The *Security of Canada Information Sharing Act*: A mosaic reflecting *Charter* and privacy rights violations

Submitted by: Katie Degendorfer
Submitted to: Professor Errol Mendes
Submitted on: December 7, 2016
Submitted for: CML4101B

THE SECURITY OF CANADA INFORMATION SHARING ACT: A MOSAIC REFLECTING *CHARTER* AND PRIVACY RIGHTS VIOLATIONS

TABLE OF CONTENTS

INTRODUCTION

Robert Morrison, a retired Chief Superintendent RCMP officer,[1] explains that the *Security of Canada Information Sharing Act*[2] (*SCISA*) was developed with the intention of, "increas[ing] security for Canadians by supporting intelligence and information sharing within government and supporting provincial, territorial, and municipal agencies."[3] He further suggests that information sharing disclosed as a result of *SCISA* will be done in a manner consistent with the *Charter of Human Rights and Freedoms*[4] (*Charter*) and citizens privacy interests in order to "support information sharing initiatives nationally and internationally with the right information, to the right person, at the right time."[5] These sentiments are also laid out in the preamble of *SCISA;* however, *SCISA* has failed to meet each of these objectives. The information sharing *SCISA* enables has resulted in *Charter* violations (particularly Section 7) and a failure to meet the standard for the protection of privacy set out in the *Privacy Act*[6]. The sharing of information has been carried out in a manner that undermines those rights and freedoms that are central to Canadian "security"[7], and has provided *incorrect* information to the *wrong* people, endangering Canadian citizens' lives. One must only look to the examples of Maher Arar, Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nurredin to understand the negative repercussions a lack of accountability and responsibility in information sharing can yield. Given Canada's intelligence gathering and sharing initiatives as part of the Five Eyes (the information sharing between

[1] Mr. Robert Morrison also formed part of the Treasury Board Secretariat initiative for Intelligence Sharing Across Canada formerly known as Information Sharing Environment (ISE).
[2] SC 2015, c 20, s 2.
[3] *Senate of Canada for the Committee of National Defence*, 41st Parl, 2nd Sess, Part 3 (May 25, 2015) online: <www.cpac.ca/en/programs/in-committee-from-the-senate-of-canada/episodes/39827427/> (Mr. Robert Morrison providing evidence on Bill C-51).
[4] C QLR c C-12.
[5] *Supra* note 3.
[6] RSC 1985, c P-21.
[7] Security can be defined as something that secures, or a quality or state of being secure. Although the word "security" is being used by government officials to imply measures that are being taken to protect citizens, here I am also referring to security in its simplest sense. The quality of being free from danger, fear or anxiety which SCISA is actually preventing since individuals, particularly those mentioned above were instead of free from danger, fear or anxiety, directly placed in this position by the information sharing initiatives. See the definition of "Security" *Miriam Webster*, online: <www.merriam-webster.com/dictionary/security>.

Canada, the United States, Britain, Australia, and New Zealand) and the recent Presidential election in the United States, arguably, Canada should consider either curtailing the information sharing initiatives *SCISA* facilitates, or ensuring more oversight and review so that the government is held accountable, and Canadian citizens and their rights are better protected in the years to come. This paper will argue that *SCISA* as it currently exists is not able to effectively fulfill the imposing purpose that it set out for itself. In order to explore *SCISA,* the paper will be organized in the following manner: (i) defining what *SCISA* is, (ii) defining what *SCISA* can do, (iii) understanding how *SCISA* impacts *Charter* rights and privacy rights, (iv) understanding *SCISA* in the current political context and finally, (v) what changes should be advocated for *SCISA*.

WHAT IS THE *SECURITY OF CANADA INFORMATION SHARING ACT* (*SCISA*) REALLY ABOUT?

SCISA forms Part 1 of Bill C-51[8] known as the "Anti-terrorism Act, 2015". Former Prime Minister Stephen Harper provides context to understand the broad aim of Bill C-51 as providing measures to "meet evolving threats and keep us safe, by giving [police and security agencies] the authority to stop planned attacks, to allow them to share information, to get threats quickly off our streets, to criminalize the promotion of terrorism, and to prevent terrorists from travelling and recruiting others."[9] This statement sheds light on his "tough on crime" mandate and his conservative approach to dealing with security concerns. The purpose of this paper is to highlight specifically how *SCISA*, similar to the broader Bill C-51, fails to effectively protect Canadians or balance the security and freedom of citizens.

SCISA seeks to "encourage and facilitate information sharing between government of Canada institutions in order to protect Canada against activities that undermine the security of

[8] *Supra* note 2.
[9] "Stephen Harper stresses importance of Anti-Terrorism Act during Montreal visit", *CBC News*, (21 May 2015), online: <www.cbc.ca/news/canada/montreal/stephen-harper-stresses-importance-of-anti-terrorism-act-during-montreal-visit-1.3083083>.

Canada".[10] *SCISA* was drafted to address overarching security issues[11] born from terrorist activities such as the Air India Bombing in 1985, and as a response to the "terrorist"[12] concerns that Martin Couture-Rouleau and Michael Zehaf-Bibeau presented in 2014. The concerns that were highlighted post-Air India was that information contained by various government department/agencies was not appropriately shared between them, and if it was shared this could have potentially mitigated the likelihood of an attack.[13] As such *SCISA* specifically, was a reaction to the "siloed" nature of information sharing.[14] To contextualize, it is helpful to return to Mr. Morrison's evidence presented to the National Defence Committee as it encapsulates the driving force behind the implementation of *SCISA*:

> For an example we might have an oil refinery, the company reports that there was a hole cut in the fence around the perimeter; that alone really is that a really big issue? A municipality next door to the oil refinery, reports that overnight a laundry and dry-cleaning facility had a break in and 40 uniforms were stolen that belonged to that oil refinery. The next municipality over reported that there was a large theft of fertilizer; that on its own doesn't mean anything. Add to that, there was an intelligence agency that had information from one of their sources that there was going to be some action taken on

[10] *Supra* note 2, preamble.
[11] Craig Forcese & Kent Roach, "Bill C-51: the Good, the Bad…and the Truly Ugly", *The Walrus*, (13 Feb 2015), online: <www.thewalrus.ca/bill-c-51-the-good-the-bad-and-the-truly-ugly/>.
[12] The term terrorist is in quotes here because terrorists act can be defined as: "(a) appear[ing] in the form of serious crimes against individual or social values (attacks upon the life or the physical integrity of persons, kidnappings, possession of weapons and explosives, destruction of public facilities, transport systems, etc.). (b) They often aim at specific symbolic targets, but they hit 'ordinary' targets as well, whenever terrorists want to draw attention to their action or to compel a government or an international organization to perform a certain act. (c) The crimes committed are always planned by groups that match the profile of a 'criminal organization', i.e. a group of more than two members, instituted over a period of time, built up around a central …distribution of roles, manoeuvring international links, well-trained members and equipment in order to carry out its criminal activities. (d) All terrorist groups use violence for political ends, aiming at overthrowing or destabilizing an existing socio-political system. (See: Elizabeth Symeonidou-Kastanidou, "Defining Terrorism" (2004) 12:1 European J of Crime, Criminal L & Criminal Justice 14-35 at 21 [footnotes omitted].) Based on the limited information that is public knowledge surrounding the incidents committed by Martin Couture-Rouleau and Michael Zehaf-Bibeau I am hesitant to label them as "terrorists" rather than criminals as it is unclear if they would meet this categorization. I am also hesitant to over-label when this creates issues and a type of fear mongering that arguably preceded Bill C-51.
[13] See Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Toronto, ON: Irwin, 2015) at 139 [*False Security*] speaking about Justice John Major: "there was enough information in the hands of various Canadian authorities to make it inexcusable that the system was unable to process that information correctly and ensure that there were adequate security measures in place to deal with the threat".
[14] The term siloed is often used to describe the nature of information sharing throughout these discussions. See for example, *False Security*, *supra* note 13 at 140.

> the oil refinery in Northern Alberta. If we look at all of those independently it really doesn't mean much, but when you start putting the pieces together it means a lot.[15]

This statement is key to understanding the driving force behind *SCISA*: the hope that by overcoming the siloed nature of information sharing that previously existed, relevant pieces of information would be examined and pieced together in time to prevent a serious "action". Conscious of the use of language in legislation and in statements by officials, the word "action" is no accident. This language is taken directly from Mr. Morrison and highlights that *SCISA* is much broader than referring to "terrorist activities". Rather, it is concerned with <u>any</u> action that may be taken and affect the security of Canada. Moreover, the examples to which Mr. Morrison refers are only effectively linked when there are no other explanations for these activities. In other words, there could be perfectly reasonable explanations for each of these individual concerns that in no way link them together. There could be petty thefts occurring in the area, youths seeking to protest the oil refinery, a whole myriad of reasonable and lawful explanations that in no way undermine the security of Canada. These tenuous linkages that information sharing under *SCISA* promote is likely to produce vulnerabilities, such as *Charter* and privacy rights violations; the assumption is that amassing a vast amount of data and collating the pieces together will yield prevention rather than missteps and misinformation. In reality the language in *SCISA* is overbroad and functionally works to suggest that the violations of privacy and *Charter* rights are the cost of protection. Rather than this being the case, there must either be limitations put in place, for example changing the definition of what is considered to "undermine" the security of Canada, or more effective accountability mechanism – such as oversight, review, and training so that employees involved in the sharing of information are held accountable.

[15] *Supra* note 3 [emphasis added on "action"].

WHAT DOES *SCISA* ACTUALLY DO?

SCISA has broadened the scope of security law in Canada and has placed a significant amount of power and trust in the government employees that make up the various departments specified in Schedule 3 of *SCISA*.[16] Paul Champ, on behalf of the International Civil Liberties Monitoring Group, in evidence presented to the Standing Committee on Public Safety and National Security points to two features of *SCISA*, which are unique amongst legislation pertaining to national security. First, "[an] expanded definition of the security of Canada […] that is unprecedented in our legislation"[17] Here Mr. Champ is referring to the language in Section 2 of *SCISA* which refers to, "activity that undermines the security of Canada".[18] This is, a relatively expansive step from the language that is used in the *Canadian Security Intelligence Service Act* (*CSIS Act*)[19], which refers to "threats to the security of Canada".[20] The difference may seem small at first blush but bears implications. As a report from the Canadian Bar Association points out, the word "undermine" is not defined in *SCISA*, "leaving open a range of actions that may trigger information sharing powers."[21] Moreover, an activity that *undermines* the security of Canada can be much broader than the narrow *threats* to the security of Canada. "Undermine" by definition can include that which weakens, while "threat" implies likely damage

[16] These government institutions include the 17 listed in Schedule 3 of *SCISA*, *supra* note 2: Canada Border Services Agency, Canada Revenue Agency, Canadian Armed Forces, Canadian Food Inspection Agency, Canadian Nuclear Safety Commission, Canadian Security Intelligence Service, Communications Security Establishment, Department of Citizenship and Immigration, Department of Finance Department of Foreign Affairs, Trade and Development, Department of Health, Department of National Defence, Department of Public Safety and Emergency Preparedness, Department of Transport, Financial Transactions and Reports Analysis Centre of Canada, Public Health Agency of Canada, Royal Canadian Mounted Police.

[17] *House of Commons, Standing Committee on Public Safety and National Security on the Anti-Terrorism Act, 2015,* 41st Parl, 2nd Sess, No 54 (March 12, 2015), online: <parlvu.parl.gc.ca/XRender/en/PowerBrowser/PowerBrowserV2/20150312/-1/14243?globalstreamId=20&useragent=Mozilla/5.0%20(Macintosh;%20Intel%20Mac%20OS%20X%2010_10_5)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Chrome/54.0.2840.71%20Safari/537.36> (Paul Champ).

[18] *Supra* note 2 [emphasis added].

[19] RSC 1985, c C-23.

[20] *Ibid*, s 2 [emphasis added].

[21] Submission of the Canadian Bar Association, "Bill C-51: Anti-Terrorism Act, 2015 – Executive Summary" *Canadian Bar Association* (March 2015) online: <www.iclmg.ca/wp-content/uploads/sites/37/2015/03/15-15-eng-Executive-Summary.pdf>.

or danger - a higher threshold to meet. Furthermore the term "activity" which proceeds "undermines the security of Canada" implies again that the definition is broader than "threats". Arguably, the fact that the government modified the previous definition and used this more expansive language implies that *SCISA* is to be used for more than terrorist threats and may apply to activities more generally, which attempt to "weaken" the security of Canada. This is supported by the fact that "interference with critical infrastructure" is included under the named activities,[22] an activity that may not impact Canadian national security, [23] but may apply, particularly in the year ahead, to protests.[24]

The second feature of *SCISA* Paul Champ notes as being unique is the, "dropping [of] the walls around privacy across government and […] giv[ing] a mandate to government officials across all departments to basically spy on Canadians."[25] This is highly problematic as the bill allows 17 government institutions, representing over 100+ agencies[26] to share information. Although *SCISA* has some "safeguards" in place to attempt to control the disclosure of information (see Section 5) in effect, the reality is those departments, agencies, and subsequently the employees that work there, untrained in the art of intelligence surveillance, will have the ability to share information. As Paul Champ goes onto describe, "this bill […] is turning all government employees into spies and it is going to facilitate the creation of secret files on Canadians because someone feels that a persons' lifestyle or opinions or travels are suspicious."[27] Non-specialized government employees piece together information creating a

[22] *Supra* note 2 at s 2(f).
[23] *Supra* note 21.
[24] Here I am particularly interested in the pipeline. See for example: Jenny Uechi, "Trudeau's pipeline approvals spark protests across Canada", *National Observer* (30 November 2016), online: <www.nationalobserver.com/2016/11/30/news/trudeaus-pipeline-approvals-spark-protests-across-canada>; Catharine Tunney, "Jim Car says military comments not a threat to pipeline protesters", *CBC News* (2 December 2016), online: <www.cbc.ca/news/politics/jim-carr-protests-pipeline-military-1.3878258>.
[25] *Supra* note 17.
[26] Michael Vonn, "4) The Security of Canada Information Sharing Act" (21 October 2016), *BCCLA* (Blog), online: <www.bccla.org/2016/10/security-canada-information-sharing-act/>.
[27] *Supra* note 17.

"mosaic"[28] that can then be used to support finding of suspected activities that undermine the security of Canada. *SCISA* aims to ensure that all institutions share information that "could be important for national security institutions".[29] This is even the case for institutions that "do not have a national security mandate…but must be able to disclose that information to institutions that have a mandate to act on it."[30] While this may be a legitimate concern: if the institution does not have a national security mandate and the employees are not trained for screening information that may concern national security, how can this information be vetted to ensure its importance? The answer is, as it currently stands – it cannot.

SCISA YIELDS VIOLATIONS OF CANADIAN CITIZENS *CHARTER* & PRIVACY RIGHTS **

The virtually unprecedented scale of information sharing that is already occurring as a result of the technological evolution as well as the "big-data[31] propelled information sharing"[32] that *SCISA* permits yields negative consequences including *Charter* and privacy rights violations. While the *Charter* violations may be more obvious on their face, privacy rights violations can effectively be occurring at an unprecedented level while citizens do not realize it is occurring.[33] Although Section 8 of the *Charter* protects against unreasonable search and seizure, the *Privacy Act*

[28] For more information about the "mosaic of information", "mosaic effect" or "mosaic theory" see for example: *False Security*, *supra* note 13 at 139; Yavar Hameed & Jeffrey Monaghan, "Accessing Dirty Data: Methodological Strategies for Social Problems Research" in Mike Larsen & Kevin Walby (eds.) *Brokering Access: Power, Politics, and Freedom of Information Process in Canada* (British Columbia: UBC Press, 2012); Craig Forcese & Kent Roach, "Stumbling Toward Total Information Awareness: The Security of Canada Information Sharing Act" (2015) 12:7 Canadian Privacy L Rev 66-76 online: <www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2622703> [*Stumbling Toward*]; Craig Forcese, "Many Shades of Secrecy: Challenges and Conundrums In the World of Canadian National Security Secrecy" (12 November 2016), *National Security Law: Canadian Practices in International Perspective* (blog) online: <www.craigforcese.squarespace.com/national-security-law-blog/2016/11/12/many-shades-of-secrecy-challenges-and-conundrums-in-the-worl.html>.

[29] Government of Canada, "Our Security, Our Rights: National Security Green Paper, 2016" Public Safety Canada, online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx#s5>.

[30] *Ibid*.

[31] Lisa M Austin et al., "How C-51 Undermines Privacy", *National Post*, (30 March 2015), online: <www.news.nationalpost.com/full-comment/how-c-51-undermines-privacy>.

[32] "Bill C-51: An Attack on Privacy" *FIPA* (20 April 2015), online: <www.fipa.bc.ca/bulletin-c-51/>.

[33] Tonda Maccharles, "CSIS official admits reporters may have been under surveillance in the past", *Toronto Star*, (28 November 2016) online: <www.thestar.com/news/canada/2016/11/28/csis-official-admits-reporters-may-have-been-under-surveillance-in-the-past.html>.

goes further to include positive rights and obligations to "protect the privacy of individuals with respect to personal information about themselves held by a government institution and […] provides individuals with a right of access to that information."[34] The implication of having the *Charter* and *Privacy Act* as safeguards to other laws and legislation in Canada is to balance the individual and collective interests in Canada. However, Section 8 of the *Privacy Act* provides for a vast number of exemptions and is subject to any other Act of Parliament, which may permit the disclosure of information. Since *SCISA* seeks to provide for the disclosure of information it effectively trumps any protections that the *Privacy Act* sets out.[35]

Although laws contain features to restrain government over-action, the broad terms that are implemented in *SCISA* make it easier to circumvent those laws under the pretense of protecting national security at the expense of *Charter* and privacy violations. The government is not taking the steps it has stated it would and is keeping the public in the dark about many realities, for example the amount of information that is being shared, or how this sharing is being reviewed (if at all). In the preamble to *SCISA* the act recognizes that, "there is no more fundamental role for a government than protecting its country and its people".[36] The wording of the act lends itself to suggest that *SCISA* protects citizens' interests. However, the price of national security should not be violations of peoples' rights. Professors Forcese and Roach on privacy suggest that, "law stands…as the remaining bulwark against the end of privacy".[37] However, when provisions of *SCISA* are broad and unclear, it is unlikely that the protections will function as they should. The Department of Public Safety in the *Green Paper* attempts to recognize and address the issue by suggesting that, "[i]nformation sharing under […] SCISA may be reviewed like other instances of government information sharing. In particular,

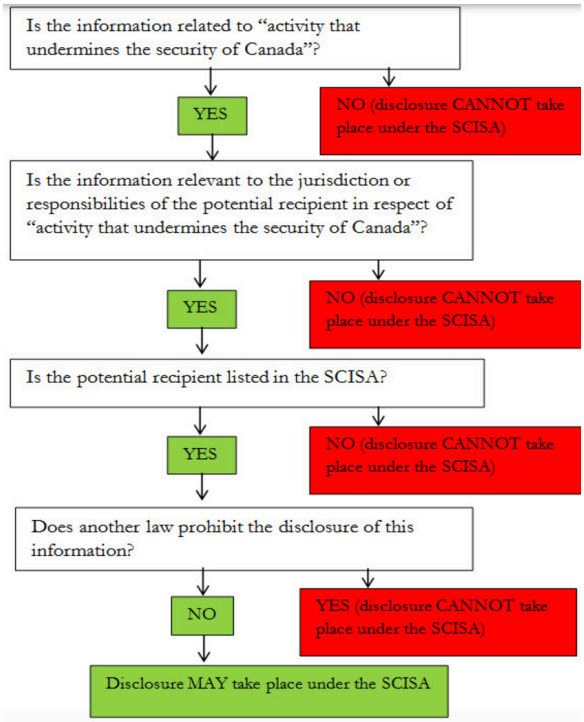
[34] *Supra* note 6, s 2.
[35] See also, Lisa M Austin, Benjamin J Goold, Avner Levin and Andrea Slane, "How C-51 Undermines Privacy" The National Post (30 March 2015), online: < http://news.nationalpost.com/full-comment/how-c-51-undermines-privacy>.
[36] *Supra* note 2, preamble.
[37] *Stumbling Toward*, *supra* note 28 at 66.

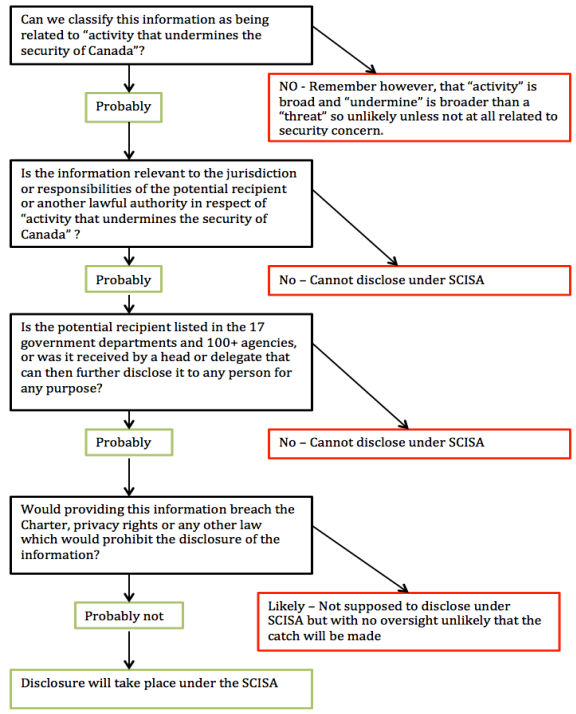
the *Privacy Act* allows the Privacy Commissioner of Canada to review institutions' handling of personal information and to hold institutions accountable by releasing public reports."[38] However, in practice, *SCISA* is not like other instances of government information sharing due to its broad definitions and applicability. Moreover, the release of public reports, which are supposed to function as an accountability mechanism, do not happen regularly.[39]

The disclosure of information pursuant to section 5 of *SCISA*, is hypothetically set to restrain the provision of information sharing on the part of the government, "subject to any provision of any other Act or Parliament…that prohibits or restricts the disclosure of information".[40] However, as Professors Forcese and Roach point out, based on "restrictions on information sharing [being] … riddled with exceptions" the section may not be as restraining as the government suggests.[41] Furthermore, the inclusion of the 17 institutions and 100+ agencies that share information will increase the quantity and flow, which without adequate accountability mechanisms, will likely not be properly overseen to ensure compliance with somewhat vague disclosure requirements.[42] The Department of Public Safety drew up a chart in the *Green Paper*, which serves to highlight the safeguards that are in place for determining when information can be disclosed under *SCISA*, but in reality the decision to disclose can "circumvent" the stages in place. See for example the original chart[43] provided below on the left, implemented in the *Green Paper* which suggests all of the stages that must be passed, with the key word at the end that disclosure "may" take place under SCISA, highlighting that at the end the option is discretionary. However, the reality is that the chart looks much more like the one below on the right.

---

[38] *Supra* note 29.
[39] Alex Boutilier, "Canada's privacy law 'Ill-suited' to 21st century, watchdog warns Trudeau", *Toronto Star*, (24 June 2016), online: <www.thestar.com/news/canada/2016/06/24/canadas-privacy-law-ill-suited-to-21st-century-watchdog-warns-trudeau.html>; Michael Geist, "Canada's Privacy Failure: My Appearance Before the Standing Committee on Access to Information, Privacy and Ethics" (6 October 2016) *Michael Geist* (blog), online: <www.michaelgeist.ca/2016/10/canadas-privacy-failure-my-appearance-before-the-standing-committee-on-access-to-information-privacy-ethics/>.
[40] *Supra* note 2, s 5(1).
[41] *Stumbling Toward*, *supra* note 28 at 66.
[42] *Ibid*.
[43] *Supra* note 29.


Is the information related to "activity that undermines the security of Canada"?
YES
NO (disclosure CANNOT take place under the SCISA)
Is the information relevant to the jurisdiction or responsibilities of the potential recipient in respect of "activity that undermines the security of Canada"?
YES
NO (disclosure CANNOT take place under the SCISA)
Is the potential recipient listed in the SCISA?
YES
NO (disclosure CANNOT take place under the SCISA)
Does another law prohibit the disclosure of this information?
NO
YES (disclosure CANNOT take place under the SCISA)
Disclosure MAY take place under the SCISA


Can we classify this information as being related to "activity that undermines the security of Canada"?
Probably
NO - Remember however, that "activity" is broad and "undermine" is broader than a "threat" so unlikely unless not at all related to security concern.
Is the information relevant to the jurisdiction or responsibilities of the potential recipient or another lawful authority in respect of "activity that undermines the security of Canada" ?
Probably
No – Cannot disclose under SCISA
Is the potential recipient listed in the 17 government departments and 100+ agencies, or was it received by a head or delegate that can then further disclose it to any person for any purpose?
Probably
No – Cannot disclose under SCISA
Would providing this information breach the Charter, privacy rights or any other law which would prohibit the disclosure of the information?
Probably not
Likely – Not supposed to disclose under SCISA but with no oversight unlikely that the catch will be made
Disclosure will take place under the SCISA

The differences that this "re-imagined" chart seeks to highlight are: first, that the answers, "yes" and "no" do not necessarily work in this context given the fluid nature of the provisions in *SCISA*. These words have therefore been substituted with "probably" where appropriate to highlight that the provision of disclosure in certain circumstances is likely to occur given the low threshold of prevention and broad discretionary nature. Second, some of the categorizations highlight the nature of the language in the act being much more broad than it may first appear, as well as the scheduled list of government institutions, departments, and agencies being much more significant than simply those listed in the schedule. Third, as seen from previous examples, we know that disclosure has been and may in the future be provided in cases where the information is in breach of other laws if no changes are instituted – specifically *Charter* or privacy rights. The chart highlights that this is specifically linked to a lack of oversight, as there is no review mechanism currently in place that may effectively mitigate when violations may occur. Finally, this re-imagined chart points out the potential breadth and impact the disclosure of information can have; breadth in the sense that there is much information and many government departments and agencies implicated by the legislation, and impact because of the effect it can have on citizens' *Charter* and privacy rights given the information being collected and retained under the guise of "national security".

(I) *SCISA INFRINGES CHARTER RIGHTS*

The potential for *Charter* rights violations is significant, and represents one of the darkest clouds overshadowing the beneficial aims of *SCISA*. Rather then there being a restraint in the information that is disclosed to government institutions, accountability and oversight are mechanisms to ensure that the information that is shared amongst government institutions is done in a way that does not necessarily infringe on citizens' *Charter* rights. Significant *Charter* violations can be seen in the examples of Maher Arar, Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nurredin, which occurred prior to the enactment of *SCISA*, and prior to the

broadening of the terms that *SCISA* now embodies. This paper recognizes that these individuals' experiences represent extreme *Charter* violations, which may not always be the outcome of information sharing; however, careful consideration must be placed on whether it is acceptable to have a few (documented) cases of horrific and significant *Charter* violations. For some proponents, the suffering of a few is warranted for the protection of the many. However, this paper argues that the suffering of a few that *SCISA* may yield is unacceptable and furthermore does not effectively protect the many.

The *Charter* violations stemming from the detention and torture of Maher Arar, highlight that prior to SCISA and the expansion of the sharing of information there were issues with what was disclosed. Maher Arar was a Canadian citizen from Syria who ended up being detained in the US and subsequently deported to Syria where he was tortured for information under suspicion of being a terrorist. One *Charter* right that was demonstrably infringed was his Section 7 right to life, liberty, and security of the person, as he was imprisoned and subjected to torture for approximately one year. The disclosure of information contributed to the *Charter* violation(s) experienced by Mr. Arar, as incorrect information was obtained and passed along from Canadian authorities to the Americans, and then finally Syrians. This information was not adequately screened and is an example of how information sharing can go terribly wrong.

Professors Forcese and Roach use the phrase "Arar amnesia" to describe the reality that *SCISA* does nothing to "ensure the reliability and (for the most part) relevance of the information that is shared."[44] Although the Arar Commission recommended that, "[t[he RCMP should ensure that those involved in national security investigations are properly trained in the particular features of such investigations" there is no such effort that is being undertaken. Moreover, with even more responsibility upon non-RCMP government officials to engage in the

[44]Kent Roach & Craig Forcese, "Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience" (16 February 2015), *Antiterror Law* (blog), online: <www.ssrn.com/abstract=2565886>.

information sharing, the potential for further *Charter* violations and disclosure of incorrect or unrelated information contributes to building a mosaic of information against someone that should not exist.

Subsequently, the Iacobucci Inquiry examined the mistreatment of Abdullah Almalki[45], Ahmad Abou-Elmaati, and Muayyed Nurredin. In a statement prior to the report's release, Justice Iacobucci explained, "For the terrorist, the end justifies the means".[46] Here Justice Iacobucci is referring to the constraint on their rights and freedoms due to the illegal activity that terrorist suspects may be engaged in. He continues, "[a] democracy, however, must justify the means to any end – including, in this case, its response to terrorism."[47] As such, Justice Iacobucci highlights that although the national security concern is live and of significant importance, there a balance must be struck to ensure that the individual's [the alleged terror suspect] rights are protected. It is also important to understand that at the information gathering stage (which was the stage for Mr. Arar, Mr. Almalki, Mr. Abou-Elmaati, and Mr. Nurredin), these individuals are only *allegedly* involved in the said activity. They are being detained not convicted of any crime, which would then trigger potentially appropriate limits upon their *Charter* rights. Just as in Mr. Arar's case, in the case of these three Canadian citizens, the sharing of information contributed to their mistreatment while they were detained in Syria, or in Mr. Abou-Elmaati's case, Egypt. A conclusion from this inquiry was that "Canadian officials indirectly contributed to the maltreatment of these individuals in foreign custody when they shared

[45] Although please note that information pertaining to Abdullah Almalki is also discussed in some detail in the Arar Commission report provided that Mr. Arar's "link" to Al-Queda was supposedly made through his connected with Mr. Almalki. See the Honorable Justice Dennis O'Connor, *Report of the Events Relating to Maher Arar: Factual Background: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa, ON: Public Works and Government Servics Canada, 2006) online: <www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf> at 16.
[46] The Honorable Justice Frank Iacobucci, Commissioner, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Ottawa, ON: Public Works and Government Services Canada, 2008), online: <www.publicsafety.gc.ca/lbrr/archives/cn73612699-eng.pdf>.
[47] *Ibid*.

information about the detainees".[48] Again, there are no lessons learned as information was shared without adequate steps and efforts taken to ensure that the information was credible. Just like the "Arar amnesia" there seems to be a blatant disregard to putting in place effective mechanisms to prevent further *Charter* rights violations which may result from information sharing. This is a critical flaw that *SCISA* has perpetuated.

(II) *SCISA VIOLATES PRIVACY RIGHTS*

The Privacy Commissioner, Daniel Therrien, explains in his opening statement for the Standing Committee on Access to Information, Privacy and Ethics (ETHI), that *SCISA* "authorizes information to be shared where it is merely relevant to national security goals" and warns that "[s]etting such a low standard is a key reason why the risks to law abiding citizens are excessive."[49] The difference between relevant and necessary is highlighted in both Therrien's opening statement and the *Green Paper*, where the government explains at footnote 13, that, "[b]ecause national security information sharing often engages privacy rights, the SCISA requires that information be disclosed only if it is actually—and not potentially or possibly—*relevant* to the recipient's lawful responsibilities for activity that undermines the security of Canada."[50] Although the language in the *Green Paper* attempts to highlight the benefits of the word "relevant", in effect there will be much more information that will be applicable and covers a much broader scope than that information which *necessarily* implicates an activity that undermines the security of Canada. By applying this definition, the government suggests that the disclosure of information "satisfies the "lawful authority" exception under the *Privacy Act*."[51] The *Privacy Act* is supposed to protect information and ensure that the government cannot

[48] Craig Forcese & Kent Roach, *Sharing Information and lost lessons from the Maher Arar experience* (Ottawa, ON: Canadian Electronic Library, 2015) at 6.
[49] Daniel Therrien, "Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the study of the *Security of Canada Information Sharing Act (SCISA)*" (16 November 2016), *Office of the Privacy Commissioner of Canada*, online: <www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20161122/>.
[50] *Supra* note 29 at footnote 13.
[51] *Supra* note 29.

collect the information without the individual's knowledge and consent.[52] However, as Professors Forcese and Roach point out, the *Act* allows for some exceptions including when another Act may allow it, for the "disclosure [of] prosecutorial and lawful investigation purposes, for research purposes, and even for general purposes where the public interest outweighs any harm to privacy".[53] With all of these opportunities to evade obtaining an individual's consent, or informing individuals that the information is being collected, there are likely substantial privacy breaches that are occurring through *SCISA*.

Moreover, there is no indication in *SCISA* of how long information that has been shared will be retained for. That may suggest that if information is collected and shared between departments, it can be retained for a significant amount of time and used when other materials surface. Applying the mosaic model for piecing together information, this is particularly worrisome as the information may be irrelevant based on reasonable alternatives, but also out of context given the span of time between the pieces of information being collected and then collated together. Thinking back to the example provided by Mr. Morrison, it would be worrisome indeed if each of these occurrences took place weeks, or months apart; collating them as part of a larger mosaic would seem to make little sense. However, given that various departments and that there is an unspecified amount of time for retaining information, this may be a concerning reality. Given the current concerns that CSIS failed to inform the court about the collection and retention of sensitive data for the purpose of spying on journalists for years, the concern is all the more active and real.[54] As the *Green Paper* also seeks to further extend state surveillance

---

[52] *Supra* note 35 at s 5(2).
[53] *False Security*, *supra* note 13 at 151 [footnotes omitted].
[54] *Application by X for Warrants Pursuant To Sections 12 and 21 of the Canadian Security Intelligence Act, RSC 1985, C C-23 and in the Presence of the Attorney General and Amici and in the Matter of X Threat-Related Activities*, 2016 FC 1105, online: <cas-cdc-www02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20public%20judgment%20FINAL%20(ENG).pdf>. See also: Jim Bronskill, "CSIS broke law by keeping sensitive metadata Federal Court Rules", *CBC News* (3 November 2016), online: <www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472>; "Canadian judge blasts spy agency for illegally hoarding private data", *The Guardian* (4 November 2016), online: <www.theguardian.com/world/2016/nov/04/canadian-judge-blasts-spy-agency-for-illegally-hoarding-private-data>.

powers specifically in the areas of basic subscriber information, data retention and compelled passwords, [55] the firm stance in regards to this should be that it is ill-advised. Not only has CSIS recently been implicated in unprecedented and unfettered surveillance, but also the 2016 SIRC report indicated that there was bulk data collection of private information that was occurring outside of the "legal context".[56] With these lingering concerns, no further surveillance powers should be granted. In fact, the powers that are currently provided should be seriously restrained as it is clear that there are untrammelled privacy rights breaches occurring even amongst non-targeted citizens. Professor Geist, points out, "the Privacy Act is already out-dated and effectively neutered by the bill".[57] With this in mind, the question remains: should *SCISA* be provided so much power? The answer is inevitably, no. There should instead be mechanisms in place to mitigate the potential for mass privacy rights breaches so that personal information is protected.

SCISA IN AN AGE OF POLITICAL CHANGES: THE POTENTIAL FOR DISASTROUS REPERCUSSIONS

As a piece of Canadian legislation, *SCISA* does not govern information sharing with other countries. However, the gathering of information that *SCISA* promotes will inevitably have an impact on the intelligence sharing that makes up part of its international relationships within the Five Eyes and specifically the United States. Since international information sharing is important for our national security and will be sustained in the future, it is necessary that there be safeguards and an understanding of the potentially negative repercussions for over-zealous information sharing (think Maher Arar), and the subsequent *Charter* and/or privacy violations.

---

[55] This list is pulled from Michael Vonn, "Surveillance scandals break while government presses for more surveillance powers" (7 November 2016), *BCCLA* (blog), online: <www.bccla.org/2016/11/surveillance-scandals-breaking-government-presses-surveillance-powers/>.

[56] See, Michael Vonn, "4) Security of Canada Information Sharing Act" (21 October 2016) *BCCLA* (blog), online: <www.bccla.org/2016/10/security-canada-information-sharing-act/>; Pierre Blais (Chair)"Maintaining Momentum – 2015-2016 Report" *Security Intelligence Review Committee* (Ottawa, ON: Public Works and Government Services Canada, 2016) online: <www.sirc-csars.gc.ca/pdfs/ar_2015-2016-eng.pdf>.

[57] Michael Geist, "Why the Anti-Terrorism Bill is Really an Anti-Privacy Bill: Bill C-51's Evisceration of Privacy Protection" (12 March 2015) *Michael Geist* (blog), online: <www.michaelgeist.ca/2015/03/why-the-anti-terrorism-bill-is-really-an-anti-privacy-bill-bill-c-51s-evisceration-of-government-privacy/>.

Recently, there have been news reports suggesting that CSIS has been able to spy on Canadians in foreign prisons using the broader terminology in *SCISA*.[58] This is one example of how information sharing can be negatively implicated in the future. Moreover, with newly elected US President Trump and his statements about using, "waterboarding, torture and 'much stronger' techniques on terrorism suspects", [59] sharing information without appropriate accountability mechanisms – like improved oversight and review – could undoubtedly yield further human rights violations. As such, with changes occurring, the advice to the Canadian government should be to improve the system within the country so as to mitigate the risk of being implicated in negative situations in the future. With an over-zealous US President, there may be situations arising where it is important not to over-disclose in order to continue to ensure that our citizens have the right to abide by *Charter* and privacy rights.

WHAT IS NECESSARY: CURTAILING INFORMATION SHARING OR IMPROVED OVERSIGHT AND REVIEW MECHANISMS?

There must be some fundamental changes that are taken to improve the current state of *SCISA*. The current consultations occurring on national security[60] based on the *Green Paper* emphasize the potentially positive steps that the government is taking to hear what civil liberties groups, academics, students, and the general population have to say concerning amendments to be made to legislation. However, this paper posits that there are effectively two changes that could be made (although other possibilities include a combination of the two and nothing being changed). The first is curtailing information sharing to limit the scope of the information that is shared and potentially limiting the government institutions that can access and share the

[58] Jim Bronskill, "CSIS Using Bill C-51 to spy on Canadians in foreign prisons memo reveals", *The Toronto Star* (3 October 2016), online at: < https://www.thestar.com/news/canada/2016/10/03/csis-using-c-51-to-spy-on-canadians-in-foreign-prisons-memo-reveals.html>. See also: Dean Beeby, "CSIS locks horns with diplomats over anti-terror info sharing", *CBC News* (28 Jun 2016), online: <www.cbc.ca/news/politics/csis-spies-terrorists-isis-global-affairs-canada-rcmp-privacy-c51-1.3654861>.
[59] Tamara Keith, "On Waterboarding, A President Trump Could Face Resistance From Some Republicans", *NPR* (21 November 2016), online: <www.npr.org/2016/11/21/502871948/on-waterboarding-a-president-trump-could-face-resistance-from-some-republicans>.
[60] See for example: "Online Consultation on National Security", *Public Safety Canada* (2016), online: <www.publicsafety.gc.ca/cnt/cnslttns/ntnl-scrt/index-en.aspx>.

information. The second is improved oversight and review mechanisms with the view to yielding greater accountability and holding each of the institutions to a high standard.

(I) CURTAILING INFORMATION SHARING

Information sharing is something that in the current day and age is a reality. Provided that Canada relies so heavily on the information provided to us from the Five Eyes, abating information sharing completely will not happen, nor would it be advisable. Instead, curtailing information sharing is a plausible solution as there are some effective options, which would translate into improved rights protection for individuals while keeping in mind legitimate national security concerns. The changes that are recommended include the following:

1. *Return to the terminology that was used in the CSIS Act in regards to the "threat to national security" rather than "activities that undermine the security of Canada" from SCISA*

Replacing the new preamble and returning to the definition contained in CSIS would allow for a more narrow interpretation of when information can be shared and assist in mitigating some of the extraneous flow of information that the current terminology may yield.

2. *Mitigate and/or specify the agencies that end up being able to share information in the listed institutions*

By narrowing down the number of agencies that are involved, there may be improved control surrounding the government employees that are able to share information. This would also make it more challenging for the institutions to open up the number of agencies that may be able to share information.

3. *Be specific about the nature of disclosure of information so the information of individuals that are not suspected of terrorist activities cannot be so easily shared*

The provision here attempts to mitigate the privacy concerns that were discussed above while also balancing the disclosure of information that is potentially related to suspected terrorist activities.

Curtailing information sharing is a feasible option and would arguably mitigate some of the concerns that were raised by civil liberties groups. However, a potential issue will be the government's reluctance to redraft these portions of the legislation especially considering that the *Green Paper* indicates they are in fact trying to expand the scope of their information sharing powers.

(i) IMPROVED OVERSIGHT AND REVIEW

Improved oversight and review mechanisms are what most scholars are advocating for in the context of the entire Bill C-51. The goal, with an improved oversight mechanism, would be that there is less likelihood that the wrong information is being received by the wrong people as the information is being vetted. Daniel Therrien, expressed this concern and the need for oversight, since "most of the organizations that would receive and use more personal information under the legislation introduced today are not [subject to independent oversight of all of their activities]".[61] Considering that there are 17 institutions and 100+ agencies that will be able to share information under *SCISA*, implementing effective oversight committees in each of these institutions seems to make the most sense. Oversight would ensure that, for the most part, information that is being shared is useful and relates back to the fundamental purpose of the Act, which is to provide information that indicates an activity may undermine the security of Canada. Oversight of each individual agency seems far-fetched considering limitations of the budget and also the implementation of oversight bodies in each institution. However, as Daniel Therrien highlights, there would have to be a way to ensure that the oversight bodies are

[61] "Statement from the Privacy Commissioner of Canada following the tabling of Bill C-51" (30 January 2015), *Office of the Privacy Commissioner of Canada*, online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2015/s-d_150130/>.

educating and informing the agencies that are subsumed within their larger departments. The oversight could also ensure a bare minimum for educating employees about the type of information that is supposed to be shared.

Improvements in the review mechanisms would ensure that there is accountability and transparency for errors that were made along the way as information was being shared amongst government departments. With a mind to the reality of the vast number of agencies implicated by *SCISA*, there has been some debate about the best way to implement effective review. The first method is through a "super agency"[62] where there would be "independent review to the national security activities of all federal national security actors not currently subject to such review".[63] This idea was first discussed in the Arar Inquiry, however, as of yet has not been implemented. This may be because there are issues the drawbacks of a "super-SIRC" or super Security Intelligence Review Committee (SIRC), including that it may be unlikely for this body to effectively deal with all the agencies implicated under *SCISA*. Bill C-22 proposes a committee of parliamentarians, which would contribute to the review aspect of information sharing, as its mandate is to review:

> (a) the legislative, regulatory, policy, administrative and financial framework for national security and intelligence
> (b) any activity carried out by a department that relates to national security or intelligence unless the appropriate Minister determines that the review would be injurious to national security; and
> (c) any matter relating to national security or intelligence that a minister of the Crown refers to the Committee[64]

As such, Bill C-22 represents a significant step forward to ensuring that there are improvements made if there are issues that arise from information sharing. Although, it still remains to be seen how much information would be made available to the members of the committee of

---

[62] The Honourable Dennis O'Connor (Commissioner*), A New Review Mechanism for the RCMP's National Security Activities: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa, ON: Public Works and Government Services Canada, 2006) online: <http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf> at 560.
[63] *Ibid*.
[64] Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, 1st, 42 Parl, 2016, s 8 (second reading 04 November 2016).

parliamentarians while conducting their reviews and how all-encompassing their review would be, it would also put Canada on par with the other Five Eyes countries who all currently have Parliamentary review mechanisms.[65]

Whether the government chooses to curtail information sharing, improve oversight and review, or ideally both, there is much work that remains to be done to ensure that citizens *Charter* and privacy rights are not violated and that the information is being used for the more narrow purpose that *SCISA* intended – national security. Advocating for both seems like a far stretch but it would be an effective way to improve upon the issues that have already come up since Bill C-51 passed in 2015.

CONCLUSION: LOOKING BACK AND MOVING FORWARD

As it currently stands, *SCISA* fails to meet the appropriate standards that should exist for information sharing. Information sharing implicates a key balance between national security and individuals' rights. Although there are times when individuals' rights should be trumped in order to ensure nationwide protection, the current information sharing practices do not seem to relate solely to the purposes of ensuring national security. Rather, the breadth of the information that can be collected and shared, the number of institutions that are implicated, the lack of time restraints, the vagueness of other laws and regulations, all create the perfect storm for individuals' *Charter* and privacy rights to be taken advantage of. We have already seen the consequences of unfettered information sharing in the cases of Maher Arar, Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nurredin. If nothing is learned or applied from the O'Connor and Iacobucci Inquiries, it is at the country's own peril. Collating a mosaic of information in order to attempt to mitigate the likelihood of potential terrorist attacks may be one of the only methods that we can currently apply. While national security is a concern, there is too much emphasis and faith being placed on *SCISA* to help find the needle in the haystack.

[65] Ralph Goodale, "Bill C-22 is designed to protect Canadians rights and defend their security", *National Post* (3 October 2016), online: <www.news.nationalpost.com/full-comment/ralph-goodale-bill-c-22-is-designed-to-protect-canadians-rights-and-defend-their-security>.

There has to be improvements in information sharing so that the appropriate balance between privacy, *Charter* and security rights can be obtained and all Canadian citizens can truly feel secure.

WORKS CITED

Legislation

Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, 1st, 42 Parl, 2016, s 8 (second reading 04 November 2016).

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

Charter of Human Rights and Freedoms, C QLR c C-12.

Privacy Act, RSC 1985, c P-21.

Security of Canada Information Sharing Act, SC 2015, c 20, s 2.

Jurisprudence

Application by X for Warrants Pursuant To Sections 12 and 21 of the Canadian Security Intelligence Act, RSC 1985, C C-23 and in the Presence of the Attorney General and Amici and in the Matter of X Threat-Related Activities, 2016 FC 1105, online: <cas-cdc-www02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20public%20judgment%20FINAL%20(ENG).pdf>

Government Documents

Government of Canada, "Our Security, Our Rights: National Security Green Paper, 2016" *Public Safety Canada*, online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx#s5>.

The Honorable Justice Dennis O'Connor (Commissioner), *Report of the Events Relating to Maher Arar: Factual Background: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa, ON: Public Works and Government Servics Canada, 2006) online: <www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf>.

The Honourable Dennis O'Connor (Commissioner*), A New Review Mechanism for the RCMP's National Security Activities: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa, ON: Public Works and Government Services Canada, 2006) online: <http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf> at 560.

The Honorable Justice Frank Iacobucci (Commissioner), *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Ottawa, ON: Public Works and Government Services Canada, 2008), online: <www.publicsafety.gc.ca/lbrr/archives/cn73612699-eng.pdf>

House of Commons, Standing Committee on Public Safety and National Security on the Anti-Terrorism Act, 2015, 41st Parl, 2nd Sess, No 54 (March 12, 2015), (Paul Champ). online: <parlvu.parl.gc.ca/XRender/en/PowerBrowser/PowerBrowserV2/20150312/-1/14243?globalstreamId=20&useragent=Mozilla/5.0%20(Macintosh;%20Intel%20Mac%20OS%20X%2010_10_5)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Chrome/54.0.2840.71%20Safari/537.36>

Pierre Blais (Chair), “Maintaining Momentum – 2015-2016 Report” *Security Intelligence Review Committee* (Ottawa, ON: Public Works and Government Services Canada, 2016), online: <www.sirc-csars.gc.ca/pdfs/ar_2015-2016-eng.pdf>.
Senate of Canada for the Committee of National Defence, 41st Parl, 2nd Sess, Part 3 (May 25, 2015) online: <www.cpac.ca/en/programs/in-committee-from-the-senate-of-canada/episodes/39827427/>.

Secondary Materials: Blogs

Craig Forcese, “Many Shades of Secrecy: Challenges and Conundrums In the World of Canadian National Security Secrecy” (12 November 2016), *National Security Law: Canadian Practices in International Perspective* (blog) online: <www.craigforcese.squarespace.com/national-security-law-blog/2016/11/12/many-shades-of-secrecy-challenges-and-conundrums-in-the-worl.html>.

Kent Roach & Craig Forcese, “Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience” (16 February 2015), *Antiterror Law* (blog), online: <www.ssrn.com/abstract=2565886>.

Michael Geist, “Canada’s Privacy Failure: My Appearance Before the Standing Committee on Access to Information, Privacy and Ethics” (6 October 2016) *Michael Geist* (blog), online: <www.michaelgeist.ca/2016/10/canadas-privacy-failure-my-appearance-before-the-standing-committee-on-access-to-information-privacy-ethics/>.

Michael Geist, “Why the Anti-Terrorism Bill is Really an Anti-Privacy Bill: Bill C-51’s Evisceration of Privacy Protection” (12 March 2015) *Michael Geist* (blog), online: <www.michaelgeist.ca/2015/03/why-the-anti-terrorism-bill-is-really-an-anti-privacy-bill-bill-c-51s-evisceration-of-government-privacy/>.

Michael Vonn, “4) The Security of Canada Information Sharing Act” (21 October 2016), *BCCLA* (blog), online: <www.bccla.org/2016/10/security-canada-information-sharing-act/>.

Michael Vonn, “Surveillance scandals break while government presses for more surveillance powers” (7 November 2016), *BCCLA* (blog), online: <www.bccla.org/2016/11/surveillance-scandals-breaking-government-presses-surveillance-powers/>.

Secondary Materials: Books

Craig Forcese & Kent Roach, *Sharing Information and lost lessons from the Maher Arar experience* (Ottawa, ON: Canadian Electronic Library, 2015).

Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Toronto, ON: Irwin, 2015).

Yavar Hameed & Jeffrey Monaghan, “Accessing Dirty Data: Methodological Strategies for Social Problems Research” in Mike Larsen & Kevin Walby (eds.) *Brokering Access: Power, Politics, and Freedom of Information Process in Canada* (British Columbia: UBC Press, 2012).

Secondary Materials: Journal Articles

Craig Forcese & Kent Roach, "Stumbling Toward Total Information Awareness: The Security of Canada Information Sharing Act" (2015) 12:7 Canadian Privacy L Rev 66-76 online: <www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2622703>

Elizabeth Symeonidou-Kastanidou, "Defining Terrorism" (2004) 12:1 European J of Crime, Criminal L & Criminal Justice 14-35 at 21.

Submission of the Canadian Bar Association, "Bill C-51: Anti-Terrorism Act, 2015 – Executive Summary" *Canadian Bar Association* (March 2015) online: <www.iclmg.ca/wp-content/uploads/sites/37/2015/03/15-15-eng-Executive-Summary.pdf>.

Secondary Materials: Newspaper Articles

Alex Boutilier, "Canada's privacy law 'Ill-suited' to 21st century, watchdog warns Trudeau", *Toronto Star*, (24 June 2016), online: <www.thestar.com/news/canada/2016/06/24/canadas-privacy-law-ill-suited-to-21st-century-watchdog-warns-trudeau.html />

"Canadian judge blasts spy agency for illegally hoarding private data", *The Guardian*, (4 November 2016), online: <www.theguardian.com/world/2016/nov/04/canadian-judge-blasts-spy-agency-for-illegally-hoarding-private-data>.

Catharine Tunney, "Jim Car says military comments not a threat to pipeline protesters", *CBC News*, (2 December 2016), online: <www.cbc.ca/news/politics/jim-carr-protests-pipeline-military-1.3878258>.

Craig Forcese & Kent Roach, "Bill C-51: the Good, the Bad…and the Truly Ugly", *The Walrus*, (13 Feb 2015), online: <www.thewalrus.ca/bill-c-51-the-good-the-bad-and-the-truly-ugly/>.

Dean Beeby, "CSIS locks horns with diplomats over anti-terror info sharing", *CBC News*, (28 Jun 2016), online: <www.cbc.ca/news/politics/csis-spies-terrorists-isis-global-affairs-canada-rcmp-privacy-c51-1.3654861>.

Jenny Uechi, "Trudeau's pipeline approvals spark protests across Canada", *National Observer*, (30 November 2016), online: <www.nationalobserver.com/2016/11/30/news/trudeaus-pipeline-approvals-spark-protests-across-canada>;

Jim Bronskill, "CSIS broke law by keeping sensitive metadata Federal Court Rules", *CBC News*, (3 November 2016), online: <www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472>;

Jim Bronskill, "CSIS Using Bill C-51 to spy on Canadians in foreign prisons memo reveals", *The Toronto Star*, (3 October 2016), online at: < https://www.thestar.com/news/canada/2016/10/03/csis-using-c-51-to-spy-on-canadians-in-foreign-prisons-memo-reveals.html>.

Lisa M Austin et al., "How C-51 Undermines Privacy", *National Post*, (30 March 2015), online: <www.news.nationalpost.com/full-comment/how-c-51-undermines-privacy>.

Lisa M Austin, Benjamin J Goold, Avner Levin and Andrea Slane, “How C-51 Undermines Privacy” The National Post (30 March 2015), online: < http://news.nationalpost.com/full-comment/how-c-51-undermines-privacy>.

Ralph Goodale, “Bill C-22 is designed to protect Canadians rights and defend their security”, *National Post*, (3 October 2016), online: <www.news.nationalpost.com/full-comment/ralph-goodale-bill-c-22-is-designed-to-protect-canadians-rights-and-defend-their-security>.

“Stephen Harper stresses importance of Anti-Terrorism Act during Montreal visit”, *CBC News*, (21 May 2015), online: <www.cbc.ca/news/canada/montreal/stephen-harper-stresses-importance-of-anti-terrorism-act-during-montreal-visit-1.3083083>.

Tamara Keith, “On Waterboarding, A President Trump Could Face Resistance From Some Republicans”, *NPR*, (21 November 2016), online: <www.npr.org/2016/11/21/502871948/on-waterboarding-a-president-trump-could-face-resistance-from-some-republicans>.

Tonda Maccharles, “CSIS official admits reporters may have been under surveillance in the past”, *Toronto Star*, (28 November 2016), online: <www.thestar.com/news/canada/2016/11/28/csis-official-admits-reporters-may-have-been-under-surveillance-in-the-past.html>.

Secondary Materials: Websites

“Bill C-51: An Attack on Privacy” *FIPA* (20 April 2015), online: <www.fipa.bc.ca/bulletin-c-51/>.

Daniel Therrien, “Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the study of the *Security of Canada Information Sharing Act (SCISA)*” (16 November 2016) *Office of the Privacy Commissioner of Canada*, online: <www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20161122/>.

Online Consultation on National Security”, *Public Safety Canada* (2016), online: <www.publicsafety.gc.ca/cnt/cnslttns/ntnl-scrt/index-en.aspx>.

Statement from the Privacy Commissioner of Canada following the tabling of Bill C-51” *Office of the Privacy Commissioner of Canada* (30 January 2015), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2015/s-d_150130/>.