter, since its purpose is to prevent unjustified searches and seizures before they happen. Moreover, the absence of oversight measures on the disclosure process hinders our ability to ascertain whether public servants will receive adequate legal training on the exceptions in the PA and relatedly, strictures on disclosure. Absent safeguards to this effect, the risk that personal information might be illegally disclosed, or mishandled, is not unlikely.

---

26 House of Commons Debates, 41st Parl, 2nd Sess, No 174 (18 February 2015) at 1535 (Hon. Steven Blaney) [Blaney Second Reading].
28 False Security, supra note 25 at p 152. Searches and seizures must be authorized by law in order to be reasonable. The state must be able to justify the search or seizure by pointing to a rule; the search must be carried out in accordance with the procedural and substantive requirements the law provides; and the scope of the search must be limited to the area and items for which the law grants the authority to search or seize (R v Caslake, [1998] 1 SCR 51 at para 12 [Caslake]).
29 The Privacy Commissioner also argues that the breadth of the Act leaves much discretion to institutions in interpreting what constitutes “activities that undermine the security of Canada”, which may result in an inconsistent approach in applying the legislation (Annual Report Privacy Commissioner, supra note 1 at p 17).
30 Annual Report Privacy Commissioner, supra note 1 at pp 2-3.
31 See Hunter v Southam, [1984] 2 SCR 145 at p 160 in which Dickson J. suggests that post facto analyses are at odds with section 8 because the “purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place” [Hunter v Southam].
(b) What is the threshold for disclosure?

Presumably, information is disclosable so long as it fits within the relevance criteria under section 5. Control over the lawful disclosure of information is downloaded to disclosing institutions, who carry the onus of ensuring that the information is relevant to the recipient institution’s jurisdiction or responsibilities. Relevance, however, is not defined in the SoCIS.

Black’s Law Dictionary defines “relevant” as something that is “logically connected and tending to prove or disprove a matter in issue having appreciable probative value – that is, rationally tending to persuade people of the probability or possibility of some alleged fact.”32 Given the breadth of the mandates, and responsibilities of SoCIS-authorized institutions, what is deemed relevant by one institution may not be the case for another. For example, if X’s tax donation came to the attention of Heritage Canada because of a joint project with the Muslim community, it may not have attracted similar suspicions as it would in the context of CRA. Considered in this way, interpretation of what is relevant may depend on institutional mandates and the interpretation of information. Nevertheless, it remains unclear.

Roach explains that the relevance threshold is “deliberately provocative”, evincing the “broadest definition of national security” ever seen in Canada’s national security history.33 When testifying on the bill at the committee stage, he questioned why the government did not incorporate the strictly necessary threshold under section 234 of the CSIS Act instead, which provides a more focused, defined mandate for the collection of information.35 To date, the government has not

32 Black’s Law Dictionary, 10th ed, Brian A Garner Ed in Chief at p 1481 sub nom “relevance.”
34 Section 2 defines “threats to the security of Canada” as: (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; (c) activities within or relating to Canada directed toward or in support of 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 cover unlawful acts, or directed toward or intended ultimately to read 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).”
35 House of Commons, Standing Committee on Public Safety and National Security, Anti-terrorism Act, 2015
implemented this recommendation, leaving the relevance threshold as it currently reads in the SoCIS. However, after a series of consultations commissioned by the Standing Committee on Public Safety and National Security in 2016, the committee tabled several recommendations, in which they call for a dual threshold that requires a relevance threshold for disclosing institutions and necessity and proportionality for recipient institutions. These recommendations were merely tabled in the House of Commons, meaning they have no legal force or effect.

In addition to the meaning “relevance” is concern about whether innocuous data will assist in ascertaining the temporal proximity of threats. According to the Green Paper, information can only be exchanged if it is “actually - and not potentially or possibly - relevant to the recipient’s lawful responsibilities for activity that undermines the security of Canada.” Notwithstanding this assurance, it is not clear how federal institutions can know, without any certainty from intelligence bodies or law enforcement officials, whether something is “actually relevant” unless the information is exchanged and assessed. The receiving institution is better equipped to determine relevance. With respect to X, the CRA has little to no experience in determining what constitutes a threat to national security. Disclosing institutions without experience in national security matters will likely call for direction from recipient agencies, at the risk that deference will be afforded to the opinion of an agency with a national security mandate, like the RCMP or CSIS. In that vein, the imminence of threats may be prematurely gauged by the threshold for disclosure.

Practically, the relevance threshold opens the floodgates to the disclosure of information, both domestically, and to foreign entities. The effect is that information which ought not to be disclosed in the first place, might be compounded by a further wrongful disclosure under section 6. Consider this. CRA discloses X’s information to the FBI for concern that he may abscond. Intelligence agencies begin an investigation. White House officials are briefed. The President discloses this information to a foreign government, which is subsumed within a bundle of other

(March 2015) at 1835 (Kent Roach) (Chair: Daryl Kramp). See also Righting Security, supra note 20 at p 23; Annual Report Privacy Commissioner, supra note 1 at p 16 where the Commissioner writes that the relevance threshold “could expose the personal information of law-abiding Canadians.”


37 Green Paper Backgrounder, supra note 17 at p 28 see footnote 13.
intelligence. This is no different than President Donald Trump’s recent mercurial treatment of classified intelligence, in which he shared classified information with a foreign government. If the intelligence provides inaccurate leads or information, it risks jeopardizing the liberty of the subject in question.

Better yet, consider the implications of a surveillance program, resulting from the initial disclosure about X, initiated by CSIS or the RCMP. CSIS shares intelligence about X with American counterparts. Upon traveling through the United States, X is detained, interrogated, and transferred to his home country where X is tortured. These were essentially the facts involving the illegal detention and torture of Maher Arar, which resulted in a commission of inquiry that made a series of recommendations on the importance of using caveats when disclosing intelligence both domestically and with foreign partners. In his report, Commissioner O’Connor explained that the RCMP did not obtain CSIS’ consent in transferring intelligence about Mr. Arar to American agencies due to a “free flow of information agreement,” which eventually led to the rendition of Mr. Arar to Syria. While Mr. Arar’s case did not commence with a tax return, X’s information is not foreclosed from being shared with foreign partners for similar reasons. Therefore, in an age when information-sharing knows no borders, we must be circumspect about how section 6 of the SoCIS is employed. Considered in toto, the relevance threshold is problematic both given its scope and its failure to require the use of caveats in the disclosure process.

---

39 Caveats restrict the way in which information is used. For example, the RCMP uses caveats to control how and for what purposes classified and designated information is used (Internal Inquiry Into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Almaati and Muayyed Nureddin (Ottawa: Public Works and Government Services Canada, 2008) at p 82 [Iacobucci Report]).
40 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar: Factual Background, vol 1 (Ottawa: Public Works and Government Services, 2006) at p 94 [Arar Vol 1].
(c) What are these activities?

The definition of activities that undermine the security of Canada are covered by a non-exhaustive list under section 2 of the SoCIS and include, but are not limited to terrorism. However, anything that “undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada” is also included. In this respect, the minutiae of other activities not listed in the Act is not publicly available.42

However, the Office of the Privacy Commissioner provides some insight into which entities are receiving and disclosing information from which we can draw inferences about the nature of the information. In a survey administered to 128 Government of Canada institutions, the Commissioner’s office studied the impact of the SoCIS within the first six months of its enactment.43 Entities responding to the survey reported 58 disclosures collectively by the Canada Border Services Agency, Immigration, Refugees and Citizenship Canada, and Global Affairs, as well as 52 disclosures collectively received by the Canada Border Services Agency, CSIS, Immigration, Refugees and Citizenship Canada, and the RCMP.44 To that extent, we can infer that biographical information relevant to the immigration context, or information captured by one’s biometric passport is, at the very least, engaged by this legislation.

Beyond this information, the public is not fully apprised as to the content of such disclosures, which leaves meaningful analysis to speculation. In the case of our hypothetical, information about the tax donation is not the only data legally authorized for sharing under the SoCIS. Everything including but not limited to X’s name, family affiliations, country of origin, financial information, ideological beliefs, and employment, at the very least, is available to CSIS. Worse, it can be disclosed without requiring verification protocols to ensure that the information is accurate. Perhaps X is a Canadian of Scottish descent, who has converted to Islam. Perhaps X is an Arab-Canadian, with deep familial and financial connections to a community in Toronto,

42 In his 2015 Report, the Privacy Commissioner of Canada confirms that, when asking federal institutions what types of specific or categories of individuals were captured by the SoCIS, and whether they were suspected of undermining the security of Canada at the time of the disclosure, the entities responding to the survey did not provide any meaningful clarification (Annual Report Privacy Commissioner, supra note 1 at p 19).
44 Annual Report Privacy Commissioner, supra note 1 at p 2.
motivated to assist a mosque in need. Perhaps the money was donated to assist Syrian refugees the mosque pledged to sponsor. Without cross-referencing these details, CRA cannot truly know whether their suspicions indeed constitute a threat.

While I do not wish to belabor this point, the underlying premise is that information will always be subject to various interpretations. Although the initial disclosure of information might seem benign, the “secondary use” of that information is difficult to predict, making it “hard for people to assess the dangers of the data being in the government’s control.”45 Put simply, innocuous data enables intelligence and law enforcement officials to draw conjectures about subjects who are not bona fide targets. It is not unlikely that intelligence officers will use profiling tools to draw conclusions about what the data suggests.46

Beyond these problems, it might seem that because the definition of activities under section 2 of the SoCIS does not include protests, dissents, and artistic expression, that its scope is narrow. However, upon close examination, section 2 does not foreclose information-sharing about these activities when deemed violent. For example, the biographical information of an individual involved in an anti-Trump protest in front of the American Embassy might fall within its purview. Similarly, personal information about persons developing a human shield at the border between Canada and the United States to protest the construction of a new pipeline, may be classified as an activity that undermines the security of Canada. That the spectre of “violence” is not prescribed by law means law enforcement is left with discretion to deem protests violent at its pleasure. Consequently, the scope of section 2 is broader than meets the eye.

In this context, it is fair to say that the nature and extent of disclosure is simply unpredictable. The Act does not instruct government officials on the circumstances that might give rise to such

---

45 Daniel Solove refers to “secondary use” as the exploitment of data obtained for one purpose for an unrelated purpose without the subject’s consent” (Daniel Solove, Nothing to Hide: The False Tradeoff between Privacy and Security (New Haven: Yale University Press, 2011) at p 28 [Solove]).

46 For example, “In 2005, CSIS (2012a: 42-60) published its first study on “how Canadian Islamic extremists were radicalizing.” Subsequently, CSIS authored a number of reports focusing on Islamic radicalization and extremism […] As recently as October 2010, CSIS integrated an Islamic-component to their definition of radicalization […] Use of discourses of radicalization have emerged as the new discursive frame for articulating the threat to the Canadian public, yet the expression of the new menace of radicalization rests on non-articulation of the inconvenient and often unspoken truth facing security governance agencies: the threat of terrorism in Canada is very remote” (Jeffrey Monaghan, “Security Traps and Discourses of Radicalization: Examining Surveillance Practices Targeting Muslims in Canada” (2014) 12(3) Surveillance & Society 485 at p 487 [Monaghan]).
“activities” and when they should be of concern. It leaves the task in the hands of public servants, and to some extent, Ministerial regulations. Relatedly, there are inevitable privacy concerns with this structure that taint the constitutionality of the Act. Before I explain why this is the case, I must highlight why there is a privacy interest in the information I highlighted. To do so, I turn to section 8 of the Charter for direction.

(ii) Reasonable Expectations and Informational Privacy: The “Epistemological” Nexus Between the SoCIS and Section 8

Section 8 guarantees that “everyone has the right to be free from unreasonable search or seizure”, which protects the right to privacy from unjustified state intrusion. It is a right benefiting the public at large, which protects people, not places. Privacy interests can be personal, territorial and informational in nature. To benefit from the protections in section 8, an individual must prove that he or she has a reasonable expectation of privacy on a balance of probabilities, which determines whether there has been a search or seizure. Once a REP is established, the inquiry shifts to whether the search or seizure is authorized by law, the law is reasonable, and the manner in which the search or seizure was conducted is reasonable. For the purpose of this section, I am primarily concerned with whether there is a REP in information captured by the SoCIS, and whether sharing information amounts to search or seizure.

---

47 I endorse the work of Associate Professor at the University of Copenhagen, Klemens Kappel, who frames his philosophical questions about privacy as “epistemological” dimensions of informational privacy. By epistemological, Kappel refers to the knowledge gained by access to sensitive personal information and the disclosure or distribution of it by public and private institutions (Klemens Kappel, “Epistemological Dimensions of Informational Privacy” (2013) 10(2) Episteme 179 [Kappel]).
48 Charter, supra note 7 at s 8 [emphasis added].
49 Hunter v Southam, supra note 31 at p 160.
50 R v Edwards, [1996] 1 SCR 128 at para 59 (per LaForest, dissenting) [Edwards].
51 Katz v United States 389 US 347 (1967), as adopted in several Canadian Supreme Court cases including but not limited to Hunter v Southam, supra note 31 at p 159; Edwards, supra note 50 at para 29; R v Tessling, 2004 SCC 67, [2004] 3 SCR 432 at para 22 [Tessling].
52 Tessling, supra note 51 at para 20.
53 Hunter v Southam, supra note 31 at p 159.
(a) The Case for a Reasonable Expectation of Privacy

Determining whether a reasonable expectation of privacy exists is a normative inquiry, meaning that it accounts for extant social values at the time of the assessment. In *R v Spencer*, the Supreme Court of Canada provided that in determining whether a REP exists, we must consider the totality of the circumstances, which includes: (1) the subject matter of the alleged search; (2) the claimant’s interest in the subject matter; (3) the claimant’s subjective expectation of privacy; and (4) whether this subjective expectation of privacy was objectively reasonable. In this section, I explore whether Canadians have privacy interests in information shared through the *SoCIS*, and whether these exchanges constitute searches or seizures. The *Spencer* factors listed above are applied hereinafter.

While privacy is a protean concept, it is broadly defined as the “right of personhood, intimacy, secrecy, limited access to the self, and control over information.” By extension, informational privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Informational privacy protects the data, or the subject matter of a search. The subject matter of this information might tend to reveal patterns including but not limited to how one thinks, financial habits, race, gender, relationships, health issues, political leanings and viewpoints. These might encompass a biographical core of information which tends to reveal intimate details about the lifestyle and personal choices of the individual. In *R v Cole*, the Supreme Court of Canada cites personal situations, interests, likes, medical issues, propensities, what we read, watch, and

---

56 *Tessling*, supra note 51 at para 42; *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 at para 18 [*Spencer*].
57 The evolution of section 8 reflects the doctrine of the living tree, first espoused in *Edwards v Canada (Attorney General)*, [1930] AC 124 at para 54 (JCPC). On this concept, Lord Sankey L.C. writes, “The *British North America Act* planted in Canada a living tree capable of growth and expansion within its natural limits. The object of the Act was to grant a Constitution to Canada. Like all written constitutions it has been subject to development through usage and convention. [*Canadian Constitutional Studies, Sir Robert Borden* (1922) p. 55.]”
58 *Spencer*, supra note 56.
59 Ibid at para 18.
60 *Tessling*, supra note 51 at para 25.
63 *Cole*, supra note 11 at para 41.
65 *Cole*, supra note 11.
listen to as factors that go to the biographical core of information. The closer information “lies to the biographical core” of one’s personhood, the more the subject matter of the information “will favour a reasonable expectation of privacy.”

One scholar argues that “some features of our life and existence just deserve informational privacy protection per se, irrespective of individual or social consequences of protecting this information.” When measured against public safety concerns, this is a controversial position to maintain. Indeed, sensitive facts about our “religious denomination, health, sexual preferences and certain parts of our lifestyle”, among many other elements, are protected as a matter of social convention. While stand-alone facts about us may not depict our innermost secrets, construed together, they might explain a great deal about who we are, how we think, and why we behave as we do. This phenomenon is referred to as the “mosaic effect”, which is the idea that the release of benign or innocuous information, when pieced together, or connected by a knowledgeable reader, cumulatively discloses matters of true national security significance. Julie Cohen expounds upon this point, emphasizing that:

> The universe of all information about all record-generating behavio[u]rs generates a “picture” that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it.

Cohen’s observations are equally applicable to the unsupervised exchange of information under the SoCIS, particularly since it is not unlikely that it will be used to generate “profiles” of people. These profiles can be more intrusive than those gathered in the private context by the likes of corporations such as Google, Facebook and Twitter. After all, corporations are more concerned with accruing consumer profiles, than investigating crimes against national security.

---

66 Cole, supra note 11 at para 46.
67 Kappel, supra note 47 at p 183.
68 Ibid at p 183.
71 Bernard E. Harcourt describes this phenomenon in the United States as follows: “Google collects and mines our Gmials, attachments, contacts and calendars. Twitter watches our activity on all the websites that carry its little icon. Facebook’s smartphone app collects information from all our other phone apps… And, thanks to the Snowden revelations, we know that the federal government can easily obtain all of this information” (Bernard Harcourt, “Surveillance State? It’s so much worse” (2015) 62(14) The Chronicle of Higher Education B15 at p B15).
Going back to our hypothetical, X’s financial\(^{72}\) information is one aspect of his biographical core of information. As explained in the previous section, the fact that X has made a sizeable donation to a mosque might suggest that X is somehow both affiliated with the Muslim community and is presumably affluent. To the extent that the information tends to reveal socio-economic, cultural and religious details, it goes to the biographical core of X’s person, which bolsters the nature of the privacy interest.

\((b)\) Applying the Spencer Factors

The first Spencer factor, the subject matter of the alleged search or seizure, is X’s donation to the mosque, and more broadly, what can be inferred from his tax returns.

Secondly, X likely has an expectation that the information disclosed to the CRA will be kept confidential rather than exchanged for the purposes of an incriminating investigation. This is his “interest in the subject matter” under the second Spencer factor. As indicated earlier, unbeknownst to X, CSIS might draw several inferences about X stemming from the donation alone, which may or may not be true, and X might simply be a generous person.

Thirdly, X may also have a high subjective expectation of privacy, pursuant to the third factor in Spencer. This analysis is contingent on the totality of the circumstances surrounding X.

Fourthly, X’s expectation must be objectively reasonable. This factor is meted out because X’s expectation of privacy in his donation is objectively reasonable. X disclosed his donation for the limited purposes required by the federal Income Tax Act. However, when shared, it potentially generates a great deal of informational value. A range of other implications are also possible:

- The information may be algorithmically assessed\(^{73}\) to detect behavioural patterns, which could be used to justify the surveillance;

---

72 See Cole, supra note 11 at para 47 which also cites details of our medical and personal situations, our interests, likes, dislikes, propensities, what we read, watch, listen to, browse on the Internet, etc.

• X’s profile may be captured by surveillance practices targeting Muslims;\textsuperscript{74}

• X’s donation may be stored in the Operational Data Analysis Centre (“ODAC”), a data retention program used by CSIS to store “associated data” about non-targets;\textsuperscript{75}

• The donation may incite intelligence officials to begin gathering metadata\textsuperscript{76} about X. CSIS’ collection of metadata is known to target innocent persons.\textsuperscript{77} That Canada has an active metadata collection and retention program increases the chance that innocent people will be captured by the SoCIS. This reality strengthens the objective expectation of privacy;

• Pursuant to section 6 of the SoCIS as articulated in section A, X’s information is not precluded from being further disclosed after the initial disclosure under the SoCIS. This poses concerns about whether government departments will attach caveats to the information both domestically and extra territorially.\textsuperscript{78} If foreign entities are at the receiving end of this information, the subject might carry a continuing expectation of privacy, pursuant to \textit{Wakeling v United States}\textsuperscript{79}, as I will explain in Part II below.\textsuperscript{80} Additionally, any efforts to assemble information about X for the purposes of a criminal investigation in a warrantless fashion circumvents the golden rule in \textit{Hunter v Southam}, which provides that warrantless searches are \textit{prima facie} unreasonable.\textsuperscript{81}

\textsuperscript{74} See generally \textit{Monaghan}, supra note 46.

\textsuperscript{75} See the comments of Mr. Justice S. Noël in \textit{Re X}, 2016 FC 1105 at paras 12, 24, 37 on the ODAC [\textit{Re X}]. According to \textit{Re X}, reference to the ODAC during litigation involving \textit{Charkaoui v Canada}, 2008 SCC 38, [2008] 2 SCR 326.

\textsuperscript{76} Metadata is information about information that can be used to paint intimate images about work, sleep habits, travel patterns, relationships, places of employment, visits to social and commercial establishments, etc. (Craig Forcese, \textit{“Law, Logarithms and Liberties: Legal Issues Arising from CSE’s Metadata Collection Initiatives”} in \textit{Law, Privacy and Surveillance}, supra note 41 at p 129).


\textsuperscript{78} Lisa Austin explains that “while section 6 adds the qualification that sharing be “in accordance with the law”, the \textit{Privacy Act} permits government institutions to share information with foreign governments and their institutions under an “agreement or arrangement” with that government and does not even require that such arrangements to be in writing (Section 8(2)(f)) (Lisa Austin, \textit{“Anti-Terrorism’s Privacy Sleight-of-Hand: Bill C-51 and the Erosion of Privacy, Edward M Iacobucci & Stephen J Toope, eds, After the Paris Attacks: Responses in Canada, Europe and Around the Globe} (Toronto: University of Toronto Press, 2015) at p 186).

\textsuperscript{79} 2014 SCC 72 [\textit{Wakeling}].

\textsuperscript{80} Ibid at para 39 in which the court states that the: “The highly intrusive nature of electronic surveillance and the statutory limits on the disclosure of its fruits suggest a heightened reasonable expectation of privacy in the wiretap context.”

\textsuperscript{81} \textit{Hunter v Southam}, supra note 31 at p 161.
On the foregoing grounds, it is objectively reasonable for X to expect that his information, and his donation details, will remain with the CRA, rather than being disseminated among government departments for unknown purposes.

To the contrary, there is a line of jurisprudence which obfuscates the argument above, suggesting that records produced in the ordinary course of regulated activities attract a diminished expectation of privacy.\(^{82}\) Case law suggests that a taxpayer’s privacy interest in records that may be relevant to the filing of a tax return is relatively low.\(^{83}\) To that extent, the state might argue that information exchanged under the SoCIS has a diminished expectation of privacy because it was disclosed for regulatory reasons.

Notwithstanding this case law, a diminished expectation of privacy does not foreclose access to section 8 of the Charter. This is made clear in \(R v Cole\), whereby the Supreme Court of Canada emphasized that “a reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy protected by section 8.”\(^{84}\) Returning to our hypothetical, while X might have a diminished expectation of privacy in his tax returns because he or she is statutorily required to produce them, X’s objective expectation of privacy is not jettisoned. Even if a disclaimer is provided on his tax return forms, indicating that the information he discloses may be shared in accordance with the PA,\(^{85}\) this does not mean he has relinquished his expectation of privacy in information about his donation, and any other biographical information arising from this disclosure. That X disclosed tax returns to CRA does not, \textit{ipso facto}, supplant

\(^{83}\) Ibid. See also \textit{McKinlay Transport Ltd.}, [1990] 1 SCR 627 and \textit{R v Ling}, 2002 SCC 74, [2002] 3 SCR 814 a companion decision issued alongside Jarvis.
\(^{84}\) \textit{Cole}, supra note 11 at para 9.
\(^{85}\) For example a standard Income Tax and Benefit (T1 General 2016) form provides the following disclaimer: “Personal information is collected under the \textit{Income Tax Act} to administer tax, benefits, and related programs. It may also be used for any purpose related to the administration or enforcement of the Act such as audit, compliance and the payment of debts owed to the Crown. It may be shared or verified with other federal, provincial/territorial government institutions to the extent authorized by law. Failure to provide this information may result in interest payable, penalties or other actions. Under the \textit{Privacy Act}, individuals have the right to access their personal information and request correction if there are errors or omissions …” (Canada revenue Agency, Income Tax Benefit and Benefit Return, online: <http://www.cra-arc.gc.ca/E/pbg/tf/5000-r/5000-r-16e.pdf> (accessed 25 May 2017)).
his privacy interest in the information and what it tends to reveal. As such, the informational data captured by the SoCIS attracts a REP.

(c) The Case for a Search or Seizure

In addition to the REP analysis, SoCIS disclosures must also constitute searches or seizures for X to claim a section 8 interest. I argue that “sharing up” (from law enforcement/non-security intelligence institutions to security intelligence institutions) and “sharing down” (from security intelligence institutions to law enforcement/non-security intelligence institutions) amounts to search and seizure. Disclosing institutions must search for and identify relevant information captured by the Act, while the receiving institution seizes the information. It is noteworthy that the language of the Charter uses the words search and seizure disjunctively, allowing a search or seizure simpliciter to offend against the section. That is, they are independently sufficient to trigger section 8.

At a basic level, the Supreme Court of Canada defines a search as an inspection and a taking a seizure. In R v Dyment, the Court provided that “the essence of a seizure under section 8 is the taking of a thing from a person by a public authority without that person’s consent.” As it relates to a search, Abella J. in R v Tessling wrote as follows:

First, “not every form of examination conducted by the government will constitute a ‘search’ for constitutional purposes. On the contrary, only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a ‘search’ within the meaning of s. 8”; Evans, supra, at para. 11.

Whereas the basic definition above equates an inspection with a search, Tessling broadens the ambit of a search by interlacing it with intrusions upon privacy. In other words, where a privacy

---

86 As noted in Spencer, supra note 56 at para 44, “the mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public.”
87 Stanley A Cohen, Privacy, Crime and Terror: Legal Rights in a Time of Peril (Markham: Lexis Nexis, 2005) at pp 396 and 397 [Cohen].
88 Milton v The Queen (1985), 16 CRR 215 at p 226 (BC Co Ct).
89 Cole, supra note 11 at para 34.
91 Ibid at p 26; R v Colarusso, [1994] 1 SCR 20 at para 42.
92 Tessling, supra note 51 at para 18 [emphasis added]. See also R v Law, 2002 SCC 10, [2002] 1 SCR 227 at para 15 [emphasis added]
interest is invaded, a search may be meted out. This means that a search need not always manifest in the traditional sense of physically examining a receptacle. In fact, courts have recognized a range of inspections as searches, including the forensic search of a computer, the discovery of an Internet Protocol (IP) address, and the use of a surreptitious camera in a hotel room.

Recall the language of section 5 of the SoCIS. The provision permits disclosures to the head of a government institution or their delegate where authorities intend to detect, identify, analyze, prevent, investigate or disrupt activity that undermines the security of Canada. The use of the terms “detect” and “identify” suggests that authorities will have to search information in some way, be it through a database, or at the very least, using physical records. Otherwise, the information may reach the institution through a regulatory process, like the case of X in the donation hypothetical with CRA. That an institution is authorized to disclose on its own initiative also suggests that the information must be located before the disclosure takes place. Moreover, that an institution must determine relevance requires an inspection of the information, which fits squarely within the definition of a search in *Tessling*.

In *Wakeling, supra*, the Supreme Court of Canada flatly rejected the argument that the disclosure of previously intercepted communications by the state to a foreign entity constitutes a search. Writing for the majority, Moldaver J. concluded that a disclosure of intercepted communications to the United States, authorized by the *Criminal Code*, is “simply the communication to the third party of previously acquired information.”

However, *Wakeling* is distinguishable because the information was obtained by way of prior judicial authorization before it was shared with the Americans. That is not the case with the SoCIS. The SoCIS is a warrantless information-sharing regime which does not require prior judicial authorization. On this basis alone, it is entirely distinguishable from the Criminal Code regime considered in *Wakeling*. It is also noteworthy that, while the traditional analytical approach using a search and seizure did not favour access to section 8 in *Wakeling*, Moldaver J.

---

94 *Spencer*, supra note 56.
96 *Spencer*, supra note 56 at para 32.
97 *Wakeling*, supra note 79 at para 34.
nevertheless found that section 8 protections should apply given the highly intrusive nature of wiretap intercepts and the expectation of privacy that necessarily attaches.

As detailed above, the essence of a search or seizure is the taking of something - information or otherwise. Depending on the factual context, the SoCIS might require government to search for information before it is exchanged or simply seize it from an organization in whose possession it lies. Either way, a search or seizure is triggered depending on the factual context to which the SoCIS is applied. Before I continue with the section 8 analysis to assess whether the SoCIS is unreasonable, it is worth studying what makes laws unreasonable in the first place.
CHAPTER II
SAFEGUARDS AND ACCOUNTABILITY MEASURES IN INFORMATION-SHARING REGIMES

The discussion above would be incomplete without a primer on the constitutional standards demanded by section 8 of the Charter, particularly in terms of what makes a law reasonable or unreasonable. In Part I, I referred to these standards as “safeguards” and “accountability” measures. These are measures that ensure the law strikes a reasonable balance between privacy and the objective of the legislation. For our purposes, I assess whether the SoCIS strikes a reasonable balance between privacy and the ability to thwart activities that undermine the security of Canada. The more intrusive legislation is on one’s REP, the higher the demand for formality and the level of regulation should be.  

In this part, I examine the practical and constitutional rationale for accountability measures and safeguards in Canadian jurisprudence, and having regard for the Commissions of Inquiry involving Maher Arar and Air India. I conclude by identifying the safeguards missing in the SoCIS.

(iii) Safeguards, Accountability and the Reasonableness of Legislation through a Jurisprudential Lens

The case of Hunter v Southam, supra, is a seminal blueprint setting out the basic safeguards required of search and seizure law. As a starting premise, it provides that warrantless searches are prima facie unreasonable under section 8 of the Charter. In declaring the provisions of the Combines Investigation Act unconstitutional, and of no force or effect, Chief Justice Dickson concluded, inter alia, that the impugned provisions failed to provide the appropriate standards

---

98 Stanley Cohen, supra note 87 at p 384.
99 Hunter v Southam, supra note 31 at p 161.
100 Ibid at p 148 reproducing the Combines Investigation Act at s 10. (1) Subject to subsection (3), in any inquiry under this Act the Director [of Investigation and Research of the Combines Investigation Branch] or any representative authorized by him may enter any premises on which the Director believes there may be evidence relevant to the matters being inquired into and may examine any thing on the premises and may copy or take away for further examination or copying any book, paper, record of other document that in the opinion of the Director or his authorized representative, as the case may be, may afford such evidence.(3) Before exercising the power conferred by subsection (1), the Director or his representative shall produce a certificate from a member of the [Restrictive Trade Practices] Commission, which may be granted on the ex parte application of the Director, authorizing the exercise of such power.
for the issuance of warrants including an independent and impartial person authorized to act judicially. The safeguards enumerated eventually became the hallmarks of search and seizure law.

In reaching this conclusion, Dickson J. highlighted that section 8 was intended to protect from unjustified state intrusions before they happen, “not simply determining, after the fact, whether they ought to have occurred in the first place.” This explains why a provision that authorizes an unreviewable power would be inconsistent with section 8. These standards are captured by the following excerpt in Hunter v Southam, where Dickson J. wrote:

While the courts are guardians of the Constitution and of individuals’ rights under it, it is the legislature’s responsibility to enact legislation that embodies appropriate safeguards to comply with the Constitution’s requirements. It should not fall to the courts to fill in the details that will render legislative lacunae constitutional. Without appropriate safeguards legislation authorizing search and seizure is inconsistent with s. 8 of the Charter. As I have said, any law inconsistent with the provisions of the Constitution is, to the extent of the inconsistency, of no force or effect.

Thus, the onus is on legislatures to ensure that privacy interests are protected when enacting laws that authorize search and seizure. The greater the intrusion on privacy, the greater the justification for doing so must be, and the greater the degree of constitutional protection. By this logic, significant intrusions on one’s biographical core of information requires heightened safeguards within the authorizing legislation to ensure that the intrusion is minimized to the greatest extent possible. In that sense, section 8 is a proactive provision, requiring front-end protections to mitigate the harms of the invasion before it occurs.

After Hunter v Southam, two cases provided guidance on the necessity of safeguards in search and seizure legislation: R v Tse and Wakeling, supra.

---

101 Ibid at p 153 citing Prowse J.A. in the decision of Court of Appeal for Alberta and p 169.
102 Ibid at p 160.
103 Ibid at p 166.
104 Ibid at p 169 [emphasis added].
105 R v Simmons, [1988] SCJ No 86 (SCC).
106 Stanley Cohen, supra note 87 at p 43 alludes to this where he writes that greater intrusions on privacy are constrained by supervisory authority.
In *Tse*, section 184.4, the emergency wiretap provision under Part VI of the *Criminal Code*, was struck down because it did not strike a balance freedom from unreasonable search and seizure and the state’s interest in preventing serious bodily harm. Assessing what types of accountability measures would be constitutional imperatives, the Court in *Tse* concluded that: (1) Parliament failed to provide a notice requirement to the subject of the intercept, which prevents the target from ever challenging the police use of the power. Notice would provide some transparency and serve as a further check that the extraordinary power is not being abused; (2) while the absence of a reporting requirement to Parliament and record-keeping on the use of the provision would make sense, they are not constitutional imperatives, and (3) that a statutory restriction on the use of a search and seizure provision is not necessary for constitutional purposes. On the whole, that the provision lacked both a mechanism permitting oversight of police power, and a notice requirement to the person whose private communication is intercepted, rendered it constitutional infirm. Despite the fact that the provision was subsumed by Part VI of the *Criminal Code*, which contained a range of after-the-fact accountability measures, it could not be saved by section 1 of the *Charter*.

*Tse* is noteworthy because it emphasizes the importance of providing notice to the subject. Notice requirements square well with the prospective feature of section 8 which seeks to prevent illegal searches and seizures. Notice also enables the subject to challenge the constitutionality of information obtained without his or her consent. Where the information is obtained for the purposes of a criminal prosecution, notice facilitates the right to make full answer and defence, which is part and parcel of the right to life, liberty and security under section 7 of the *Charter*.

---

108 Ibid at para 19.
109 Ibid at para 84.
110 Ibid at paras 89 and 92.
111 Ibid at para 93. In this case, Parliament required that section 184.4 only be used in exigent circumstances to prevent serious harm.
112 Ibid at para 11.
113 For example, see para 23 in which the Court indicates that other provisions authorizing interceptions required annual statistical reports to Parliament on the use of authorizations and resulting prosecutions, and notice in writing to the object of the interception.
114 Ibid at para 23.
115 *Charter*, supra note 7 at s. 7 reads: “Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.” See also *R v O’Connor*, [1995] 4 SCR 411 at para 104 (SCC) and section 650(3) of the *Criminal Code*, R.S.C., 1985, c. C-46, s 650(3) [*Code*].
Considered in this way, notice is a central feature of accountability because it allows the subject to scrutinize the law authorizing a search or seizure to ensure that state power is not abused.

Two years after *Tse*, the Supreme Court of Canada reviewed the constitutionality of Part VI of the *Criminal Code* again in *Wakeling*, focusing on a different provision this time. Mr. Wakeling was the subject of a cross-border drug investigation that resulted in the RCMP lawfully monitoring and recording his communications with others. That information was shared with US law enforcement authorities and Mr. Wakeling was intercepted at the Canada-US border. In addition to challenging his extradition, Mr. Wakeling argued that section 193(2)(e) of the *Criminal Code*, which permits Canadian authorities to share wiretap information both domestically and with foreign law enforcement agencies, lacked the requisite safeguards required by section 8 of the *Charter*.

Mr. Wakeling relied on the holding in *Tse* to stress that section 193(2)(e) lacked appropriate accountability measures. He argued that it lacked record-keeping and notice requirements, protocols or international agreements, and caveats constraining the foreign state’s use and dissemination of the information. Writing for the majority, Moldaver J. distinguished the holding in *Tse* on two grounds. Firstly, *Tse* involved warrantless searches and seizures, which elevated the importance of after-the-fact notice and reporting requirements. Meanwhile, *Wakeling* involved the prior judicial authorization of private communications, in which Mr. Wakeling’s privacy interests were considered. Moreover, that the entire wiretap scheme included safeguards like written notice and prior judicial authorization was relevant to the constitutional question. The Court did not believe that a second notice requirement at the disclosure stage was necessary because that might compromise a foreign investigation.

The appeal was dismissed on its merits. The provision was upheld, and no section 8 violation was found. The disclosure contemplated by section 193(2)(e) was found reasonable given the

---

116 *Wakeling*, supra note 79 at paras 2-3.
117 Ibid at para 63.
118 Ibid at para 66.
119 Ibid at para 67.
120 Ibid at para 68.
accountability measures built into Part VI of the Code and the provision itself.\textsuperscript{121} That the scheme contemplates criminal sanctions for the improper disclosure of information “creates an incentive to maintain records about what information was disclosed, to whom and for what purpose.”\textsuperscript{122} While highly relevant in determining whether a disclosure is authorized by law, record keeping, adherence to international protocols and caveats on information-sharing were not constitutionally mandated.\textsuperscript{123} The Court concluded that determination of caveats does not guarantee that foreign states will not misuse information. The Court preferred that the assessment of appropriate safeguards plays a crucial role in determining the constitutionality of a challenged disclosure, and must be determined on a case-by-case basis.\textsuperscript{124}

In contrast, Karakatsanis J. viewed the absence of accountability measures as fatal to the scheme, concluding that the provision was unreasonable and contrary to section 8 of the Charter. She distinguished the safeguards in Part VI of the scheme, with those applicable to the disclosure of wiretap information to foreign officials, writing that “ensuring that the wiretapping itself is appropriate does not guarantee that subsequent disclosures will be.”\textsuperscript{125} She disagreed that the possibility of criminal liability is an adequate accountability measure, noting that the more important concern was whether foreign officials, and not Canadian officials, would misuse the information.\textsuperscript{126} Importantly, accountability is not only about fostering compliance with the letter of the law, but about ensuring that statutory powers are necessary and used appropriately.\textsuperscript{127} Broadly speaking, accountability measures deter and identify inappropriate intrusions.\textsuperscript{128} In this respect, Karakatsanis J. wrote:

\begin{quote}
Notice of cross-border disclosure would permit individuals -- or the executive branch of government -- to know which countries have information and perhaps how it may be used. After-the-fact reporting to the legislature would create transparency, telling Canadians how often information is disclosed to identified foreign law enforcement officials and for what purposes […] The Charter does not mandate a specific protocol; it requires only that the legislation authorizing a search be reasonable. \textit{Reasonableness, in}
\end{quote}

\begin{flushleft}
\textsuperscript{121} Ibid at para 73.
\textsuperscript{122} Ibid at para 72.
\textsuperscript{123} Ibid at para 73 and 74.
\textsuperscript{124} Ibid at para 81.
\textsuperscript{125} Ibid at para 136 (per Karakatsanis J. dissenting).
\textsuperscript{126} Ibid at para 137.
\textsuperscript{127} Ibid at para 138.
\textsuperscript{128} Ibid at para 136.
\end{flushleft}
this case, demands accountability mechanisms that ensure an appropriate balance between privacy and the state interest in the search. At a minimum, the disclosing party should be required to create a written record of what information is shared with whom, with some obligation to make the sharing ultimately known to the target or to government.\(^{129}\)

Notwithstanding the majority opinion in *Wakeling*, safeguards are critical when discerning the reasonableness of legislation. This is particularly the case when legislation authorizes the warrantless exchange of information, as is the case with the *SoCIS*. The accountability discussion in *Wakeling* is not unlike *Tse*, in that both acknowledge the nexus between the reasonableness of a law and accountability measures. Moreover, neither case provides a standard list of safeguards that serve as constitutional imperatives. They are particularized on a case-by-case basis depending on the extent of the intrusion and the effect of the impugned provision. Where prior judicial authorization is not required, it is likely that additional safeguards will be necessary to ensure the legality of the legislation.\(^{130}\) Accounting for these cases, the existence of accountability measures within a scheme do not guarantee that a provision subsumed within it will be constitutional.

Despite its laudable hallmarks, the holding in *Wakeling* deferred to Parliament’s discretion to ensure that accountability measures are built into information-sharing legislation. In that sense, the majority restrained its supervisory function. This judicial function breathes life into the rule of law as a fundamental feature of the constitution.\(^{131}\) The rule of law serves as a check on the extent of the state’s powers,\(^{132}\) including the abuse of power that section 8 was intended to protect. As Lisa Austin suggests, the rule of law challenge is about “whether mass surveillance as a mode of rational social ordering is in conflict with the deepest commitments of law as a mode of social ordering.”\(^{133}\) Hence, section 8 of the *Charter* and the rule of law are inextricably interwoven. The demand for safeguards is an expression of this relationship.

\(^{129}\) Ibid at para 142 [emphasis added].
\(^{130}\) *Tse*, supra note 106 at para 84.
\(^{132}\) Ibid at p 202.
\(^{133}\) Lisa Austin, “Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State” in *Law, Privacy and Surveillance*, supra note 41 at pp 105-106.
Overall, the dissent in *Wakeling* better appreciates the relationship between unfettered information-sharing the detrimental impact on one’s liberty. The dissent is in keeping with the purpose of section 8, which is designed to prevent encroachments. I rely on the rationale in the dissenting opinion to support the global argument in this chapter. In doing so, I undertake an analysis of some of the critical underpinnings from the Arar and Air India Inquiries.

(iv) The Danger of Unfettered Information-Sharing and Affiliated Themes with Information Silos: Commissions of Inquiry in the Case of Maher Arar and Air India

Cases like the ones above tend to discuss accountability, oversight and safeguards in abstract terms, making it difficult to appreciate the tangible effects of an unreasonable law on one’s liberty in a national security investigation. The Commission of Inquiry into the Actions of Canadian officials in relation to Maher Arar (2006)\(^ {134}\) sheds light on the reach of unfettered information-sharing by explaining how it has contributed to grave human rights violations. Similarly, the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (2010)\(^ {135}\) touches on extra-territorial distribution of intelligence. While it was more specific to the role of CSIS, it studies the contours of domestic-information sharing and the relevance of safeguards.

In this section, I canvassed the recommendations made in both inquiries, shedding light on the safeguards suggested by each Commissioner. I stressed that while Canada’s national security framework historically operated in information silos, the events of 9/11 and those that followed, have enticed our government to consolidate the gap between criminal law and national security investigations, making them virtually indistinguishable. If these investigations occur on parallel tracks, the role between entities such as the RCMP and CSIS becomes blurred, making it difficult to ensure that safeguards are appropriately implemented and ensured. Instead, the application of safeguards to intelligence_collecting bodies such as CSIS, the RCMP and CSEC are often left to the discretion of the institutions. This review will be instructive for the constitutional challenge I propose in Part III.

\(^{134}\) *Arar vol 1*, supra note 40.

\(^{135}\) *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, (Ottawa: Public Works and Government Services Canada, 2010).
(c) Air India Flight 182: Major Report

In 1985, a luggage bomb blew up Air India Flight 182 over the Atlantic Ocean killing 329 people, including 280 Canadians.\(^{136}\) Hours later, “a bomb destined for a second Air India flight killed two baggage handlers in Tokyo.”\(^ {137}\) It became infamously known as one of the largest aviation disasters in history before 9/11. Two Sikh-Canadian’s were alleged to have perpetrated the crime. These events prompted the Government of Canada to launch a commission of inquiry to understand the factual events that culminated in the fatality, and make recommendations to prevent terrorist attacks in the future.

The Commissioner found that more enhanced intelligence-sharing would have identified the threat, and furthermore, that uncooperative behaviour between CSIS and the RCMP delayed and stymied the investigation.\(^{138}\) At the time of the attack, CSIS was just under a year old, and newly adjusting to its role as Canada’s secret service.\(^ {139}\) Little thought had gone into the relationship between CSIS and the RCMP, particularly in terms of intelligence gathering and reporting requirements.\(^ {140}\) Prior to the bombing, the RCMP possessed intelligence about Sikh extremists planning to bomb Air India flights, and failed to share it with CSIS.\(^ {141}\) Needless to say, issues surrounding information sharing protocols, retention periods and screening information for accuracy, reliability and relevance were central to the Commissioner’s recommendations.

At the time, families of the victims suggested that CSIS’ discretion in disclosing information be abolished. During the inquiry, the Attorney General of Canada submitted that doing so might result in the RCMP having full access to information and innocent people being “drawn into an investigation solely on the basis of a link to a CSIS target.”\(^ {142}\) Commissioner Major agreed, recommending that CSIS should have some discretion in deciding whether to provide


\(^{137}\) Ibid

\(^{138}\) Ibid at p 46.

\(^{139}\) Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23 [CSIS Act].


\(^{141}\) Ibid.

\(^{142}\) Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, The Relationship Between Intelligence and the Challenges of Terrorism Prosecutions, vol 3 (Ottawa: Public Works and Government Services Canada, 2010) at p 86.
information to prosecutors, particularly given the risk of disclosure.\textsuperscript{143} He noted that CSIS should only be obligated to report information about threats to the national security of Canada within the scope of its statutory mandate.\textsuperscript{144} With more safeguards to protect the information and its further dissemination, CSIS might be more willing to provide information directly to the RCMP.\textsuperscript{145} After much consultation, the Commissioner encouraged greater information sharing with other agencies, and retention policies to safeguard the privacy of the information.\textsuperscript{146}

At the time the SoCIS was introduced, the federal government purported that the Air India recommendations informed the legislation. For example, Minister Blaney testified that the SoCIS was a “response to the Air India commission and to many other requests.”\textsuperscript{147} This is difficult to believe because the Air India report was released in 2010, providing the government ample opportunity to address the recommendations during its early days in office. Rather, it seems that the Act represents a feeble attempt to pay lip-service to broad stroke themes selectively chosen from the Air India and Arar reports. Overall, it fails to account for the fine print in both reports, which explains the implications of unfettered information-sharing. More importantly, it fails to strike a balance between too much information sharing, and none.

Considered alongside one another, the Arar and Air India reports appear to sit at two ends of the spectrum. On the one hand, the Arar report provides a cautionary approach to information-sharing, while the Air India recommendations embrace a more integrated approach between law enforcement and intelligence. Canada’s information-sharing dynamic seems to oscillate between the two depending on the government of the day. Despite these differences, the report findings meet on a crucial feature: information-sharing is best achieved when it is accurate, reliable, and qualified by caveats. And subject to review- Arar stresses propriety based review by SIRC whereas AI stresses efficacy based review by the National Security Advisor. This begs the question: are the information-sharing safeguards provided in both inquiries incorporated into the SoCIS? I assess this question in the next section, and refer to the measures countenanced by the Supreme Court in \textit{Wakeling} and \textit{Thompson}.

\textsuperscript{143} Ibid at p 87.
\textsuperscript{144} Ibid.
\textsuperscript{145} Ibid at p 89.
\textsuperscript{146} Ibid at pp 335 and 336, Recommendations 9 and 10.
\textsuperscript{147} House of Commons, Standing Committee on Public Safety and National Security Evidence, 41st Parl, 2\textsuperscript{nd} Sess, No 53, (10 March 2015) at 0855 (Hon. Stephen Blaney).
(d) 

Maher Arar: The O’Connor Report

As alluded in Part I, the case of Mr. Arar is a salient example of the extent to which information-sharing practices can restrict the liberty of an innocent person. The case was born out of a meeting of RCMP, domestic and foreign partner agencies at RCMP Headquarters a few days after the events of September 11, 2001.\footnote{Arar Vol 1, supra note 40 at p 37.} Discussion about the “need for increased cooperation and coordination among the agencies, including the need to share relevant information in a timely manner”, resulted in the formation of Project A-O led by the RCMP.\footnote{Ibid.}

Project A-O’s objective was to use every tool possible to ensure that 9/11 was not repeated, including sharing information with agencies both domestically and abroad.\footnote{Ibid at p 36.} The need to share information so readily was partially attributed to the RCMP’s lack of experience in terrorism investigations and the utility of other agencies in helping them learn about potential threats.\footnote{Ibid.}

Justice O’Connor found that “according to the commanding officer of “A” Division, the only way the RCMP was going to be successful in the fight against terrorism was to share information.”\footnote{Ibid.} The arrangement was described as an “open book investigation” involving the “free flow of information” without: (1) a written agreement; (2) caveats on the use and further disclosure of information; (3) the application of RCMP policies relating to national security investigations; and (4) consent from CSIS to disclose the material to American authorities.\footnote{Arar Vol 1, supra note 40 at p 38 and 39. At p 94, Commissioner O’Connor also found that “CSIS officials did not concur that an agreement was in place permitting the RCMP to transfer CSIS material subject to a third party caveat, without CSIS consent.”}

Partners in the agreement were permitted to share documents and information without the consent of the originator, or scrutiny into the relevance or reliability of the information.\footnote{Ibid at p 38.} Because the agreement was never reduced to writing, the minutiae of detail exchanged proved daunting upon review.
Nevertheless, the Commission discovered that CSIS provided a great deal of intelligence on Mr. Arar, and others suspected of being involved in threats to Canadian security, to the RCMP.\textsuperscript{155} The information was centrally stored on a database called the “Supertext”, which was eventually transferred to American authorities.\textsuperscript{156} Information disclosed included but was not unlike the information captured by the SoCIS:

(1) Detailed biographical information about Mr. Arar, including his immigration records;
(2) Canada Revenue and Canada Customs documents;
(3) Surveillance reports, photos, operational notes, situational reports, investigators’ notes and interview notes;
(4) Faxes, business materials, address books, phone lists and an agenda;
(5) References to Mr. Arar as a “suspect”, “principal subject”, target or important figure;
(6) Requests for lookouts at the border describing Mr. Arar and others suspected as a “group of Islamic Extremist individuals suspected of being linked to the al-Qaeda terrorist movement”;
(7) Information that Mr. Arar applied for a gun permit in 1992 which was referred to as a “strange thing”;
(8) Erroneous information relating to suspected affiliates including Youssef Almalki;\textsuperscript{157}

In September 2002, Mr. Arar was returning from a trip to Tunisia, and connecting through John F. Kennedy International Airport in New York. Equipped with this uncorroborated intelligence from Canadian officials, American officials detained Mr. Arar and subsequently imprisoned him at the Metropolitan Detention Centre for four days without access to a lawyer, or officials at the Canadian embassy.\textsuperscript{158}

Commissioner O’Connor found that the information provided by the RCMP to the Americans likely played a role in the decision to transfer Mr. Arar to Syria on October 2, 2002.\textsuperscript{159} Meanwhile, the Commission did not receive a first-hand explanation from the Americans as to why Mr. Arar was transferred to Syria, as American authorities denied the invitation to testify in the inquiry, but it was determined that he was removed for allegedly being a member of Al-Qaeda.\textsuperscript{160}

\textsuperscript{155} Ibid at pp 14-16.
\textsuperscript{156} Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar: Factual Background, vol 2 (Ottawa: Public Works and Government Services, 2006) at p 545, 559 and 561 [Arar Vol 2].
\textsuperscript{157} Ibid at p 561 and 562.
\textsuperscript{158} Arar Vol 1, supra note 40 at p 195.
\textsuperscript{159} Ibid at p 37.
\textsuperscript{160} Ibid at p 204.
In October 2003, just over one year after his detention in the United States, Mr. Arar was released and returned to Canada. He reported being tortured by the Syrians both physically and psychologically.\(^{161}\) At the time, reported methods of torture in Syria included electrical shocks, pulling out fingernails, and forcing objects into the rectum beating, among several other techniques.\(^{162}\)

Mr. Arar’s experience is a resounding case of unfettered information-sharing gone wrong, and it is not the only such example in Canada. Consider the cases of Ahmad Elmaati, Muayyed Nureddin, and Abdullaah Almalki who were also caught by CSIS’ intelligence sweep after 9/11. Elmaati and Almalki were allegedly affiliated with Arar, while Nureddin, an Iraqi-geologist, was believed to be a financial courier for Islamic extremists.\(^{163}\) Their biographical information was shared with American authorities based on these suspicions about their affiliations. When traveling through Syria, they too were detained, interrogated, and tortured. Justice Frank Iacobucci, who led a commission of inquiry on these cases, concluded that by sharing information with the Americans, the actions of Canadian officials, directly or indirectly, resulted in the detention and torture of Elmaati, Nureddin and Almalki.\(^{164}\)

In terms of common ground, both the Iacobucci and the O’Connor reports recognize the importance of information-sharing to avoid future threats of terror. However, the O’Connor report is stalwart in recommending that information exchanged is relevant, reliable and accurate.\(^{165}\) It guides the intelligence community by providing examples of safeguards to facilitate the smarter exchange of information. It is worth considering Commissioner O’Connor’s findings in this respect:

---

\(^{161}\) *Arar Vol 2*, supra note 156 at p 473.

\(^{162}\) Ibid at p 567.

\(^{163}\) *Iacobucci Report*, supra note 39 at p 253.


\(^{165}\) *Arar, Vol 2*, supra note 156 at p 334.
... it can be dangerous to rely on implicit or verbal understandings when dealing with foreign agencies because there is often more unpredictability and a lesser degree of accountability in such circumstances than when interacting with domestic agencies. As I discuss below, respect for human rights cannot always be taken for granted. Caveats are thus particularly important to limit the use and dissemination of information shared with foreign agencies.\textsuperscript{166}

[...]

One of the significant flaws in Project A-O Canada’s investigation was the Project’s failure to place caveats on information that it shared with American agencies. Failure to attach caveats is unacceptable because it increases the risk that information will be distributed by the recipient to unanticipated institutions and that it will be used for unintended and possibly unacceptable purposes. Attaching proper caveats is a routine administrative matter that is vital for ensuring that, when information is shared in national security investigations, it is for specific purposes and with specific institutions. Caveats ensure responsible and accountable information sharing.\textsuperscript{167}

On a similar note, Commissioner O’Connor aptly warned that information-sharing agreements should ensure that investigations are not founded upon racial, religious or ethnic profiling.\textsuperscript{168} He added that this would necessarily prompt the need to train staff on issues dealing with the Muslim and Arab community.\textsuperscript{169}

While the primary concern of the O’Connor report was the exchange of information to foreign entities, the issue of safeguards in the domestic information sharing sphere, particularly between CSIS and the RCMP, was also salient to the analysis. Commissioner O’Connor recommended law enforcement should ensure that information-sharing agreements are reduced to writing.\textsuperscript{170} He emphasized that oversight of the RCMP ought to focus on “practices pertaining to information sharing”, including the provision and receipt of information.\textsuperscript{171} Furthermore, accuracy and precision when screening for the relevance and reliability of information, prior to sharing it, was heavily scrutinized.\textsuperscript{172} For example, he stressed that suspects should always be distinguished

\textsuperscript{166} Ibid at p 321 [emphasis added].
\textsuperscript{167} Ibid at p 339 [emphasis added].
\textsuperscript{168} Ibid at p 356.
\textsuperscript{169} Ibid at p 357.
\textsuperscript{170} Ibid at p 316.
\textsuperscript{171} Ibid at pp 331, 332.
\textsuperscript{172} Ibid at pp 333-334.
from persons of interest where information falls short of creating a suspicion that the person committed an offence or constitutes a threat.\textsuperscript{173}

On application, findings from the O’Connor report suggest that the absence of legislative caveats, and independent oversight in the SoCIS is troublesome for the future of information-sharing in Canada and with foreign partners. While the guiding principles in the SoCIS emphasize the importance of respecting caveats, they are virtually unenforceable. On the other hand, an absolute bar on information sharing would not do either. The benefits of information sharing are multi-faceted, particularly from a public safety standpoint. This was highlighted by the Air India inquiry, which was released after the Arar inquiry, and which equally gained the attention of the intelligence community.

(ii) Accountability, Safeguards and Oversight: Reasons that the SoCIS is an Unreasonable Law

Having regard for the Air India and Arar recommendations, I argue that the SoCIS lacks accountability measures, proper oversight, and adequate safeguards. By accountability, I mean the “processes in which officials and organizations provide explanations and justifications for their conduct.”\textsuperscript{174} By oversight, I refer to the “command and control process where those who practice oversight may be able to influence the conduct that they are examining.”\textsuperscript{175} Finally, safeguards include the measures I described above, including but not limited to caveats on information-sharing. Safeguards and oversight mechanisms sit under the broader accountability umbrella.

(a) The SoCIS Cannot Borrow its Lawfulness from Other Acts

As a starting premise, the SoCIS cannot escape Charter scrutiny simply because it is authorized by law. Borrowing from Stanley Cohen, “the fact that government lawfully acquires personal

\textsuperscript{173} Ibid at p 336.
\textsuperscript{174} Kent Roach, “Permanent Accountability Gaps and Partial Remedies” in Law, Privacy and Surveillance, supra note 41 at p 168.
\textsuperscript{175} Ibid at p 167 citing Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, A New Review Mechanism for the RCMP’s National Security Activities (Ottawa: Public Works, 2006) at pp 456-458.
information does not mean that it can necessarily share it with others.”

Similarly, “the requirement of a lawful authority cannot be avoided by resorting to less demanding prerequisites for information sharing applicable in an administrative process in order to secure information for purposes of a criminal prosecution.”

Our hypothetical explains why. Assuming that X’s information is lawfully collected under the Income Tax Act, other institutions cannot latch on to this authority, claiming it for themselves. Collecting institutions should be cognizant that, where the predominant purpose of disclosure is related to a penal outcome, it will be subject to the same constitutional standards applied to CSIS and the RCMP. This means that the SoCIS requires its own safeguards and accountability measures to pass constitutional muster. It cannot simply prefer the exchange of information en masse, “throwing wide open the barn doors on information sharing but in such a complex and unnuanced way.” Having regard for these issues, this section identifies why the SoCIS that fail to meet the constitutional standards provided in section 8 of the Charter.

(b) The Manner Information is Shared and Stored

The SoCIS does not dictate the medium of exchange for information-sharing. Platforms may include, but are not limited to emails, physical mail, or telephone calls. How information is exchanged bears a direct relationship with its susceptibility to being lost or compromised through a data breach.

Different means of sharing information carry inherent advantages and disadvantages. For example, an email can easily be forwarded to an unintended recipient prematurely or by error. Similarly, a physical exchange of documents can be photocopied, misplaced or accidentally discarded. Where information is accidentally deleted, it is difficult to discern whether it was shared in the first place, making it difficult for X to challenge the initial disclosure. Electronic communications are also vulnerable to hackers. In 2017, several public institutions around the world, including hospitals, were hacked by a malware virus, which required a ransom of bitcoin

176 Cohen, supra note 87 at p 97.
177 Ibid at p 358.
178 Jarvis, supra note 82 at para 2.
179 False Security, supra note 25 at p 140.
currency to salvage files from computers.\textsuperscript{180} The breach was described as unprecedented, with a reach that spanned several countries, and impacting thousands, including medical patients whose information was compromised.\textsuperscript{181} These types of large-scale breaches are difficult to thwart, rendering information obtained through the SoCIS vulnerable if exchanged and/or electronic stored.

Canada is not immune from cyber-attacks or data breaches. In 2012, Environment Canada reported the loss of a laptop containing the personal information of thirteen people the department was intent on hiring.\textsuperscript{182} Around the same time, the Department of Employment Skills Development Canada reported losing “a small portable hard drive containing personal information of about 583 0000 Canada Student Loan recipients” and “250 departmental employees.”\textsuperscript{183} Information included names, date of birth, addresses, social insurance numbers and financial information.\textsuperscript{184} The drive was not password-protected.\textsuperscript{185}

Similarly, between 2011 and 2012, the Privacy Commissioner of Canada reported more than 50 inappropriate disclosures of taxpayer information.\textsuperscript{186} In that timeframe, a CRA employee permitted a friend to download 2, 700 personal tax files onto a laptop.\textsuperscript{187} In 2017, the largest breaches in the agency’s history transpired, whereby eight CRA employees were fired for improperly accessing taxpayer information.\textsuperscript{188} These are just a few of the publicly disclosed breaches, although there may be more. While these departments do not have mandates to collect intelligence, information they collect might be used for such purposes, elevating the need for safeguards to protect it.

\textsuperscript{181} Ibid.
\textsuperscript{183} Ibid.
\textsuperscript{184} Annual Report Privacy Commissioner, supra note 1 at p 10.
\textsuperscript{185} Press, supra note 177.
\textsuperscript{186} Privacy Commissioner of Canada, Audit Report of the Privacy Commissioner of Canada on Canada Revenue Agency (Ottawa: Minister of Public Works and Government Services Canada, 2013) at p 22.
As it stands, institutions are not legally required to report data breaches to the Privacy Commissioner, although the Treasury Board of Canada requires institutions to report material breaches. In his 2015-2016 Annual Report, the Commissioner reported 298 Privacy Act data breach reports among a range of several others in the private sector. He explains that as technological change increases collection, storage and sharing of information exponentially, there ought to be a legal requirement safeguarding personal information. That hundreds of institutions reported data breaches points “to a lack of adequate safeguards.” Some institutions, including Health Canada, even failed to report such breaches. It goes without saying that data breaches are not new phenomena – they remain ongoing and it is unclear which institutions captured by the SoCIS have the safeguards necessary to protect sensitive information.

If the need for safeguards at the departmental level is critical, it stands to reason that safeguards for intelligence stored by Canada’s spy service warrant greater attention. This concern is echoed by Noël J. in Re X, 2016 FC 1105. In Re X, the Federal Court convened an en banc panel of all designated national security judges. The hearing was convened after the Court discovered, through the 2015-2016 report from CSIS’ oversight body, the Security Intelligence Review Committee [“SIRC”], that CSIS was storing associated data in a database called the Operational Data Analysis Centre (ODAC), alluded to above. Associated data is bulk data collected through warrants “from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defense, or international affairs” The ODAC is designed to process information, draw links between sources that humans are incapable of doing, and reveal specific intimate details on the life and environment of the suspect investigated. Since 2006, data has been stored in the ODAC for investigative purposes. It is retained indefinitely, even if the underlying content is non-threat related.

---

189 Annual Report Privacy Commissioner, supra note 1 at p 11.
190 Ibid at p 7.
191 Ibid at p 10.
192 Ibid.
193 Ibid at p 11.
194 This issue originally arose because CSIS wanted to amend its draft warrant templates in light of recent legislative changes and apply for warrants under sections 12(1) and 21 of the CSIS Act, supra note 160 (Re X, supra note 75 at para 1).
195 Re X, supra note 75 at para 33.
196 Ibid at para 42.
197 Ibid at para 44.
By failing to inform the court of its retention program, CSIS breached its duty of candour.\footnote{Ibid at para 7.} After all, CSIS is only statutory authorized to collect information within the meaning of “threats to the security of Canada”, only to the extent that it is “strictly necessary” as provided by in the \textit{CSIS Act}.\footnote{\textit{CSIS Act}, supra note 136, s 12 reads: “12 (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.”} Noël J. examined this issue in \textit{Re X}, concluding that:

\ldots it is crucial to distinguish that incidental collection of non-target and non-threat related information does not form part of what is “strictly necessary” to collect. Therefore, non-targeted and non-threat third party information may only be retained for a short period of time in order that it is not related to national security. If, after a short time period, the information is determined not to be related to threats to the security of Canada as defined by section 2 of the \textit{CSIS Act}, or of assistance to a prosecution, to national defence or international affairs, it must be destroyed.\footnote{\textit{Re X}, supra note 75 at para 186.}

The above excerpt signifies the court’s concern with accountability as a broader theme. Relatedly, the court rejected CSIS’ request to allow service employees to make decisions about warrant conditions. It stated that “the transfer of such responsibilities to a category of unidentified CSIS employees would not serve to enhance accountability.”\footnote{Ibid at para 22.}

The Court’s pronouncement bears equal application to the \textit{SoCIS} and our hypothetical. Noël J. explained that CSIS was no longer required to request a warrant to obtain information from CRA.\footnote{Ibid at para 46.} This leaves X’s information available to share. Moreover, it is not unreasonable to suggest that CSIS will use the ODAC to store \textit{SoCIS} data. Given the ODAC’s correlation capabilities, and the fact that the \textit{SoCIS} encourages and facilitates the analysis and detection of activities that undermine the security of Canada, it would be imprudent for CSIS to store the information anywhere else given its investment in a state of the art data retention program. Undoubtedly, the program’s massive data-retention capacity suggests a high capacity to retain biographical information. One would be remiss to argue that CSIS is unaware of the privacy
implications of its bulk data sets. How it will manage these privacy concerns moving forward, given the increase of unassociated data that will accrue under the SoCIS, is a morass that is unclear.

While very little is known about the ODAC, it will likely be scrutinized in the immediately foreseeable future. The SIRC, CSIS’ oversight body, explains that it will continue to monitor how CSIS “leverages information received from other government agencies and departments” moving forward, particularly in respect of the SoCIS. This signals the faint possibility that the public will learn more about how information is exchanged and stored at some point in the future.

By implication, institutions with or without national security mandates may be subsumed by the SIRC’s oversight capacity. Where that is not the case, several institutions will be free of independent scrutiny. It is noteworthy that SIRC’s mandate is exclusive to the CSIS. If other institutions are mentioned in its review, it will be because they have interacted with CSIS, not because they are accountable to the SIRC. Presently, fourteen of the seventeen institutions authorized to receive information for national security purposes under the SoCIS are not subject to independent review or oversight.

In light of the foregoing, the current iteration of the SoCIS is unlikely to withstand constitutional scrutiny. Absent any meaningful safeguards prescribing how information must be shared, and stored, it is difficult to salvage the Act. As made clear by the dissent in Wakeling, absent meaningful safeguards embedded in the regime, there is a risk that the legislation will be rendered unconstitutional. Since domestic safeguards tend to lose their force when shared across jurisdictional lines, the potential for the SoCIS’s international reach calls for strong internal safeguards.

---

204 CSIS Act, supra note 136 at ss 34 and 38.
206 Annual Report Privacy Commissioner, supra note 1 at p 17.
207 Wakeling, supra note 79 at para 118 (per Karakatsanis, dissenting)
(c) The Absence of Training, Designated Staff, and Related Unknown Regulations

Oversight of data retention is only one piece of the accountability puzzle. Heads of institutions and their delegates, as mandated by the SoCIS, are linchpins to information-sharing programs. Many institutions captured by the Act neither have specific national security mandates, nor do their staff have sufficient training to: (a) identify information that is relevant to threats that undermine the security of Canada; (b) ensure that the method of exchange is safeguarded to protect privacy interests; or (c) ensure that the data is stored securely.

Section 10 of the SoCIS provides a general framework for regulations that touch on these issues. However, it leaves that discretion entirely in the hands of Cabinet. The provision reads:

The Governor in Council may, on the recommendation of the Minister of Public Safety and Emergency Preparedness, make regulations for carrying out the purposes and provisions of this Act, including regulations:

(a) Respecting the manner of disclosure under section 5;
(b) Requiring requires to be kept and retained in respect of that disclosure; and
(c) Respecting the manner in which those records are kept and retained.

In addition to these powers, Cabinet may also add or remove institutions, and the title of their heads, in the schedules appended to the SoCIS.\(^{208}\)

In effect, the presence or absence of safeguards rests with Cabinet. This means that regulations may come and go rapidly, depending on the government of the day. Regulations may be difficult to follow and implement, particularly if often amended. The benefit of maintaining consistent rules will better equip staff to learn how to apply them, without adjusting to new procedures. It is noteworthy that while regulations are implemented on the recommendation by the Minister of Public Safety, the SoCIS does not indicate whether the heads of each disclosing institution will be consulted in the process.

Meanwhile, there is some indication that the Department of Public Safety produced a Deskbook to assist institutions in implementing the SoCIS. According to the Privacy Commissioner of

\(^{208}\) SoCIS, supra note 6 at ss 10(2) and (3).
Canada, it is a confidential manual that guides employees on how to employ the SoCIS,\(^{209}\) but does little to mitigate the likelihood of data breaches. Upon inspection of the Deskbook, the Privacy Commissioner concluded that it lacks guidelines on core elements that should form information sharing agreements, adequate explanation of thresholds that trigger the SoCIS, specific case scenarios where information should be disclosed, guidance on preventing inadvertent disclosures and destroying or returning information that cannot be lawfully collected, factors that mitigate against disclosure, and contents of records that should be kept.\(^{210}\) Notably, internal directions, including this Deskbook, are confidential and inaccessible to the public.\(^ {211}\)

Without access to the contents of the Deskbook, it is not clear which federal staff will be authorized, trained and knowledgeable about the strictures of the Act. As it stands, many of the heads of institutions authorizing or receiving disclosures are presidents or chiefs of the institution. Some heads are listed as Ministers, including the Minister of Public Safety and Emergency Preparedness, National Defence, Foreign Affairs, Citizenship and Immigration, and Finance.\(^ {212}\) As members of Cabinet, Ministerial decisions on lateral or horizontal departmental exchanges will likely be influenced by the political orientation if the governing party. Other heads, including the Chief of the Communications Security Establishment, or the Chief of Defence Staff, are likely to favour the interests of their institution over privacy interests.

It is unlikely that the heads of institutions will have the time to review all SoCIS disclosures. Decision-making authority will likely be delegated to public servants at the departmental level. This raises a questionable delegated authority. A common principle of administrative law emerging from the Latin maxim “delegatus non potest delegare” prohibits delegated authority or power to be re-delegated.\(^ {213}\) Drawing on this principle, it might be argued that Parliament only delegated authority to disclose to the head of a recipient institution, and by consequence, lay staff should not be responsible for SoCIS disclosures. For the sake of efficiency and expediency, this suggestion might seem ludicrous. However, when measuring the nature of the information

\(^{209}\) Annual Report Privacy Commissioner, supra note 1 at p 18.

\(^{210}\) Ibid at p 18 and 19.


\(^{212}\) SoCIS, supra note 6, Schedule 3.

captured by the Act against this restraint, it seems far from unreasonable. Based on the foregoing, and pursuant to the second prong of the section 8 framework, the SoCIS is an unreasonable law.\textsuperscript{214}

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{214} In the alternative, the analysis would continue to the third and fourth prong of the section 8 test. Given the word limitations on this thesis, further analysis is not feasible.
\end{itemize}
\end{footnotesize}
CHAPTER III

THE SoCIS CANNOT BE JUSTIFIED BY SECTION 1 OF THE CHARTER

Once a law is found unreasonable, the onus shifts to the state to justify the infringement on a balance of probabilities, pursuant to section 1 of the Charter. Section 1 “guarantees the rights and freedoms set out in it subject only to such reasonable limits as can be demonstrably justified in a free and democratic society.” In the seminal case of R v Oakes, Dickson J. explained that free and democratic society is one that embodies

…respect for the inherent dignity of the human person, commitment to social justice and equality, accommodation of a wide variety of beliefs, respect for cultural and group identity, and faith in social and political institutions which enhance the participation of individuals and groups in society.

In this section, I assess whether the SoCIS is justified under section 1, having regard for the values espoused in Oakes, and others that have evolved since. In doing so, I study whether: (1) the SoCIS has a pressing and substantial objective; and (2) the means used to further the objective are reasonable and demonstrably justified, and therefore proportional. I conclude that while the SoCIS presents a pressing and substantial objective, the measures used to obtain the objective are disproportionate to the limitations on the right to be free from unreasonable search and seizure.

(j) Does the SoCIS have a pressing and substantial objective?

According to the Green Paper Backgrounder, the SoCIS appears to have two broad objectives. First, it creates “an explicit authority, which provides greater certainty about when institutions can share information for national security reasons.” Secondly, it “provide[s] flexibility to accommodate new forms of threats that may arise” in Canada as part of the global war on
Put another way, there are both micro and macro level objectives built into the scheme – the former domestic and the latter international.

There is some indication that the first objective is true, given the complexity of information-sharing laws in Canada. An internal CSIS briefing note pre-dating Bill C-51, obtained by way of access to information, speaks to the same issue:

Currently, departments and agencies rely on a patchwork of legislative authorities to guide information sharing…. Generally, enabling legislation of most departments and agencies does not unambiguously permit the effective sharing of information for national security purposes.

Reports also demonstrate that the “complexity of the legal landscape” slows the process of information sharing down, producing delays that hinder critical and time sensitive public safety investigations. On this issue, Minister Blaney said this at second reading in the House of Commons:

Canadians legitimately expect that if one branch of government is aware of a threat to their security that this information would be shared with other branches of government to protect Canadians. This is not the case and we need to fix this with this bill.

In many cases, barriers to effective information sharing are rampant across government, slowing the speed of this exchange to a crawl or acting as a total barrier. These barriers exist in the form of often well-intentioned legislation; however, in the national security context, they manifest themselves into unacceptable silos that put Canadians at risk.

These information silos are references to the Air India inquiry. However, his words signal the government’s intent to fill “legislative gaps by providing clear authority to share information in

---

221 Ibid at p 27.
222 Righting Security, supra note 20 at p 21 citing CSIS, “Memorandum to the Director, Deputy Minister Meeting on National Security Information Sharing” (5 February 2014) CSIS ATIP request 117-2014-393 at 2.
224 Blaney Second Reading, supra note 26.
cases where such authority currently does not exist or is subject to competing interpretation."225
The breadth of the information-sharing authority speaks to this intention.

This micro-level, domestic justification seems to be the underlying reason for enacting the SoCIS. However, legislative debates suggest that Canada’s role in maintaining international security may have played a more dominant role in determining the framework of the SoCIS. Excerpts from Minister Blaney’s speech continued from the above are worth reviewing:

Mr. Speaker, I rise in the House today to deliver on our government's firm commitment to fight and protect Canadians from jihadist terrorists who would destroy the very principles that make Canada, our country, a nation of freedom and democracy that is the envy of the world.

The international jihadist movement has declared war on Canada and our allies. As we have seen, terrorists are targeting Canadians simply because they despise our society and the values it represents. Let us not forget the October 20 attack in Saint-Jean-sur-Richelieu and the attack that happened right here in our national capital. Those incidents are etched in our hearts and in our memory and show us how serious these issues are for us as a country.

While Hansard Debates often mirror partisan talking points, they are relevant in determining the objective of legislation. Legislative intent “is often stated in the legislation, but it may also be ascertained by reference to extrinsic material such as Hansard and government publications.”226

In this case, Hansard debates are clear that the objective of the Act is essentially two-fold: clarity in the law for national-security related information sharing and the protection of both domestic and international security in the so-called “war on terror.” On these grounds, it would be difficult to argue that the SoCIS lacks a pressing and substantial objective.

(v) Are the measures in the SoCIS reasonable and demonstrably justified in a free and democratic society?

The second half of the Oakes analysis assesses the proportionality of the law.227 It is three-pronged, requiring the impugned legal measures to: (1) be rationally connected to the objective of the law; (2) minimally impair the right or freedom in question; and (3) be proportional in their

225 PSC Public Framework, supra note 235.
227 R v Big M Drug Mart, [1985] 1 SCR 295 at p 352 (SCC) [Big M Drug Mart].
effects with the objective of the law.\textsuperscript{228} In \textit{Big M Drug Mart}, the Supreme Court of Canada recognized that the purpose and effect of the law are clearly linked, if not indivisible.\textsuperscript{229} That is why the intended and actual effects are often considered in determining the legislative object and its validity.\textsuperscript{230} Having regard for these principles, I begin my analysis with the first component of the proportionality test.

\textit{(vi) \textit{Rational Connection}}

To establish a rational connection, the state must show a causal connection between the infringement and the benefit sought based on reason and logic.\textsuperscript{231} This means that the limitation on the right must not be arbitrary, unfair or based on irrational considerations.\textsuperscript{232} A “law that does not rationally advance the pressing and substantial purpose for which it was enacted can be described as unnecessarily restricting the right or freedom.”\textsuperscript{233} This stage of the proportionality analysis is focused on the coherence between the measures and the government’s goals underpinning the legislation.\textsuperscript{234} I argue that the effects of the privacy-infringing provisions of the \textit{SoCIS} are rationally connected to the objectives of the law.

The infringing measures of the \textit{SoCIS} are largely found in sections 2, 5 and 6. These provisions respond to the two objectives listed above. There is both a theoretical and practical connection between these measures and the objective of the law.

Theoretically, sharing national-security related information to detect, identify, analyze, prevent, investigate and disrupt activities that undermine Canada’s security directly relates to the objective of protecting the public. While agencies such as CSIS, CSEC and the RCMP have

\begin{itemize}
\item \textsuperscript{228} \textit{Oakes}, supra note 227 at para 70.
\item \textsuperscript{229} \textit{Big M Drug Mart}, supra note 221 at para 80.
\item \textsuperscript{230} Ibid.
\item \textsuperscript{232} \textit{Oakes}, supra note 209 at para 70; \textit{Hutterian Brethren}, supra note 243 at para 48.
\item \textsuperscript{233} Patrick Macklem & Carol Rogerson eds, \textit{Canadian Constitutional Law}, 4\textsuperscript{th} ed (Toronto: Emond Montgomery Publications, 2010) at p 777.
\item \textsuperscript{234} \textit{Hutterian Brethren}, supra note 243 at para 51.
\end{itemize}
sufficient investigatory tools, the global reach of extremist networks is pervasive, and often requires cooperation between law enforcement bodies and their corollaries.235

Practically, by sharing information, institutions with national security mandates will benefit from intelligence that might then be used to extrapolate further information. Moreover, that institutions have the discretion to share information when they determine its relevance, provides a clear legislative authority that does not exist elsewhere in Canadian law. The “relevance” threshold built into section 5 facilitates exchanges because it is intended to capture a wide ambit of information. By not requiring prior judicial authorization, the Act also enhances the expedience of information-sharing.

Finally, there is a rational connection between information-sharing for the purpose of filling gaps between information-silos. Minister Blaney described barriers to information-sharing manifesting “into unacceptable silos” that put the public at risk.236 Similarly, both the Air India and Arar reports emphasize the importance of information-sharing in the context of preventing national security threats.237

Such links between the rationale for an information-sharing regime, the protection of the public and a clear authorizing authority suggest that the SoCIS is not arbitrary, unfair or based on irrational principles. It is not unlikely that the SoCIS would survive this part of the Oakes test.

(vii) Minimal Impairment

The measures of a law can be rationally connected to its purpose, but it must still be minimally impairing to survive the Oakes test. This stage is akin to an overbreadth analysis, in which the court must decide whether a law falls within a range of reasonable alternatives available to Parliament when enacting the law.238 At this stage, we must ask whether there are less harmful means of achieving the legislative goal.239

235 Stanley Cohen, supra note 87 at p 255 who supports this proposition by stating that “Ordinary law enforcement can be an important source of domestic intelligence (even as regards international investigations) on matters affecting the national security…”
236 Blaney Second Reading, supra note 26.
238 RJR, supra note 243 at para 160.
239 Hutterian Brethren, supra note 243 at para 53.
Firstly, at the very least, the subject should be provided with notice. Without notice, X would have no way of knowing that his personal information was shared. If X were charged with terrorism-related offences arising out of a SoCIS disclosure, his counsel would undoubtedly request all available disclosure. Whether the government would disclose the information about how the SoCIS disclosure was obtained in the first place is not entirely certain. If the disclosure is declared claimed? a national security privilege under section 38 of the *Canada Evidence Act*, X’s likelihood of obtaining it would be poor. Section 38 might permit an enforceable privilege claim if disclosure would be injurious to international relations, national defence or national security, given the nature of information caught by the *SoCIS*. This could be problematic because it has the potential to frustrate an accused’s ability to make full answer and defence, and furthermore, for counsel to vigorously defend X.

Contrarily, the issue of notice might jeopardize the integrity of a national security investigation. For example, where privilege is claimed, notice to the subject may not be possible. This quandary may call for a more nuanced, case-specific notice regime with application that is contingent on the factual basis of the case.

Irrespective of the privilege issue, it would be difficult to formulate a defence without knowledge of the information originally disclosed under the *SoCIS*. Earlier, I discussed the notice requirement under the wiretap scheme in Part VI of the *Criminal Code*. In *Tse*, the notice requirement was critical to determining the constitutionality of the scheme. The Court ruled that a notice requirement would not frustrate the wiretap framework. Without it, the scheme was not minimally impairing. By parity of reasoning, the objectives of the *SoCIS* could be maintained with a notice requirement. While one might argue that a notice requirement would compromise a national security investigation, that suggestion is a slippery slope fallacy. Investigators resort to the wiretap scheme in the *Criminal Code* for major crimes with similar public safety implications.

---

240 R.S.C., 1985, c C-5 at ss 38 and 38.02(1). Section 38.01(1) reads: “Every participant who, in connection with a proceeding, is required to disclose, or expects to disclose or cause the disclosure of, information that the participant believes is sensitive information or potentially injurious information shall, as soon as possible, notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of the proceeding.”

241 Supra note 114.

242 I owe this idea to my supervisor, Kent Roach, who flagged it during the editing process.
as those involving national security. Sometimes the jeopardy faced by a subject is greater in a national security investigation. Thus, the absence of a notice requirement is not minimally impairing.

Secondly, the absence of caveats on information-sharing is not minimally impairing. While the purposes and principles in the *SoCIS* note that “respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing”, it does not specify any caveats. Instead, it authorizes Cabinet to create regulations that might impact the disclosure of information. Professors Roach and Forcse explain that this is particularly problematic because, when regulations are left in the hands of the executive, “the public will not know what the state is doing unless and until a scandal like that which engulfed Maher Arar arises.” These sentiments are echoed in *Wakeling’s* dissent, wherein Karakatsanis J. observed that “[t]he torture of Maher Arar in Syria provides a particularly chilling example of the dangers of unconditional information sharing.” As such, since the *SoCIS* does not necessarily prohibit future disclosures, domestically or abroad, the risk that inaccurate, untested, and unverifiable information can be disclosed is a live issue. The constitutionality of the legislation should not be saved by the potential that caveats may be imposed by regulation. Thus, the absence of caveats is not minimally impairing.

Thirdly, the “relevance” threshold for disclosure is arguably the least minimally impairing. A broad range of stakeholders and academics, including the Privacy Commissioner of Canada, who testified at the committee stage of the *SoCIS*, expressed that this threshold is exceptionally low, opening the door to a floodgate of information. As expressed earlier, some of the same critics recommend that the standard be changed to “necessity”, making disclosure “needed”, rather than “having a sufficient bearing on.”

---

243 *False Security*, supra note 25 at p 150.
244 *Wakeling*, supra note 79 at para 104 (per Karakatsanis J. dissenting).
246 *Righting Security*, supra note 20 at p 23.
Interpretation of the “relevance” threshold will inevitably attract different opinions within government circles. Recall that the disclosing institution is responsible for determining relevance. Several institutions do not have the knowledge or training to discern whether a piece of information is relevant to the jurisdiction or responsibilities of the receiving institutions. The Green Paper explains that the disclosing institution “may need discussions with the potential recipient to see if the information relates to the national security responsibilities of the recipient.” It is not clear how X’s privacy can be protected in the course of these “discussions.” Inevitably, persons relaying information would have to reveal the nature of the information for the recipient to understand whether it is relevant to their responsibilities. In that sense, seeking an advisory opinion on whether the relevance threshold is met suggests that more than one person within the government will dabble with the information.

Moreover, as detailed above, officials will not be ad idem on the level of imminence required for the disclosure to constitute a threat. Whether an impending, or present activity will meet the threshold for disclosure is not made clear by the legislative language of the SoCIS. At the committee stage of the bill, one policy analyst from the department of public safety explained that “information must actually undermine the sovereignty, security or territorial integrity of Canada.” However, this is not made clear in the Act, nor can we determine whether the Public Safety Deskbook clarifies this issue. Therefore, the scope of activity that might be captured will include a hodge-podge of personal information incidental to a so-called “threat.” That the Act does not delineate the imminence requirement does not make it minimally impairing.

Having regard for these areas, the measures of the SoCIS do not minimally impair the right to be free from unreasonable search and seizure. The framework is not within a reasonable range of outcomes, opting for a wide sweep of information-sharing, rather than a principled one. A recent report on national security tabled in the House of Commons by the Standing Committee on Public Safety and National Security supports the position that alternative information-sharing schemes are available. For example, the committee suggested, among many things, a narrowed list of activities subject to information sharing, a revised definition of “activities that undermine

---

the security of Canada”, and a dual threshold requiring relevance for the disclosing institution and one of necessity and proportionality for the receiving institution. The objectives of the SoCIS could have been achieved if the government carefully tailored the measures in the ways described above to reduce the adverse effects on the right to privacy.

(iv) Overall Proportionality: Salutary versus Deleterious Effects

The final prong of the proportionality assessment balances the harms of the law with the benefits of its objective. At issue is whether the benefits of the legislation are worth the cost of the impugned limitation. Aharon Barak explains that a proportionality assessment of this nature requires us to place colliding interests side by side and balance them according to their weight. We must consider the degree to which the measures trench upon the central principles of a free and democratic society. Even if I am incorrect about the minimal impairment analysis, the SoCIS must also pass this third and final proportionality assessment to be justified. In this section, I detail the deleterious effects first, and conclude by balancing them against the salutary effects of the Act.

The sheer magnitude of personal information that will be captured by the SoCIS is the most patent deleterious effect. Given that the “information” is not defined, it will inevitably provide institutions with discretion to capture a comprehensive spectrum of intimate details about a person, which may be used to generate metadata, and in turn, high level predictive analysis. In some cases, data will capture innocent people. All federal institutions will be engaged in this process, rendering the free exchange of this information accessible by several public servants, including but not limited to those who identify the data, analyze it, receive it, and then rely on it for investigatory purposes. Understood in this way, the SoCIS amplifies surveillance capabilities, developing an environment no different than the dystopias envisioned by George Orwell in

\[249\text{ See recommendations 22, 23 and 26 of the 2017 Report.}\]
\[250\text{ Patrick Monahan, Constitutional Law, 3d ed (Toronto: Irwin Law, 2006) at p 414.}\]
\[251\text{ Hutterian Brethren, supra note 243 at para 73.}\]
\[252\text{ Ibid at para 76.}\]
\[254\text{ Oakes, supra note 209 at para 71.}\]
1984,\textsuperscript{255} or Franz Kafka in \textit{The Trial},\textsuperscript{256} in which national security trumps the right to live free from state intrusion.

As I explored above, information is now processed using programs that synthesize, classify, isolate and identify big data. CSIS’ reliance on the ODAC is an example of how bulk data can be centrally stored and analyzed. What is known about the ODAC is limited to the \textit{en bane} Federal Court decision of \textit{Re X}, supra. Regrettably, the decision was heavily redacted, simply revealing that the ODAC “exploits data banks” and “assumes numerous tasks.”\textsuperscript{257} However, as indicated earlier, technologies which store mass data are now capable of using algorithms to target information in a more specific way using words and phrases.\textsuperscript{258} The extent to which these types of measures will be used to store information disclosed under the \textit{SoCIS} is unknown, unpredictable, and disassociated from public scrutiny.

If information is not stored in intelligence service repositories like the ODAC, then it will likely be stored in police databases. For example, in 2016, an Access to Information request revealed that the RCMP compiled a list of 89 persons from the Idle No More and Mi’kmaq-led anti-shale gas demonstrations deemed to be threats.\textsuperscript{259} This was part and parcel of the RCMP’s decision to designate indigenous demonstrations as “National Tactical Intelligence Priorities.”\textsuperscript{260} Protester files included “individual’s name, photograph, alias, date of birth, height weight, phone number, email, address, affiliations, vehicles, history of demonstrations, ability to move across the country and “category of protester”” and are stored in systems accessible to the RCMP and other law enforcement agencies.\textsuperscript{261} Under the \textit{SoCIS}, information about these persons could easily be

\begin{itemize}
\item \textsuperscript{257}\textit{Re X}, supra note 75 at para 37.
\item \textsuperscript{258}CBC News, supra note 73. See also House of Commons, Standing Committee on Public Safety and National Security Evidence, 41st Parl, 2nd Sess, No 56, (23 March 2015) at 1915 (Professor Garth Davies, Associate Professor, Simon Fraser University) and Chris Strohm, “Predicting Terrorism from Big Data Challenges U.S. Intelligence” \textit{Bloomberg Online} (13 October 2016): online, Bloomberg <https://www.bloomberg.com/news/articles/2016-10-13/predicting-terrorism-from-big-data-challenges-u-s-intelligence>.
\item \textsuperscript{260}Ibid.
\item \textsuperscript{261}Ibid.
\end{itemize}
shared with CSIS without a warrant because it is deemed violent, profiling dissenters based on their affiliated causes and culture.

While the definition of “activities that undermines the security of Canada” in section 2 excludes “advocacy, protest, dissent and artistic expression”, this will likely include activities labelled “violent.” The deleterious effect is that individuals will likely be profiled depending on their associations, which can be detrimental to visible minority communities. This was the case with Nurredin, Almalki and Elmaati, whose religious and cultural affiliations raised suspicion with the intelligence community after 9/11. The danger with this type of profiling is that it places the power in the hands of law enforcement to label a protest, group of people, or event as a “threat to national security” or a “danger to the public.” It does not foreclose the possibility that the biographical core of information of persons involved in protests or larger cultural communities with known political views, will be shared. This type of profiling will undoubtedly encroach on freedom of speech and association, in addition to the privacy interests already discussed.

Relatedly, the breadth of section 2 engenders a range of deleterious effects. It downloads the responsibility to inexperienced public servants to determine what constitutes an “activity” that undermines the security of Canada. In practice, this section will not apply uniformly across government agencies and departments, resulting in a hodge-podge of interpretations. Since section 2 steers the interpretation of the disclosure provisions under sections 5 and 6, it unduly complicates the regimes even further. Where information is improperly captured by section 2, disclosed, and used to spearhead an investigation, the evidence deriving from such investigations cannot simply be cast aside. In other words, once the damage is done, it cannot be reversed.

Review and oversight of this type of discretion will be limited to only three agencies – the RCMP, CSIS and CSEC. Some institutions are accountable to their respective Ministers, who typically report annually to the House of Commons. Others have no statutory reporting requirements. This means that institutions will, for the most part, be left to their own devices to ensure that they are reporting accurate and reliable data. The public will be unaware of whether the SoCIS is interpreted and applied in a manner that is not overbroad. Without reporting mechanisms, review or oversight agencies, it becomes nearly impossible to ascertain how much information is shared, with whom, and for what purpose.
To the contrary, the SoCIS also has salutary effects. Firstly, it enhances the rapidity with which information will be exchanged among law enforcement and intelligence agencies, which will facilitate the disruption of activities that undermine the security of Canada. The case of Aaron Driver is one example of how this might work. After the FBI informed the RCMP about a planned attack on an urban centre within 72 hours, Mr. Driver was intercepted by the RCMP at which point he detonated a bomb in the backseat of a cab.²⁶² This disruption is the kind that the SoCIS contemplates, and which can protect communities from harm.

Secondly, and as previously expressed, the Act fills a legislative gap in the national security domain by providing an authority for disclosure. While its interaction with other acts is not entirely made clear, the breadth of information sharing powers are so significant that they may alleviate doubt about whether information can be shared. This is in keeping with the legislative objective, which responds to information silos that could adversely affect the early detection of activities that undermine the security of Canada.

Despite these points, the deleterious effects far outweigh the salutary ones because they impinge on human dignity and autonomy to such a great extent, both of which are Charter values. These infringements are so severe that they require safeguards, which are not contemplated by the SoCIS. It is important to weigh the deleterious effects of impugned legislation on the impact of Charter values. These values include “liberty, human dignity, quality, autonomy, and the enhancement of democracy.”²⁶³ Human dignity and autonomy are essential aspects of the societal values espoused by our Charter, supported by the rights guaranteed by sections 7 and 8 of the Charter. By enhancing the state’s ability to intrude upon the person through the collection of personal information, the SoCIS runs afoul of these Charter values. It places greater emphasis on the preservation of state security, sovereignty, and overall, the protection of the public. As we know from the Supreme Court of Canada, privacy is not an all or nothing concept.²⁶⁴ Even when we are required to disclose information to the state, we expect that “private information will

remain confidential to the persons to whom and restricted to the purposes for which it was divulged.’\textsuperscript{265} For the reasons identified, the \textit{SoCIS} cannot be justified in a free and democratic society, and should be declared of no force or effect.

**CONCLUSION**

At the outset of this thesis, I likened the enactment of the \textit{SoCIS} with the state of exception – one in which the constitutional order is suspended for the sake of protecting the security of a nation. The notion that there is “no liberty without security,”\textsuperscript{266} as expressed by the federal government when the \textit{SoCIS} was introduced, perpetuates this phenomenon. Put differently, the unfettered exchange of information, writ large, is not the only way to protect Canadians. While circumventing prior judicial authorization is an expedient way of facilitating the exchange of information, it is done at the expense of the autonomy of the individual and the right to live free from state intrusion. It embodies the state of exception that Carl Schmitt prudently warned against.

For the benefit of clarity, my argument is not intended to disparage the utility of information-sharing as a matter of national importance.\textsuperscript{267} Rather, I attempted to shed light on the framework of the \textit{SoCIS}, and its interpretation by reviewing its most contentious provisions. I explained why the legislative intent of the Act disregards the dangers of unencumbered information-sharing by drawing on the need for oversight, safeguards and more broadly, accountability to the public. In doing so, I highlighted that Canadian law does not permit the use of information collected for one regulatory purpose, for the benefit of a separate investigatory need. Against this backdrop, I explained why Canadians have a privacy interest in the information that will be exchanged under the \textit{SoCIS}, why the law is unreasonable, and infringes the right to be free from unreasonable search and seizure. Upon careful review, I argued that the infringement cannot be justified in a free and democratic society.

\textsuperscript{266} Blaney Second Reading, supra note 26.
\textsuperscript{267} Stanley Cohen, supra note 87 at p 354 speaks about information sharing as “a matter of national importance particularly given evolving threats, and the transnational nature of crime.”
A society is one that requires total information control on its people is not free and democratic. It is one in which the power imbalance between the state and the individual grows, creating a permanent state of distrust between the “watchers” and those “watched.” The state of exception is now the rule. The war on terror is a political construct - so too are the means chosen to “fight” it. Regrettably, the SoCIS is one of those means.

---

268 Law, Privacy and Surveillance, supra note 41. In this chapter, Michael Geist makes reference to the “watchers”, or the state. I adopt this concept and use “watched” to describe those surveilled by the state – i.e. the citizenry.
BIBLIOGRAPHY

LEGISLATION

Anti-terrorism Act, 2015, SC 2015, c 20


Canada Evidence Act, R.S.C., 1985, c C-5

Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23

Criminal Code, R.S.C., 1985, c. C-46

Privacy Act, RSC, 1985, c P-21

Security of Canada Information Sharing Act, SC 2015, c 20

JURISPRUDENCE

Edwards v Canada (Attorney General), [1930] AC 124 (JCPC)

Charkaoui v Canada, 2008 SCC 38, [2008] 2 SCR 326


Hunter v Southam, [1984] 2 SCR 145 (SCC)

Hutterian Brethren of Wilson Colony v Alberta, 2009 SCC 37, [2009] 2 SCR 567


McKinlay Transport Ltd., [1990] 1 SCR 627 (SCC)

Milton v The Queen (1985), 16 CRR 215 (BC Co Ct)

Re X, 2016 FC 1105

R v Big M Drug Mart, [1985] 1 SCR 295

R v Caslake, [1998] 1 SCR 51 (SCC)

R v Colarusso, [1994] 1 SCR 20 (SCC)


R v Collins, [1987] 1 SCR 265 (SCC)

R v Dyment, [1988] 2 SCR 417 (SCC)


R v Jarvis, 2002 SCC 73, [2002] 3 SCR 757

R v Law, 2002 SCC 10, [2002] 1 SCR 227

R v Mills, [1999] 3 SCR 668 (SCC)

R v Morgentaler, [1993] 3 SCR 463

R v Oakes, [1986] 1 SCR 103

R v O’Connor, [1995] 4 SCR 411 (SCC)

R v Plant, [1993] 3 SCR 281 (SCC)

R v Quesnelle, 2014 SCC 46, [2014] 2 SCR 390

R v Simmons, [1988] SCJ No 86 (SCC)

R v Spencer, 2014 SCC 43, [2014] 2 SCR 212


R v Tse, 2012 SCC 16, [2012] 1 SCR 531

R v Vu, 2013 SCC 60, [2013] 3 SCR 657

Katz v United States 389 US 347 (1967)
SECONDARY MATERIAL: MONOGRAPHS


Carl Schmitt, *Dictatorship: From the Beginning of the Modern Concept of Sovereignty to the Proletarian Class-Struggle*, 7th ed (Berlin: Duncker & Humblot, 2006)


SECONDARY MATERIAL: ARTICLES

Aharon Barak, “Proportional Effect: The Israeli Experience” (2007) 57 UTLJ 369


Klemens Kappel, “Epistemological Dimensions of Informational Privacy” (2013) 10(2) Episteme 179

Lisa Austin, “Information Sharing and the Reasonable Ambiguities of Section 8 of the Charter” (2007) 57 UTLJ 499


SECONDARY MATERIAL: GOVERNMENT DOCUMENTS AND REPORTS

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar: Factual Background, vol 1 (Ottawa: Public Works and Government Services, 2006)

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar: Factual Background, vol 2 (Ottawa: Public Works and Government Services, 2006)


Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, The Relationship Between Intelligence and the Challenges of Terrorism Prosecutions, vol 3 (Ottawa: Public Works and Government Services Canada, 2010)

CSIS, “Memorandum to the Director, Deputy Minister Meeting on National Security Information Sharing” (5 February 2014) CSIS ATIP request 117-2014-393

House of Commons Debates, 41st Parl, 2nd Sess, No 174 (18 February 2015) at 1535 (Hon. Steven Blaney)

House of Commons, Standing Committee on Public Safety and National Security, Anti-terrorism Act, 2015 (March 2015) at 1835 (Kent Roach) (Chair: Daryl Kramp)


House of Commons, Standing Committee on Public Safety and National Security Evidence, 41st Parl, 2nd Sess, No 62, (31 March 2015) at 0920 (Ms. Élise Renaud)


House of Commons, Standing Committee on Public Safety and National Security Evidence, 41st Parl, 2nd Sess, No 56, (23 March 2015) at 1915 (Professor Garth Davies, Associate Professor, Simon Fraser University

House of Commons Canada, Standing Committee on Public Safety and National Security, Review of the Findings and Recommendations Arising from the Iacobucci and O’Connor Inquiries: Third Report” (June 2009) (Chair: Garry Breitkreuz)
Internal Inquiry Into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Almaati and Muayyed Nureddin (Ottawa: Public Works and Government Services Canada, 2008)


**SECONDARY MATERIAL: MISCELLANEOUS**


