



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

**SAFEGUARDING CANADA'S NATIONAL
SECURITY WHILE PROTECTING CANADIANS'
PRIVACY RIGHTS: REVIEW OF THE SECURITY OF
CANADA INFORMATION SHARING ACT (SCISA)**

**Report of the Standing Committee on
Access to Information, Privacy and Ethics**

**Blaine Calkins
Chair**

MAY 2017

42nd PARLIAMENT, 1st SESSION

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Standing Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the Parliament of Canada Web Site
at the following address: <http://www.parl.gc.ca>

**SAFEGUARDING CANADA'S NATIONAL
SECURITY WHILE PROTECTING CANADIANS'
PRIVACY RIGHTS: REVIEW OF THE SECURITY OF
CANADA INFORMATION SHARING ACT (SCISA)**

**Report of the Standing Committee on
Access to Information, Privacy and Ethics**

**Blaine Calkins
Chair**

MAY 2017

42nd PARLIAMENT, 1st SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Blaine Calkins

VICE-CHAIRS

Daniel Blaikie
Nathaniel Erskine-Smith

MEMBERS

Bob Bratina	Pat Kelly
Emmanuel Dubourg	Wayne Long
Eli Ehsassi	Raj Saini
Matt Jeneroux	

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Mike Bossio	Marc Serré
Colin Carrie	Ramesh Sangha
Pierre-Luc Dusseault	Brenda Shanahan
Bernadette Jordan	Robert Sopuck
Joël Lightbound	Filomena Tassi
Rémi Massé	Nick Whalen
Pierre Paul-Hus	

CLERK OF THE COMMITTEE

Hugues La Rue

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Michael Dewing, Analyst
Chloé Forget, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FIFTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h)(vi), the Committee has studied the *Security of Canada Information Sharing Act* (SCISA) and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS	1
CHAPTER 1: INTRODUCTION.....	5
1.1 Mandate.....	5
1.2 Overview of the <i>Security of Canada Information Sharing Act</i>	5
1.2.1 Purpose and Principles of the <i>Security of Canada Information Sharing Act</i>	5
1.2.2 New Information-Sharing Authorities	6
1.2.2.1 Authorities in General	6
1.2.2.2 Definition of “Activity That Undermines the Security of Canada”	7
1.2.2.3 Civil Immunity	7
1.2.2.4 Regulations	7
CHAPTER 2: CONCERNS REGARDING THE SCOPE OF INFORMATION-SHARING AUTHORITIES IN THE <i>SECURITY OF CANADA INFORMATION SHARING ACT</i> AND ITS PRIVACY IMPACTS	9
2.1 Importance of Finding the Right Balance Between National Security and Privacy.....	9
2.2 Concerns Regarding the <i>Security of Canada Information Sharing Act</i>	10
2.2.1 Scope of Sharing Under the Act	10
2.2.1.1 Bulk Information Sharing	12
CHAPTER 3: ROLE OF THE <i>SECURITY OF CANADA INFORMATION SHARING ACT</i>	13
3.1 Views of Federal Institutions on the Role of the Act.....	13
3.2 Views of Various Witnesses on the Role of the Act	16
3.2.1 Need for Evidentiary Basis	16
3.2.2 Pre-existing Authorities.....	18
CHAPTER 4: USE AND APPLICATION OF THE <i>SECURITY OF CANADA INFORMATION SHARING ACT</i> TO DATE	21
4.1 Survey by the Office of the Privacy Commissioner	21
4.2 Use of the Act by Federal Institutions	21
4.3 Meaning of a “Disclosure” Under the <i>Security of Canada Information Sharing Act</i>	22
CHAPTER 5: THE NEED FOR LEGAL STANDARDS TO PROTECT PRIVACY	25

5.1	General Concerns About the Lack of Legal Standards	25
5.2	Institutions Able to Disclose Information Under the <i>Security of Canada Information Sharing Act</i> and Recipient Institutions in Schedule 3.....	26
5.3	Definition of “Activity That Undermines the Security of Canada”	28
5.4	Established Thresholds for Sharing Information	33
5.5	The Legal Effects of the <i>Security of Canada Information Sharing Act</i> , and its Interaction with Other Judicial Authorities.....	38
5.5.1	The Interaction Between the <i>Security of Canada Information Sharing Act</i> and the <i>Privacy Act</i>	38
5.5.1.1	The Perspective of Some Witnesses.....	39
5.5.1.2	The Perspective of Federal Institutions	40
5.5.1.3	The Committee’s Recommendations.....	40
5.5.2	Broadening the Mandate of Federal Institutions and Requiring a Warrant to Obtain Certain Information	41
5.5.2.1	Broadening the Mandate of Federal Institutions	41
5.5.2.2	The Requirement for a Warrant to Obtain Certain Information	42
5.5.2.3	The Committee’s Recommendations.....	43
CHAPTER 6:	OVERSIGHT	45
6.1	The Importance of Oversight.....	45
6.2	Currently Existing Oversight Agencies.....	48
6.2.1	The Office of the Communications Security Establishment Commissioner, the Security Intelligence Review Committee and the Civilian Review and Complaints Commission for the RCMP	48
6.2.2	The Privacy Commissioner of Canada	49
6.2.3	The Importance of Cooperation	49
6.3	The Best Oversight Model	50
6.3.1	The Need for Expert Oversight.....	50
6.3.2	The Choice of One “Super-Agency” or Several Agencies for Oversight	50
6.4	The Role of the Privacy Commissioner	54
6.5	A Parliamentary Review.....	55
6.6	Resources, Independence of Oversight Agencies and Access to Information ...	55
6.7	Record-Keeping.....	56
6.8	The View of Federal Institutions.....	57
6.9	The Committee’s Recommendations	58

CHAPTER 7: PRIVACY SAFEGUARDS	61
7.1 Reliability of Shared Information	62
7.2 Retention, Deletion and Correction of Information	64
7.3 Information-Sharing Arrangement.....	67
7.4 Privacy Impact Assessments	68
CHAPTER 8: PROTECTION FROM CIVIL PROCEEDINGS PROVIDED UNDER SECTION 9 OF THE <i>SECURITY OF CANADA INFORMATION SHARING ACT</i>	71
CHAPTER 9: CONSIDERATION OF THE COMMISSION OF INQUIRY INTO THE AIR INDIA BOMBING.....	75
APPENDIX A: CORRESPONDENCE	77
APPENDIX B: LIST OF WITNESSES	103
APPENDIX C: LIST OF BRIEFS	107
REQUEST FOR GOVERNMENT RESPONSE.....	109
SUPPLEMENTARY OPINION FROM THE CONSERVATIVE PARTY OF CANADA .	111
DISSENTING OPINION FROM THE NEW DEMOCRATIC PARTY	115

LIST OF RECOMMENDATIONS

Recommendation 1

That the Government of Canada further study which recipient institutions should be listed in Schedule 3 to the *Security of Canada Information Sharing Act* to ensure that only institutions directly relevant to Canada’s national security framework are listed. 28

Recommendation 2

That the Government of Canada amend Schedule 3 to the *Security of Canada Information Sharing Act* to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes administered or implemented by those institutions that may conceivably relate to national security concerns. 28

Recommendation 3

That the Government of Canada repeal the definition of “activity that undermines the security of Canada” in section 2 of the *Security of Canada Information Sharing Act* and replace it with a narrower definition such as the definition of “threats to the security of Canada” in the *Canadian Security Intelligence Service Act*. 33

Recommendation 4

That the Government of Canada amend subsection 5(1) of the *Security of Canada Information Sharing Act* so that any sharing of information under the Act would have to meet the standard of necessity and proportionality..... 38

Recommendation 5

That the Government of Canada amend the *Security of Canada Information Sharing Act*:

a) to clarify that the *Privacy Act* takes precedence over the *Security of Canada Information Sharing Act*.

b) to stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the *Security of Canada Information Sharing Act*..... 40

Recommendation 6

That the Government of Canada amend section 5 of the *Security of Canada Information Sharing Act* to clearly stipulate that the recipient institution must respect its mandate and current legislative and collection powers. 43

Recommendation 7

That the Government of Canada strengthen the oversight of information sharing by Government of Canada institutions, by considering the following options:

a) establishing a super-agency to provide expert oversight that would review all information-sharing activities by federal national security institutions;

b) establishing new oversight bodies, where there are existing gaps, such as the Canada Border Services Agency, capable of cooperating to review information sharing between federal institutions pursuant to the *Security of Canada Information Sharing Act*;

c) conferring new powers upon the Security Intelligence Review Committee, the Office of the Communications Security Establishment Commissioner, the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police, and the Privacy Commissioner of Canada that would enable them to:

i. oversee information sharing among the 14 Government of Canada institutions listed in Schedule 3 to the *Security of Canada Information Sharing Act* as well as their use of information; and

ii. cooperate with other agencies and conduct joint investigations;

d) establishing a parliamentary review mechanism that, on a complementary basis with one or several other expert oversight agencies, would review the information-sharing activities of federal national security institutions;

e) conferring upon the Privacy Commissioner of Canada the role of overseeing the information sharing of the 14 Government of Canada institutions listed in Schedule 3 to the *Security of Canada Information Sharing Act* as well as their use of information, and that the Privacy Commissioner report his or her findings to Parliament. 58

Recommendation 8

That the Government of Canada amend the *Security of Canada Information Sharing Act* to impose on federal institutions and on the recipient institutions listed in Schedule 3 to the Act a legal duty to keep records in order to report on any use or subsequent sharing of information provided to them under the Act..... 59

Recommendation 9

That the Government of Canada amend the *Security of Canada Information Sharing Act* in order that the guiding principles listed in section 4 become legal obligations. 62

Recommendation 10

That the Government of Canada amend the *Security of Canada Information Sharing Act* by creating a legal obligation to ensure the reliability of any shared information..... 63

Recommendation 11

That the Government of Canada amend section 10 of the *Security of Canada Information Sharing Act* to confer upon the Governor in Council the power to make regulations concerning the correction and deletion of information and that the Governor in Council make regulations regarding the correction, deletion and retention of information..... 67

Recommendation 12

That the Government of Canada amend the *Security of Canada Information Sharing Act* so as to:

- a) make it a duty for recipient institutions to enter into information-sharing arrangements with disclosing institutions; and**
- b) confer upon the Privacy Commissioner of Canada the power to review and comment on all existing or future information-sharing arrangements..... 68**

Recommendation 13

That the Government of Canada amend section 9 of the *Security of Canada Information Sharing Act* to make it clear and unequivocal that:

- a) only employees acting in good faith in the performance of their duties are immune from civil proceedings; and**
- b) the Crown remains liable for the actions of its employees. 73**

Recommendation 14

That the Government of Canada implement recommendation 10 made by the Commission of Inquiry into the Air India tragedy by amending the *Canadian Security Intelligence Service Act* to require the Canadian Security Intelligence Service to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the national security advisor..... 76

CHAPTER 1: INTRODUCTION

1.1 Mandate

On 18 October 2016, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (“the Committee”) adopted the following motion:

That the Committee undertake a study of the *Security of Canada Information Sharing Act*, its impacts on privacy since its implementation, and whether there are any changes that should be proposed in the course of the Government’s national security consultation and review.¹

The Committee began its study on 3 November 2016. Over the course of 10 meetings on the subject, it heard from 42 witnesses. It also received three briefs.

The Committee would like to thank all those who contributed to this report, including the witnesses, interpreters, Committee staff, analysts, translators and members of the publications team.

This report explores the *Security of Canada Information Sharing Act*² (SCISA) in terms of its impact on Canadians’ privacy. The Committee considered the provisions contained in SCISA, their wording, their application to date and their effect on privacy. The report presents the issues raised during the study about the extent of information-sharing authorities and their impact on Canadians’ privacy. In addition, the report addresses the proposed amendments to SCISA to resolve or mitigate these issues.

1.2 Overview of the *Security of Canada Information Sharing Act*

This section provides an overview of the provisions of SCISA addressed in the report.

In June 2015, Bill C-51, the *Anti-terrorism Act, 2015*, received Royal Assent.³ Among other measures, the bill enacted new legislation: SCISA. This new Act created additional powers for sharing national security information.

1.2.1 Purpose and Principles of the *Security of Canada Information Sharing Act*

Section 3 of SCISA states that the Act is intended to protect Canadians against “activities that undermine the security of Canada” by encouraging and facilitating the

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), 1st Session, 42nd Parliament, [Minutes of Proceedings](#), 18 October 2016.

2 [Security of Canada Information Sharing Act](#) [SCISA], S.C. 2015, c. 20, s. 2.

3 Bill C-51, [An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts](#), 2nd Session, 41st Parliament (Royal Assent, 18 June 2015).

sharing of information related to such activities among Government of Canada institutions.⁴ The preamble to the Act also lists the principles underlying the purpose of SCISA.

In addition, section 4 of SCISA sets out the principles that are to guide information sharing under the Act:

- (a) effective and responsible information sharing protects Canada and Canadians;
- (b) respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing;
- (c) entry into information-sharing arrangements is appropriate when Government of Canada institutions share information regularly;
- (d) the provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing; and
- (e) only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive information that is disclosed under this Act.

1.2.2 New Information-Sharing Authorities

1.2.2.1 Authorities in General

Subsection 5(1) of SCISA explicitly establishes a new information-sharing power for Government of Canada institutions:⁵

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 on 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 authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.

As a result, given that the information shared must relate to the recipient institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority, the criterion for sharing is that of "relevance" rather than "necessity."

Schedule 3 to SCISA lists 17 institutions that are authorized to receive information.

The wording "[s]ubject 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"

4 [SCISA](#), s. 3.

5 It should be noted that this is a discretionary power for Government of Canada institutions. Therefore, such institutions may choose whether or not to share information pursuant to SCISA.

appears to indicate that the new powers established in subsection 5(1) are subject to other Acts of Parliament or regulations made under an Act of Parliament.

Subsection 5(2) of SCISA allows the further disclosure to a Government of Canada institution listed in Schedule 3 of information that has already been shared pursuant to subsection 5(1).

Section 6 of SCISA specifies the rules that apply in the event that information initially shared pursuant to SCISA is further disclosed outside the framework of SCISA. SCISA neither prohibits nor authorizes this further disclosure, but stipulates that it must be done in accordance with the law.

There were already certain authorities related to the sharing of information in place before SCISA came into effect. Indeed, section 8 of SCISA stipulates that SCISA does not limit any pre-existing sharing authorities and that such authorities continue to apply. Specifically, several Government of Canada institutions could already share information with other Government of Canada institutions under an Act of Parliament, at common law or under the royal prerogative.

1.2.2.2 Definition of “Activity That Undermines the Security of Canada”

As mentioned above, the information-sharing authorities that SCISA confers on Government of Canada institutions deal specifically with “activities that undermine the security of Canada.” Section 2 of SCISA defines this term. It should be noted that this definition excludes “advocacy, protest, dissent and artistic expression.”⁶

1.2.2.3 Civil Immunity

Section 9 of SCISA provides for civil immunity: “No civil proceedings lie against any person for their disclosure in good faith of information under this Act.”

1.2.2.4 Regulations

Pursuant to section 10 of SCISA, on the recommendation of the Minister of Public Safety and Emergency Preparedness, the Governor in Council may make regulations implementing SCISA, including regulations respecting the manner of disclosing information. However, for the time being, no regulations have been made.⁷

6 [SCISA](#), s. 2.

7 Office of the Privacy Commissioner of Canada, [2015–2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act](#), September 2016.

CHAPTER 2: CONCERNS REGARDING THE SCOPE OF INFORMATION-SHARING AUTHORITIES IN THE SECURITY OF CANADA INFORMATION SHARING ACT AND ITS PRIVACY IMPACTS

Information sharing is a critical aspect of national security. However, information sharing can have consequences for the rights and freedoms of Canadians, especially in regards to privacy. The Committee therefore took a particular interest in the privacy impacts of information sharing under SCISA. The evidence gathered shows that there are a variety of opinions on the effects of SCISA, the scope of information sharing it permits, and the balance it strikes between national security and privacy.

2.1 Importance of Finding the Right Balance Between National Security and Privacy

Above all, multiple witnesses emphasized the importance of information sharing to national security.⁸ Mr. Kent Roach, Professor at the University of Toronto, provided the following illustration:

With the Arar saga we see the dangers of sharing information that is not reliable and is not strictly necessary for the mandate of a receiving institution. ... Just as importantly, however, the Air India commission showed the dangers of not sharing enough information.⁹

At the same time, a number of witnesses underscored the need to find the right balance between national security and privacy.¹⁰ Mr. Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment (CSE) Commissioner, argued that security measures are vital to our country, but should not “be detrimental to privacy rights.”¹¹ Ms. Sukanya Pillay of the Canadian Civil Liberties Association (CCLA) emphasized the fact that “we can only have effective security when we ensure that our civil

8 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese, Professor, Faculty of Law, University of Ottawa, as an Individual); 1120 (Ms. Sukanya Pillay, Executive Director and General Counsel, Canadian Civil Liberties Association); Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016; ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1110 (Mr. Kent Roach, Professor, Faculty of Law and Munk School, University of Toronto, as an Individual); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1130 (Mr. Anil Kapoor, Barrister, Kapoor Barristers); 1125 and 1225 (Mr. Ziyaad Mia, Member, Legal Advocacy Committee, Canadian Muslim Lawyers Association); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1140 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

9 Ibid. (Mr. Kent Roach).

10 Ibid., 1230 (Ms. Sukanya Pillay); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1235 (Mr. Wesley Wark, Visiting Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1210 (Mr. Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment Commissioner); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

11 Ibid., (Mr. Jean-Pierre Plouffe).

liberties are there.”¹² Mr. David Elder of the Canadian Bar Association (CBA) stated that his organization

supports information sharing for the purpose of national security when that sharing is necessary, proportionate, and accompanied by adequate measures against potential abuse. However, sharing too much information or sharing information for unrestricted purposes can lead to harmful consequences. Moreover, such oversharing is contrary to the principles underlying privacy laws in Canada.¹³

On the one hand, some witnesses said that SCISA does not strike the right balance between national security and privacy and this should be corrected.¹⁴ On the other hand, several witnesses noted that there are situations in which national security trumps privacy.¹⁵ Still, according to Ms. Micheal Vonn of the British Columbia Civil Liberties Association (BCCLA), the main concern with SCISA is, “does SCISA provide us with the constitutional protection that we require to be protected against what is unreasonable – not what is justifiable and reasonable, but what is unreasonable?”¹⁶

2.2 Concerns Regarding the *Security of Canada Information Sharing Act*

A number of witnesses asserted that the lack of balance between privacy and national security in SCISA is the result of several factors, including the scope of the disclosure authorities granted by SCISA.

A number of witnesses stated that SCISA’s provisions are extremely broad and could have an impact on Canadians’ privacy. In particular, some witnesses were concerned by the fact that bulk information sharing could be authorized under SCISA, given that the Act does not stipulate that information sharing must be in relation to specific individuals.

2.2.1 Scope of Sharing Under the Act

Multiple witnesses found the scope of the information sharing that SCISA allows and its impact on the privacy of Canadians worrisome. In fact, a number of witnesses pointed out that SCISA extends the information-sharing authorities of federal institutions, but offers little privacy protection.

Mr. Ziyaad Mia of the Canadian Muslim Lawyers Association (CMLA) argued that SCISA is “overly broad, unbounded information sharing.”¹⁷ According to Mr. Craig

12 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1230 (Ms. Sukanya Pillay).

13 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder).

14 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1235 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1225 (Mr. Ziyaad Mia); 1130 (Mr. Anil Kapoor).

15 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1225 (Mr. Michael Karanicolas); 1230 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1620 (Ms. Laura Tribe, Executive Director, OpenMedia).

16 Ibid. (Ms. Micheal Vonn).

17 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia).

Forcese, Professor at the University of Ottawa, the definition of an “activity that undermines the security of Canada” is “so sweeping that it encompasses things that aren’t *bona fide* national security issues. Essentially, privacy then becomes superseded by more extraneous considerations.”¹⁸

Mr. Elder of the CBA noted that SCISA “has significantly expanded intragovernmental information sharing for national security purposes in Canada, including the sharing of potentially sensitive personal information, without precise definitions, basic privacy protections, or clear limitations on the purposes for sharing.”¹⁹ The result, according to Mr. Elder, is that “there are a number of material concerns with the law as it’s currently enacted and that there’s potential for abuse. There’s potential for information sharing that I think threatens the privacy of Canadians.”²⁰

Ms. Laura Tribe of OpenMedia maintained that SCISA “contributes to an alarming privacy deficit that makes all Canadians less secure. This privacy deficit is dangerous and will have lasting consequences for the health of our democracy, for our liberty, and for our daily lives.”²¹

Lawyer David Fraser called SCISA “a privacy disaster.”²² He said that, in the past, Canadians’ information was stored in silos and could be disclosed only in accordance with specific rules. Now, however, “we have a system whereby CSIS [the Canadian Security Intelligence Service] can ask any government department for virtually any data, as long as they think it’s relevant to their task.”²³

Mr. Mia of the CMLA pointed out that the scope of the information sharing could result in agencies having too much information: “[I]f we’re trying to catch terrorists, it’s like finding a needle in a haystack. SCISA is adding a couple of trailer loads of hay to that pile.”²⁴

Finally, Ms. Vonn of the BCCLA argued that there is a crisis of public confidence in national security agencies and the organizations responsible for protecting the rights of Canadians.²⁵

18 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1135 (Mr. Craig Forcese).

19 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Eldern).

20 Ibid., 1620.

21 Ibid., 1540 (Ms. Laura Tribe).

22 Ibid., 1600 (Mr. David Fraser, Partner, McInnes Cooper, as an Individual).

23 Ibid.

24 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia).

25 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1105, 1245 and 1250 (Ms. Micheal Vonn).

2.2.1.1 Bulk Information Sharing

A number of witnesses claimed that SCISA poses risks relating to bulk information sharing. Ms. Vonn of the BCCLA noted “not only that SCISA has no requirement for individualized grounds for data collection and can facilitate the sharing of entire databases but that it also seems likely that it was enacted precisely for the purpose of bulk data acquisition.”²⁶ She further stated, “There is a grave concern about the dragnet of bulk information gathering and how it will prejudice people in the ordinary course of their participating in democratic governance.”²⁷

Ms. Lisa Austin, Professor at the University of Toronto, echoed Ms. Vonn’s statements. She pointed to the assumption that, under SCISA, “government institutions will decide to share information about specific individuals at discrete points in time rather than share institutionally held data sets for the purpose of more sophisticated analytics, including automated data processing. However, many believe that the latter is precisely what SCISA at least enables, even if it’s not being done now – I don’t know – and this raises additional privacy concerns.”²⁸ Ms. Tribe of OpenMedia made similar arguments to those of Ms. Vonn regarding the potential for bulk collection under SCISA.²⁹

Nevertheless, a number of representatives of federal institutions argued that SCISA does not expand the scope of their information collection authorities.³⁰ Mr. Stephen Burt of the Department of National Defence (DND) explained that “SCISA does not affect collection mandates whatsoever, so there is no net effect of SCISA on collection of any kind, bulk or otherwise.”³¹ Mr. Dominic Rochon of the CSE added that he has “no reason to believe that SCISA somehow now facilitates bulk sharing. It doesn’t create any new authorities.”³²

26 Ibid., 1105.

27 Ibid., 1240.

28 Ibid., 1120 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

29 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1540 (Ms. Laura Tribe).

30 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1555 (Mr. Stephen Burt, Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command, Department of National Defence); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1240 (Ms. Ann Sheppard, Senior Legal Counsel, Department of Justice); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1630 (Mr. Dominic Rochon, Deputy Chief, Policy and Communications, Communications Security Establishment).

31 Ibid., 1630 (Mr. Stephen Burt).

32 Ibid. (Mr. Dominic Rochon).

CHAPTER 3: ROLE OF THE *SECURITY OF CANADA INFORMATION SHARING ACT*

During its study, the Committee heard various viewpoints on the reasons for enacting SCISA, and on its usefulness, benefits and effectiveness. Various witnesses considered SCISA to be useful and helpful for sharing information. However, others felt it was not clear how the Act enhances the national security framework.

Based on the evidence heard, this section of the report documents the major gap between the views of federal institutions and those of numerous witnesses regarding SCISA's role. While federal institutions maintain that SCISA is useful, many witnesses argued that there is no evidence the new powers granted by SCISA are needed.

3.1 Views of Federal Institutions on the Role of the Act

A number of officials from federal institutions described the benefits of SCISA and asserted that it gives them an important new tool for sharing information effectively and improves national security.

Mr. John Davies of the Department of Public Safety and Emergency Preparedness explained the reasoning behind SCISA:

Back in 2004 the Auditor General examined how departments and agencies work together to investigate and counter threats. Then, and again in a follow-up report in 2009, she found that departments and agencies were not sharing intelligence information because of concern with violating provisions of the *Privacy Act* or the *Charter of Rights and Freedoms*, whether this concern was valid or not.

There were a number of commissions, and I won't go through the details here: in 2006, Justice O'Connor; in 2010, the commission of inquiry for the bombing of Air India; and finally, in 2011, the government of the day committed to an action on the issue of information sharing in its action plan on Air India flight 182. In 2015 that commitment was fulfilled with the introduction of SCISA.³³

According to Ms. Ann Sheppard of the Department of Justice, SCISA addresses the concerns of public servants who feared breaching the *Privacy Act* in the course of their work: "The attempt is to encourage disclosure by having one clear authority that applies to all disclosing institutions, some 200 disclosing institutions, so it's laid over the patchwork of regimes that already existed."³⁴ Similarly, Mr. David Drake of the Department of Foreign Affairs, Trade and Development (also known as Global Affairs Canada) stated that SCISA "was designed to help the government improve how it deals internally with national

33 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1210 (Mr. John Davies, Director General, National Security Policy, Department of Public Safety and Emergency Preparedness).

34 Ibid., 1245 (Ms. Ann Sheppard).

security issues, by improving national security information sharing domestically.”³⁵ Mr. Burt of DND also pointed out that SCISA simplifies information sharing:

I think all of us have probably been in situations where we were in receipt of information that we thought might be useful to someone, but we weren't sure what our authorities were to actually pass it on. This provides, as I said earlier, a couple of simple tests so you don't have to move heaven and earth to actually figure out how you can make that determination.³⁶

Ms. Alison Whelan of the Royal Canadian Mounted Police (RCMP) said that, before SCISA was enacted, “there were some government departments and agencies lacking the authority or clarity to share relevant information to protect Canada's security.”³⁷ As Mr. Donald Roussel of the Department of Transport explained, this was true of his organization:

[W]e had some limitations on what we could ask for or share. ... The other element, which is significantly troublesome, is that if we have information and we know information is out there, not being able to ask the intelligence gatherers for that information is not very useful. We have to be able to ask specifically for what we're looking for and what information they could have gathered to share with us to be able to do our work more broadly.³⁸

A number of witnesses noted that SCISA provides a useful framework for determining whether or not information can be shared to protect Canada's national security, accelerates the decision-making process for information sharing, is a more efficient framework and allows for better coordination across the government.³⁹

Ms. Whelan reported that her organization “finds SCISA to be a critical component in the information-sharing authorities we already have.”⁴⁰ As she explained

Prior to SCISA, when the RCMP needed to access information from federal departments or agencies outside the national security and intelligence community, there were disparate systems for information exchanges, and they were often lengthy. In some cases requests could take up to three weeks to process and could include more

35 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1600 (Mr. David Drake, Director General, Counter-Terrorism, Crime and Intelligence Bureau, Department of Foreign Affairs, Trade and Development).

36 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1630 (Mr. Stephen Burt).

37 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1215 (Ms. Alison Whelan, Executive Director, Strategic Policy and External Relations, Federal Policing, Royal Canadian Mounted Police).

38 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1600 (Mr. Donald Roussel, Associate Assistant Deputy Minister, Safety and Security Group, Department of Transport).

39 Ibid., 1645 (Mr. Stephen Burt); 1645 (Mr. Dominic Rochon); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1640 (Mr. David Drake); 1640 (Ms. Victoria Fuller, Director, Case Management, Consular Operations, Department of Foreign Affairs, Trade and Development); 1640 (Mr. Glen Linder, Director General, International and Intergovernmental Relations, Department of Citizenship and Immigration); 1640 (Mr. Terry Jamieson, Vice-President, Technical Support Branch, Canadian Nuclear Safety Commission).

40 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1220 (Ms. Alison Whelan).

information than investigators truly needed. SCISA allows the personnel at the national security joint operations centre to exchange information in a more streamlined way.⁴¹

Mr. Robert Mundie of the Canada Border Services Agency (CBSA) pointed out that SCISA provides an alternative to and addresses the limitations of the *Privacy Act* provisions that allow for information sharing, as the latter are “too restrictive or cumbersome to be of timely and practical use.”⁴² A number of officials from federal institutions cited section 8 of the *Privacy Act* as being one of their pre-existing information-sharing authorities, but that it is too restrictive.⁴³

According to Ms. Tricia Geddes of CSIS, her organization had trouble obtaining information from Global Affairs Canada, and SCISA proved very useful in this regard: “While we had been using the *Privacy Act* for our information exchanges with Global Affairs before this, now that we have the additional powers or the additional clarity around SCISA, there have certainly been some enhancements there, so I feel confident.”⁴⁴ Ms. Geddes said that SCISA enables her organization to obtain highly beneficial information “that’s enhancing national security.”⁴⁵

Mr. Glen Linder of the Department of Citizenship and Immigration (also known as Immigration, Refugees and Citizenship Canada (IRCC)) told the Committee that his organization sees SCISA as “creating this dedicated service channel for national security information to be discussed and exchanged among relevant experts who have the appropriate security classification.”⁴⁶

Likewise, Mr. Roussel of the Department of Transport noted that, while the pre-existing legislative provisions permitted the disclosure of information, his organization faced “a significant amount of complexity and legal challenges that made the work a lot more complicated.”⁴⁷ Consequently, SCISA enables it to move more quickly.⁴⁸ Indeed, multiple officials from federal institutions underlined that, when it comes to national security, response times are critical.⁴⁹

Although SCISA has been used by only a limited number of federal institutions since it came into force, some witnesses pointed out that it is still relatively recent

41 Ibid.

42 Ibid., 1225 (Mr. Robert Mundie, Director General and Chief Privacy Officer, Corporate Secretariat, Canada Border Services Agency).

43 Ibid., ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1600 (Mr. David Drake); 1710 (Ms. Victoria Fuller).

44 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1245 (Ms. Tricia Geddes, Director General, Policy and Foreign Relations, Canadian Security Intelligence Service).

45 Ibid.

46 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1640 (Mr. Glen Linder).

47 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1600 (Mr. Donald Roussel).

48 Ibid., ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1710 (Ms. Victoria Fuller).

49 Ibid., ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1235 (Mr. Scott Doran, Director General, Federal Policing Criminal Operations, Royal Canadian Mounted Police).

legislation and that its provisions may eventually prove useful.⁵⁰ Still, at Global Affairs Canada, “since SCISA came into force, most of the department's sharing of consular-related information with national security agencies is done under SCISA rather than pre-existing authorities.”⁵¹

Finally, Mr. Rochon of the CSE noted that SCISA “will educate departments and agencies specifically on the 17 departments and agencies that are listed as recipient agencies,” and “[a]s that education becomes deeper, I think you'll see people starting to see the benefits of being able to say, ‘Well, actually, here's an opportunity where I would be able to share because I understand their mandate better.’”⁵²

3.2 Views of Various Witnesses on the Role of the Act

Although officials from federal institutions stated that the new authorities conferred by SCISA represent important tools for safeguarding national security, a number of witnesses maintained that there was no evidence SCISA was needed to resolve an information-sharing problem and that federal institutions could resort to other authorities prior to the enactment of SCISA.

3.2.1 Need for Evidentiary Basis

Multiple witnesses felt that there was no clear justification for enacting SCISA. If there truly was a problem regarding information sharing for the purposes of national security, then the problem needed to be clearly articulated so that the most proportionate solution could be found.

In his brief, the Privacy Commissioner of Canada, Mr. Daniel Therrien, made the following argument: “Given that increased information sharing affects privacy and other rights, the justification for SCISA should be made clear.”⁵³ However, according to Commissioner Therrien and numerous witnesses who appeared before the Committee, there is no clear justification for the enactment of SCISA. The witnesses contended that a proper understanding of the problems with the pre-existing information-sharing authorities is needed in order to identify appropriate tools that strike the right balance between national security and privacy. Commissioner Therrien explained this view as follows: “A clearer articulation of the problems with the previous law would help define a proportionate solution.”⁵⁴

50 Ibid., 1600 (Mr. Donald Roussel); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1610 (Mr. Dominic Rochon); 1630 (Mr. Stephen Burt).

51 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1605 (Mr. David Drake).

52 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1610 (Mr. Dominic Rochon).

53 Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

54 Ibid.

Commissioner Therrien told the Committee that no one has shown “that the previous law was insufficient or created impediments to the work of national security agencies.”⁵⁵ He further asserted that

[i]f, previously, officials were unclear, then the officials should have received better guidance and information as to what the law provided. But if this law, SCISA, is really necessary, it should not be so on the basis that previously officials were unclear. That lack of clarity doesn't necessitate legislation. It would be on the basis that not only was it unclear, but it was insufficient, that it was an impediment, and we've not seen evidence of that.⁵⁶

A number of witnesses noted that SCISA was enacted in the wake of tragic events.⁵⁷ However, according to Ms. Vonn of the BCCLA, “[t]he question is whether, with sober hindsight now, when we apply our rationality to this, we have effected an improvement. ... We should consider very carefully not whether we have tools but whether they are the right ones.”⁵⁸ Mr. Michael Karanicolas of the Centre for Law and Democracy (CLD) made a similar argument, stating that we “need to look back in hindsight. A tragedy can give rise to particular kinds of legislation, which can be reactionary or can overstep or can fail to achieve a sober balance. We've seen that time and again.”⁵⁹

Broadly speaking, Ms. Pillay of the CCLA,⁶⁰ Mr. Karanicolas of the CLD,⁶¹ Ms. Tribe of OpenMedia,⁶² Mr. Fraser,⁶³ and Mr. Forcese⁶⁴ believe that the justification for enacting SCISA is unclear.

For Mr. Mia of the CMLA, the public justification for SCISA “is not sound,”⁶⁵ and “it was not necessary, because what we needed to do was reform a number of things in national security.”⁶⁶ Similarly, Ms. Austin said that the lack of justification for SCISA is a serious problem and that the recommendations from the Air India and Arar commissions of inquiry “are narrower in scope than what SCISA provides.”⁶⁷

55 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1115 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

56 Ibid., 1110.

57 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1210 (Ms. Sukanya Pillay); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1235 (Mr. Michael Karanicolas).

58 Ibid., 1235 (Ms. Michael Vonn).

59 Ibid., 1235 (Mr. Michael Karanicolas).

60 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1210 (Ms. Sukanya Pillay).

61 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1140 (Mr. Michael Karanicolas).

62 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1610 (Ms. Laura Tribe).

63 Ibid., 1605 (Mr. David Fraser).

64 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Mr. Craig Forcese).

65 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia).

66 Ibid.

67 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1115 (Ms. Lisa Austin).

Moreover, Mr. Tamir Israel of the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) stated that the *Privacy Act* includes provisions that enable federal institutions to share information in the event of security threats and that “we have yet to hear a compelling case for a general departure from the pre-existing exceptions already embodied in the *Privacy Act*.”⁶⁸ Indeed, Ms. Vonn of the BCCLA noted that, if the pre-existing provisions were creating confusion, the *Privacy Act* could have been amended accordingly.⁶⁹ She added that, to ensure Canada’s national security agencies have the right tools,

we need to understand the problem in greater specificity. If the problem was literally that there was some difficulty in understanding what the provisions already allowed for in the exemptions for disclosure in the *Privacy Act* were, then clarifying those exemptions is clearly the tool that we need to address those.⁷⁰

3.2.2 Pre-existing Authorities

Commissioner Therrien pointed out that other instruments that enabled the sharing of national security information were available prior to SCISA:

[T]he *Immigration Act*, the *Customs Act*, and at a more general level, the common law authority of the police in the course of investigations, to share information for the purpose of investigations, and the defence prerogative, which authorizes the defence department and the Canadian Armed Forces to share information for national security purposes. There is a whole list of other authorities that previously existed.⁷¹

The Commissioner further emphasized that “it is up to the government to demonstrate why this was insufficient.”⁷²

According to CSE Commissioner Plouffe, the pre-existing authorities were sufficient:

That CSE has neither received nor shared information under SCISA demonstrates that currently existing authorities are sufficient for it to share or disclose information with other government institutions. The point was made more broadly in the annual report of the Privacy Commissioner, Mr. Therrien, noting from a survey of government institutions his office conducted of the first six months SCISA was in effect, that only five institutions either received or shared information pursuant to the act. Most institutions, a little like CSE, have been using pre-existing authorities.⁷³

Mr. Forcese noted that, generally speaking, “Canadian information-sharing laws in the area of national security are a muddled patchwork.”⁷⁴ He explained that SCISA

68 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1220 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

69 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1145 (Ms. Micheal Vonn).

70 Ibid., 1150.

71 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1120 (Mr. Daniel Therrien).

72 Ibid., 1150.

73 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1100 (Mr. Jean-Pierre Plouffe).

74 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese).

“superimposes a new legal regime on existing legal rules that are themselves an arcane patchwork and difficult to construe.”⁷⁵ His recommendation would be “to go into the statute books of all these agencies and clean up all the differential rules that apply to govern information sharing.”⁷⁶

75 *Ibid.*, 1145.

76 *Ibid.*

CHAPTER 4: USE AND APPLICATION OF THE SECURITY OF CANADA INFORMATION SHARING ACT TO DATE

4.1 Survey by the Office of the Privacy Commissioner

The Office of the Privacy Commissioner (OPC) conducted a survey of Government of Canada institutions on the application and implementation of SCISA in the first six months since its coming into force, that is, from 1 August 2015 to 31 January 2016. The survey was issued to the 17 Government of Canada institutions that are authorized to collect and disclose information under SCISA, as well as the 111 Government of Canada institutions that may now disclose information to those 17 institutions pursuant to SCISA.

According to the OPC's survey, the CBSA, the RCMP, IRCC and CSIS reported that they had collectively received information 52 times. In addition, the CBSA, IRCC and Global Affairs Canada said they had disclosed information on a total of 58 occasions. According to the survey respondents, the "information shared under ... SCISA was for named individuals suspected of undermining the security of Canada."⁷⁷ As mentioned above, there were "legal authorities that existed before ... SCISA that permit the collection and disclosure of information for national security purposes."⁷⁸ The survey found that 13 of the 17 Government of Canada institutions authorized to collect and disclose information under SCISA had used pre-existing authorities for such sharing activities.⁷⁹

The Commissioner told the Committee that, during the second phase of his audit, his office "will review departmental records to verify whether that information is accurate and whether information sharing under authorities other than SCISA concerned suspects or persons not suspected of terrorist activities."⁸⁰

4.2 Use of the Act by Federal Institutions

CSE Commissioner Plouffe reported that the Office of the CSE Commissioner "has not shared information under SCISA, and in all probability is unlikely ever to do so."⁸¹ Likewise, the CSE "has neither received nor shared information under that law."⁸²

77 Office of the Privacy Commissioner of Canada, [2015–2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act](#), September 2016.

78 Ibid.

79 Ibid.

80 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1105 (Mr. Daniel Therrien).

81 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1100 (Mr. Jean-Pierre Plouffe).

82 Ibid., 1105.

Mr. Burt of DND stated that, at the time of the OPC's survey, his institution had not shared any information, but that since then it had disclosed information pursuant to SCISA in one instance.⁸³

The IRCC officials also said that, since August 2015, their organization "has disclosed information in response to requests from security partners on 64 occasions, and in 6 instances has proactively disclosed information to partner agencies. IRCC has also been the recipient of information on one occasion, information that has been used in an investigation for revocation of citizenship under the *Citizenship Act*."⁸⁴ Nonetheless, Mr. Linder of IRCC explained that "in all cases the information could have been provided without SCISA,"⁸⁵ but that SCISA is a simpler and faster method.⁸⁶

Mr. Mundie of the CBSA reported that, "[i]n the first half of the year of implementation, the CBSA made 24 disclosures under SCISA, and during the same time period, eight disclosures were made to the CBSA."⁸⁷

As for Global Affairs Canada, "since SCISA came into force, most of the department's sharing of consular-related information with national security agencies is done under SCISA rather than pre-existing authorities."⁸⁸ Ms. Victoria Fuller, an official with that department, said that her organization "has received requests, which we responded to 25 times. We've made 20 responses in which we did not provide information for one reason or another, and we've made 16 proactive responses."⁸⁹

Although SCISA has been used by only a limited number of federal institutions since it came into force, some witnesses pointed out that it is still relatively recent legislation and that its provisions may eventually prove useful.⁹⁰

4.3 Meaning of a "Disclosure" Under the *Security of Canada Information Sharing Act*

A number of witnesses were unable to define the term "disclosure." Does a disclosure concern a single individual, or can it involve a large number of Canadians? As a result, while the OPC's survey seems to show that SCISA is little used, the scope of the information sharing may in reality be greater.

83 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1555 (Mr. Stephen Burt).

84 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1610 (Mr. Glen Linder).

85 *Ibid.*, 1605.

86 *Ibid.*

87 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1230 (Mr. Robert Mundie).

88 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1605 (Mr. David Drake).

89 *Ibid.*, 1605 (Ms. Victoria Fuller).

90 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1600 (Mr. Donald Roussel); 1610 (Mr. Dominic Rochon); 1630 (Mr. Stephen Burt).

Mr. Linder of IRCC offered the following explanation: “In each case, the request for disclosure tends to be very specific to a particular situation. To my knowledge, it is usually associated with a single individual. I think it's possible that it could be a family as well, but in general, it is extremely limited.”⁹¹

Since the Security Intelligence Review Committee (SIRC) and the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police (CRCC) are currently conducting reviews of the information-sharing activities of CSIS and the RCMP under the new SCISA regime, Mr. Richard Evans of the CRCC and the Honourable Pierre Blais, Chair of SIRC, told the Committee that they would be able to provide more information about the concept of disclosure at the conclusion of their respective reviews.⁹²

91 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1645 (Mr. Glen Linder).

92 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1130 and 1145 (Hon. Pierre Blais, Chair, Security Intelligence Review Committee); 1100 and 1145 (Mr. Richard Evans, Senior Director, Operations, Civilian Review and Complaints Commission for the Royal Canadian Mounted Police).

CHAPTER 5: THE NEED FOR LEGAL STANDARDS TO PROTECT PRIVACY

To strike a balance between national security and privacy, several witnesses said that the best option would be to repeal SCISA because of its shortcomings and scope and start again in order to find a new solution.⁹³

However, for the purpose of finding a solution, witnesses who want to amend⁹⁴ SCISA and even those who want to repeal the Act consider it a priority to modify SCISA to include legal standards that limit the scope of its provisions. Indeed, several witnesses expressed concern about the lack of legal standards. Including such standards would better protect Canadians' privacy. A number of witnesses suggested changes to limit the Act's scope, for example with regard to the number of federal institutions subject to SCISA, the threshold in SCISA for disclosure, the definition of "activity that undermines the security of Canada," and the legal effects of SCISA and its interaction with other legislation.

5.1 General Concerns About the Lack of Legal Standards

Commissioner Therrien is concerned that SCISA does not include legal standards to protect the privacy of Canadians: "The obligation to disclose information in a manner that is consistent with privacy protection should therefore become an enforceable legal standard, as is the case with the rules governing the disclosure of information."⁹⁵ In his view, to strike the right balance between national security and privacy protection and to "ensure that not too much information is shared and retained,"⁹⁶ "you need the right safeguards and the threshold."⁹⁷ Commissioner Therrien said his concerns are not theoretical, but real:

We have seen cases in the recent past where there has been excessive, sometimes unlawful, collection or retention of information. Think of the report of the CSE commissioner who found that the CSE had disclosed metadata to other countries illegally. Think of the recent judgment by the Federal Court that found that CSIS had unlawfully retained the metadata of a large number of law-abiding individuals who are not threats to national security because CSIS felt it needed to keep that information for analytical purposes.⁹⁸

93 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125, 1140 and 1245 (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1100 and 1150 (Ms. Micheal Vonn); 1145 (Ms. Lisa Austin); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1540 (Ms. Laura Tribe); 1610 (Mr. David Fraser).

94 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1150 (Mr. Michael Karanicolas); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1620 (Mr. David Elder).

95 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1100 (Mr. Daniel Therrien).

96 Ibid., 1110.

97 Ibid., 1135.

98 Ibid., 1130.

Several witnesses made similar comments and said that one way to reduce SCISA's impact on privacy is to include adequate safeguards.⁹⁹

Mr. Karanicolas of the CLD said that sharing information needs to be done “according to clear and carefully constructed rules to ensure that the system operates and that the system can’t be pushed in abusive directions.”¹⁰⁰ In his opinion, witnesses’ recommendations to amend SCISA to include safeguards are a means of striking a balance between national security and privacy.¹⁰¹ Similarly, Ms. Austin argued that “the questions about overbreadth, safeguards, protections, and thresholds all become really important in striking that balance fairly.”¹⁰² Ms. Vonn also argued that Canadians “want the pre-stage protections to make sure that you have justification and authorization, and then by all means give law enforcement the tools they need to do their job.”¹⁰³ Mr. Fraser remarked that “a whole lot of mischief could go on within the ambit of this statute. I think we need to make sure we’re putting appropriate fences around that information.”¹⁰⁴

Lastly, Mr. Forcese noted as follows:

In the world of big data, the boundaries between collection and use are beginning to blur because of the amount of information that is currently in circulation and easily extractable from the public domain. In the absence of safeguards on how information is amalgamated by an agency and then what it can do with that information, I think that we run the risk that the net result is that the government knows more about people than it would otherwise know.¹⁰⁵

5.2 Institutions Able to Disclose Information Under the *Security of Canada Information Sharing Act* and Recipient Institutions in Schedule 3

Subsection 5(1) of SCISA permits a hundred or so institutions¹⁰⁶ to disclose information to 17 recipient institutions listed in Schedule 3 to SCISA.

Some witnesses said that the list of institutions authorized to disclose information should be reduced.¹⁰⁷ However, Mr. Anil Kapoor, Barrister, argued that this list is not a

99 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1115 (Mr. Michael Karanicolas); 1115 (Ms. Lisa Austin); 1145 (Ms. Micheal Vonn); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1225 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1610 (Mr. David Fraser).

100 Ibid., 1140 (Mr. Michael Karanicolas).

101 Ibid.

102 Ibid., 1115 (Ms. Lisa Austin).

103 Ibid., 1145 (Ms. Micheal Vonn).

104 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1610 (Mr. David Fraser).

105 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1225 (Mr. Craig Forcese).

106 According to the annual report to Parliament of the Privacy Commissioner of Canada, there are 111 institutions. See [2015-2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act](#), September 2016.

107 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1220 (Ms. Lisa Austin); 1220 (Ms. Micheal Vonn).

problem if the disclosure threshold is changed to one of necessity.¹⁰⁸ He said that these institutions could possess useful information in the context of a national security investigation.¹⁰⁹

Several witnesses noted that the list of recipient institutions in Schedule 3 to SCISA casts too wide a net and must be reduced.¹¹⁰ According to Mr. Wesley Wark, a professor at the University of Ottawa, the institution list in Schedule 3 to SCISA should “include only core elements of the Canadian security and intelligence community,”¹¹¹ and as it stands, many of the entities on the list do not play a predominant role in national security matters.¹¹² Similarly, Mr. Kapoor said that the key players in national security are CSIS, the RCMP, the CSE, the Department of National Defence and the CBSA, and that these are the organizations that should be the main recipients.¹¹³ He believes information should be directed to the main stakeholders. For example, he said that the Department of Transport’s national security remit could be seen as a “knock-on remit.”¹¹⁴

However, Mr. Blais, Chair of SIRC, explained his view of things by arguing that several of these institutions fulfill a national security role:

For example, the role of the Canada Border Services Agency is different from what it was 15 or 20 years ago. Currently, the agency directly addresses the possibility that some foreigners are entering Canada, while representing a terrorism threat. The same is true of organized crime, and the Department of Finance has a role to play in that area. The Department of Transport must deal with potentially dangerous situations that occur on board airplanes and trains or in stations.

That is why the government decided to put all these institutions in Schedule 3, even if the percentage of security information that they may provide is 2%, 10% or 80%. The government didn't want any department with security-related information to be left out.¹¹⁵

Mr. Evans of the CRCC also argued that national security is a broad field and that the number of recipient institutions in Schedule 3 to SCISA could even be higher.¹¹⁶

Mr. Elder of the CBA said that it is difficult to know whether there are too many recipient institutions in Schedule 3 to SCISA: “That’s because for a number of these listed institutions, it’s not obvious — to me, anyway — exactly what their responsibilities and authorities that relate to national security are. For some of them it’s a bit more obvious; for

108 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1235 (Mr. Anil Kapoor).

109 Ibid., 1220.

110 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1205 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1220 and 1235 (Mr. Anil Kapoor); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1610 (Mr. David Fraser).

111 Ibid., (Mr. Wesley Wark).

112 Ibid.

113 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1220 and 1235 (Mr. Anil Kapoor).

114 Ibid., 1220.

115 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1235 and 1240 (Hon. Pierre Blais).

116 Ibid., 1240 (Mr. Richard Evans).

some of them it's not obvious at all."¹¹⁷ That is why the "CBA recommends that Schedule 3 to SCISA be amended to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes supervised or implemented by those institutions that may conceivably relate to national security concerns."¹¹⁸ As a result, "[g]reater specificity would assist both disclosing and receiving institutions, as well as any oversight body in assessing whether disclosure to another institution might be appropriate."¹¹⁹

To this end, the Committee asked the institutions listed in Schedule 3 to SCISA to send it a letter explaining their respective role in national security. These letters are attached as Appendix A to this report.

In light of the evidence, the Committee recommends:

Recommendation 1

That the Government of Canada further study which recipient institutions should be listed in Schedule 3 to the *Security of Canada Information Sharing Act* to ensure that only institutions directly relevant to Canada's national security framework are listed.

Recommendation 2

That the Government of Canada amend Schedule 3 to the *Security of Canada Information Sharing Act* to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes administered or implemented by those institutions that may conceivably relate to national security concerns.

5.3 Definition of "Activity That Undermines the Security of Canada"

Under subsection 5(1) of SCISA, one of the criteria a Government of Canada institution must meet to disclose information is that this information must be in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption. The scope of the information that can be disclosed depends therefore on the definition of "activity that undermines the security of Canada" set out in section 2 of SCISA. This definition reads as follows:

activity that undermines the security of Canada means any activity, including any of the following activities, if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada:

117 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Elder).

118 Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

119 Ibid.

(a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;

(b) changing or unduly influencing a government in Canada by force or unlawful means;

(c) espionage, sabotage or covert foreign-influenced activities;

(d) terrorism;

(e) proliferation of nuclear, chemical, radiological or biological weapons;

(f) interference with critical infrastructure;

(g) interference with the global information infrastructure, as defined in section 273.61 of the [National Defence Act](#);

(h) an activity that causes serious harm to a person or their property because of that person's association with Canada; and

(i) an activity that takes place in Canada and undermines the security of another state.

For greater certainty, it does not include advocacy, protest, dissent and artistic expression.

In general, many witnesses argued that the definition of “activity that undermines the security of Canada” is far too broad.¹²⁰ However, several representatives of federal institutions argued that this broad definition was justified.¹²¹

Ms. Pillay of the CCLA said that the definition of “activity that undermines the security of Canada” “can capture all sorts of unnecessary and disproportionate information on legitimate activities, thereby effectively relegating Canadians to being potential suspects.”¹²² Mr. Mia argued that the definition of “activity that undermines the security of Canada” is vague, it includes a non-exhaustive list and other elements can be added to it.¹²³ He is concerned that the current definition “is going to put all sorts of innocent Canadians onto the national security radar when they should not be.”¹²⁴

120 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1104 (Mr. Craig Forcese); 1110 (Mr. Kent Roach); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1205 (Mr. Wesley Wark); 1220 (Mr. Tamir Israel); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1130 and 1200 (Mr. Anil Kapoor); 1145 (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas); (Ms. Lisa Austinl); 1130 (Ms. Micheal Vonn); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1655 (Ms. Laura Tribe); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Ms. Sukanya Pillay).

121 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1210 (Mr. John Davies).

122 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Ms. Sukanya Pillay).

123 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1145 (Mr. Ziyaad Mia).

124 Ibid., 1230.

Mr. Forcese said that the definition of “activity that undermines the security of Canada” includes many terms that are not defined in SCISA and that this presents a danger that the Act will be inconsistently applied.¹²⁵

Mr. Roach believes it is difficult for Canadians to have confidence in information sharing under SCISA because of the current definition of “activity that undermines the security of Canada”:

I would underline that for Canadians to have confidence in this information sharing, there need to be more limits in the legislation and also more transparency about the information sharing. ... It's very difficult to ask civil society and the public not to have concerns, and indeed suspicions, about information sharing when we have such a radical, broad definition of “activities that undermine the security of Canada”, including not only legitimate topics like terrorism but also, for example, an activity that takes place in Canada and undermines the security of another state.¹²⁶

To demonstrate the scope of the definition of “activity that undermines the security of Canada,” several witnesses compared it with the narrower definition of “threats to the security of Canada” in the *Canadian Security Intelligence Service Act*¹²⁷ (CSIS Act).¹²⁸ Mr. Forcese noted that it is “difficult to overstate how broad this definition is, even as contrasted with the existing broad national security definitions such as ‘threats to the security of Canada’ in the CSIS Act.”¹²⁹

This definition reads as follows:

threats to the security of Canada means

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.

125 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese).

126 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1110 (Mr. Kent Roach).

127 Ibid., (Mr. Kent Roach); 1105 (Mr. Craig Forcese).

128 Ibid., (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1205 (Mr. Wesley Wark).

129 Ibid., (Mr. Craig Forcese).

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).¹³⁰

Mr. Davies of the Department of Public Safety and Emergency Preparedness agreed that the definition of “activity that undermines the security of Canada” is broader than “threats to the security of Canada” in the CSIS Act.¹³¹ However, he argued that “SCISA’s definition is broader to capture the role not only of CSIS but also of all departments and agencies with a national security jurisdiction or responsibility.”¹³² Ms. Sheppard of the Department of Justice said that the definition of “activity that undermines the security of Canada” was designed that way because, as it was “intended to apply to all institutions and to cover all the mandates of the recipient institutions, and to be evergreen and evolve with threats, it is conceptual.”¹³³ She added that the definition of “threats to the security of Canada” in the CSIS Act, the *Security of Information Act* and the *Criminal Code* were sources of inspiration for the definition of “activity that undermines the security of Canada.” However, these acts weren’t cross-referenced because the department didn’t want to bind the new definition to “the interpretation of other statutes.”¹³⁴ Moreover, “with the *Criminal Code*, there was concern that people might have to prove *mens rea* [sic] before disclosing.”¹³⁵

Nevertheless, according to several witnesses, it would have been better to adopt a narrower definition of “activity that undermines the security of Canada.”¹³⁶ However, Mr. Elder¹³⁷ and Mr. Fraser¹³⁸, both lawyers, said that the definition of “activity that undermines the security of Canada” did not pose a problem.

Mr. Forcese and Mr. Roach made a recommendation to

replace [the] overbroad definition of ‘activities that undermine the security of Canada’ with the more limited and established definition of ‘threats to the security of Canada’ from s.2 of the CSIS Act. This would avoid the radical expansion of security interests currently encompassed by the ‘undermining the security of Canada’ concept.¹³⁹

130 [Canadian Security Intelligence Service Act](#), R.S.C., 1985, c. C-23.

131 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1210 (Mr. John Davies).

132 Ibid.

133 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1300 (Ms. Ann Sheppard).

134 Ibid.

135 Ibid.

136 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese); 1110 (Mr. Kent Roach); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1220 and 1225 (Mr. Tamir Israel); 1240 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1130 (Ms. Lisa Austin); 1130 (Ms. Micheal Vonn); 1110 (Mr. Michael Karanicolas).

137 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1655 (Mr. David Elder).

138 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1655 (Mr. David Fraser).

139 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 5 November 2016.

Mr. Karanicolas¹⁴⁰ of the CLD, Ms. Vonn¹⁴¹ of the BCCLA and Ms. Austin, Professor, University of Toronto¹⁴² supported Mr. Forcese and Mr. Roach's recommendation. Mr. Wark also commented in this regard, noting that the definition of "threats to the security of Canada" in the CSIS Act covers what is necessary to allow "the kind of information sharing that is necessary and appropriate to securing Canadians' safety."¹⁴³ However, Mr. Davies of the Department of Public Safety and Emergency Preparedness questioned whether "all the other 16 departments and agencies would see themselves within the CSIS Act."¹⁴⁴

Lastly, the definition of "activity that undermines the security of Canada" includes this passage: "For greater certainty, it does not include advocacy, protest, dissent and artistic expression." Mr. Forcese explained that this "list was originally qualified by the word 'lawful', but under pressures from civil society groups, the last Parliament deleted the word 'lawful'. [...] By simply dropping the word 'lawful', however, the new act seems to preclude new information-sharing powers in relation to any sort of protest, advocacy, or dissent, no matter how violent."¹⁴⁵ Ms. Pillay¹⁴⁶ of the CCLA and Mr. Mia¹⁴⁷ of the CMLA also expressed concerns about this. According to Mr. Forcese, the *National Security Green Paper, 2016*¹⁴⁸ "says that the exception does not include 'violent actions.'"¹⁴⁹ He said that it is "a policy position, not something that is binding or in the least evident from the actual statute."¹⁵⁰ When SCISA was passed, Mr. Forcese had proposed "that 'lawful' be dropped but then recommended the same compromise found in the definition of 'terrorist activity' in the *Criminal Code*. We recommended excluding both lawful and unlawful protest and advocacy, but only so long as it was not tied to violence."¹⁵¹ Mr. Forcese and Mr. Roach made the following recommendation: "Mirror the exemption to the information-sharing regime on s.83.01(b)(ii) (E) of the *Criminal Code*, thereby exempting 'advocacy, protest, dissent, or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses A to C.' (i.e., essentially that is not intended to endanger life, health or safety)."¹⁵²

In light of the evidence, the Committee recommends:

140 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

141 Ibid., 1130 (Ms. Micheal Vonn).

142 Ibid., 1130 (Ms. Lisa Austin).

143 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1240 (Mr. Wesley Wark).

144 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1300 (Mr. John Davies).

145 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese).

146 Ibid., 1145 (Ms. Sukanya Pillay).

147 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1230 (Mr. Ziyaad Mia).

148 Public Safety Canada, [Our Security, Our Rights: National Security Green Paper, 2016](#).

149 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese).

150 Ibid.

151 Ibid.

152 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 5 November 2016.

Recommendation 3

That the Government of Canada repeal the definition of “activity that undermines the security of Canada” in section 2 of the *Security of Canada Information Sharing Act* and replace it with a narrower definition such as the definition of “threats to the security of Canada” in the *Canadian Security Intelligence Service Act*.

5.4 Established Thresholds for Sharing Information

A number of witnesses addressed the threshold stipulated in SCISA for sharing information. Pursuant to subsection 5(1) of SCISA, the information disclosed by a Government of Canada institution must be relevant to the recipient institution’s jurisdiction or responsibilities under an Act of Parliament or another lawful authority. The criterion for sharing information is therefore relevance.

During his appearance, Mr. Davies of the Department of Public Safety and Emergency Preparedness explained the relevance threshold:

As a threshold, “relevant” allows institutions to disclose information when it is linked to the mandate of the recipient institution. “Relevant” also integrates important aspects of responsible information sharing. In particular, to reasonably determine whether information is relevant, the institution must assess whether the information is accurate and reliable. Finally, “relevant” requires that the connection be real and present at the time of disclosure. Information cannot be disclosed on the basis that it is potentially relevant or will likely be relevant at some time in the future.¹⁵³

However, many witnesses believe that relevance is too low a standard and that a more rigorous threshold is needed for sharing information.¹⁵⁴

Commissioner Therrien described his concerns to the Committee:

Setting such a low standard is a key reason why the risks to law-abiding citizens are excessive. If the necessity or strictly necessary criteria is adequate for CSIS to collect, analyze and retain information, as has been the case since its inception, it’s unclear to us why this standard can’t be adopted for all departments and agencies with a stake in national security. Necessity is the international privacy standard.¹⁵⁵

In his submission, Commissioner Therrien added that “necessity and proportionality, which the OPC recommended in its review of SCISA should apply to all domestic information sharing.”¹⁵⁶

153 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1210 (Mr. John Davies).

154 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1120 (Ms. Sukanya Pillay); 1130 (Mr. Kent Roach); 1125 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1100 (Mr. Daniel Therrien).

155 Ibid., (Mr. Daniel Therrien).

156 Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

CSE Commissioner Jean-Pierre Plouffe also said that he supported the necessity test proposed by Commissioner Therrien.¹⁵⁷ Similarly, Mr. Evans of the CRCC is in favour of imposing a necessity test on the recipient institution.¹⁵⁸

Other witnesses raised concerns about how relevance would affect privacy. Mr. Elder of the CBA said that “mere relevance is a very low standard ... and this could allow for unnecessary and overbroad sharing of information, undermining the privacy rights of Canadians.”¹⁵⁹ Mr. Israel, lawyer with CIPPIC, considered relevance to be too broad a standard, stating that it “is perhaps the lowest and least-defined legal evidentiary standard”¹⁶⁰ and could be used to “justify generalized information sharing.”¹⁶¹ Mr. Roach commented that relevance “allows data mining.”¹⁶²

A number of witnesses stressed that necessity and proportionality should be the standard:

- “The CBA recommends that section 5(1) of SCISA be amended to allow a government institution to disclose information to a designated recipient institution only where the information is both relevant to the recipient institution’s mandate respecting national security and ‘strictly necessary’ to fulfill that mandate.”¹⁶³ **CBA**
- “As noted, the justification found at subsection 5(1) is relevance, which is not, in my view, a tight enough criterion as it does not provide any rigorous guidance and does not allow for any real accountability. Relevance needs to be replaced by some form of language about necessity and should include a measure of proportionality that is linked to mandates and to threats.”¹⁶⁴ **Mr. Wark, Professor**
- “The ‘necessary’ test would impose some rigour that at least has the prospect of doing so more efficiently than a relevancy test would.”¹⁶⁵ **Mr. Kapoor, Barrister**
- “OpenMedia believes the principles of necessity and proportionality are workable mechanisms for sharing or receiving threat data, and there is no

157 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1245 (Mr. Jean-Pierre Plouffe); 1245 (Mr. Richard Evans).

158 Ibid.

159 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder).

160 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1215 (Mr. Tamir Israel).

161 Ibid.

162 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1130 (Mr. Kent Roach).

163 Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

164 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1205 (Mr. Wesley Wark).

165 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1200 (Mr. Anil Kapoor, Barrister).

need for SCISA's expanded definitions of security in this context.”¹⁶⁶
Ms. Tribe, OpenMedia

- “As recommended by Privacy Commissioner, amend s.5 to require shared information be ‘necessary’ or ‘proportionate’ and not simply ‘relevant’ to the receiving institution’s security jurisdiction.”¹⁶⁷ **Mr. Roach and Mr. Forcese, Professors**
- “For the recipient organization, I think they should collect only the information that's necessary for their operations, the information that relates to their statutory obligations related to threats to the security of Canada. As an example, if there was a written request for particular information and the head of that institution, which is listed in schedule 3 of the act, certified that the information was necessary for their lawful activities, and each request was subject to scrutiny and oversight, it would be a very significant improvement on the act.”¹⁶⁸ **Mr. Fraser, Lawyer**
- “[I]nformation sharing is a critical component in countering terrorist activities, but such information sharing must be effective. This means that the information collected must be reliable and subject to constitutional requirements of necessity and proportionality and constitutional safeguards including caveats on use, retention, access, and dissemination. All of these, and legally enforceable provisions, are missing in the SCISA.”¹⁶⁹ **Ms. Pillay, CCLA**
- “CIPPIC would therefore encourage two amendments to correct the existing potential overbreadth in SCISA. First, we would replace the relevance standard within the act with one of proportionality and necessity. Second, we would encourage ... an amendment to the *Privacy Act* that would adopt an overarching proportionality and necessity requirement that would apply across all government sharing practices, regardless of the specific *Privacy Act* exception under which they are occurring. This would, as we indicated in our previous testimony, apply to information sharing done under SCISA, as well. The addition of an explicit necessity and proportionality obligation would create a more precise framework for information sharing than that currently embodied in paragraph 8(2)(e) and paragraph 8(2)(m), employing the known standards of necessity and proportionality, which agencies have experience employing in a national security context.”¹⁷⁰ **Mr. Israel, CIPPIC**

166 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1540 (Ms. Laura Tribe).

167 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 5 November 2016.

168 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Fraser).

169 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1120 (Ms. Sukanya Pillay).

170 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1220 (Mr. Tamir Israel).

- “The Privacy Commissioner has also recommended that rather than the current standard, which dictates that certain federal government institutions may share information among themselves so long as it is relevant to the identification of national security threats, a standard of being necessary should be put in place. We support this recommendation, and add the note that if we’re talking about security, data minimization, whereby organizations seek to limit material stored to what is strictly necessary, is a cardinal principle of digital security.”¹⁷¹ **Mr. Karanicolas, CLD**
- “There have been a number of suggestions that you can change the ‘relevance’ standard to one of necessity. I think that would be an improvement for sure, so in those terms I would support it.”¹⁷² **Ms. Austin, Professor**

However, a number of federal institutions highlighted concerns about raising the communication threshold. As Mr. Davies of the Department of Public Safety and Emergency Preparedness stated, “If the threshold’s too low, there are, obviously, negative privacy impacts. If it’s too high, the benefits to national security and the viability of the act are threatened.”¹⁷³

According to Mr. Davies, changing from relevance to a more restrictive threshold such as necessity could have an impact on institutions that do not have a national security mandate, as they would be required to know the exact mandate of the institution receiving the information.¹⁷⁴ Ms. Geddes of CSIS emphasized that the current threshold is appropriate. She explained that her organization sometimes deals “with partners who are not national security experts,”¹⁷⁵ such as Global Affairs Canada. This institution has consular officials all over the world who are sensitized to national security issues but are not national security experts. Raising the threshold “would create some challenges and would put an awful lot of pressure on a consular officer to determine whether such-and-such is relevant or not. I think that would be a very difficult position to put them in.”¹⁷⁶ Mr. Davies stated that “if you go up to the necessity standard, then there will more than likely be less information going to the national security agencies. ... You would have to talk to the non-national security agencies that are probably most vulnerable to understanding what national security necessity is for those receiving it.”¹⁷⁷ Mr. Linder of IRCC stated as follows:

171 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

172 Ibid., 1120 (Ms. Lisa Austin).

173 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1210 (Mr. John Davies).

174 Ibid., 1210 and 1250.

175 Ibid., 1250 (Ms. Tricia Geddes).

176 Ibid.

177 Ibid., 1300 (Mr. John Davies).

If it were a test of necessity, we would need to be convinced with a lot more information that were [*sic*] necessary, in fact, not simply relevant. And what would that mean in practice? I think that would mean that our national security agencies, the investigative bodies that were requesting information from us, would possibly have to give us a lot more national security information for us to make that determination and be satisfied that it was, in fact, necessary and not simply relevant.

Could we do that? Absolutely, but it's worth considering whether the benefit of having that higher standard is outweighed by having more sensitive national security information in circulation, in order for us to make that determination. More generally—and I think this is possibly the intent—it obviously would put a chilling effect on the amount of information we would disclose under SCISA. That would be a necessary outcome.¹⁷⁸

Mr. Burt from the Department of National Defence stated that subjecting recipient institutions to a necessity test, in other words, allowing institutions to receive only information that was necessary to their mandate, would raise the bar: “It would be a more difficult bar to meet for sharing, but it would depend on how it was formulated.”¹⁷⁹

In his submission to the Committee, Commissioner Therrien suggested an alternative that could address the concerns of federal institutions:

As an alternative to adopting a “necessity and proportionality” standard for information-sharing across the board, consideration could be given to adopting dual thresholds, one for the disclosing institutions, and another for the 17 recipient institutions. An important point raised by departmental officials during the current review of SCISA by the Standing Committee on Access to Information, Privacy and Ethics is that because front line staff in non-listed departments do not necessarily have the requisite expertise or experience to make real-time and nuanced decisions as to what is necessary and proportional for purposes of carrying out a national security mandate, the onus of the higher threshold would be shifted to the 17 recipient departments that do have the capacity to make such decisions in an informed manner. The Committee discussed the issue of a “dual threshold” and this would appear a reasonable solution under the following condition. In order to close the triage gap between these two different thresholds, the 17 recipient departments should be responsible for selectively receiving and retaining only information that meets the higher threshold of necessity and proportionality (subject to any further limits imposed by their enabling laws), and under a positive legal obligation to return or destroy information that does not.¹⁸⁰

Other witnesses stated that another way to ease institutions’ fears would be to provide training on information-sharing thresholds.¹⁸¹ Mr. Israel of CIPPIC also recommended “training units within different government agencies, potentially within the existing ATIP [Access to Information and Privacy] infrastructure that most government

178 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1635 (Mr. Glen Linder).

179 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1705 (Mr. Stephen Burt).

180 Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

181 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1220 (Mr. Tamir Israel); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1155 (Mr. Anil Kapoor).

agencies have, to have expertise so that in-house capabilities can be developed to identify threat-related data.”¹⁸²

In light of the evidence, the Committee recommends:

Recommendation 4

That the Government of Canada amend subsection 5(1) of the *Security of Canada Information Sharing Act* so that any sharing of information under the Act would have to meet the standard of necessity and proportionality.

5.5 The Legal Effects of the *Security of Canada Information Sharing Act*, and its Interaction with Other Judicial Authorities

During the hearings, a number of witnesses stated that the interaction between SCISA and other judicial authorities seemed to have some unanticipated consequences that could affect Canadians’ privacy. In fact, witnesses mentioned numerous effects of SCISA that should be addressed, including the primacy of SCISA over the *Privacy Act*, the impact of SCISA on the mandate of institutions listed in Schedule 3 to that Act and the requirement for federal institutions to have a warrant to obtain certain information.

To begin with, the witnesses stated that it was unclear whether or not the *Privacy Act* took precedence over SCISA, which means that the legal protections covering privacy would not apply to information sharing under SCISA. Furthermore, they explained that the broad scope of SCISA could expand the mandate of the Government of Canada institutions listed in Schedule 3 to the Act. Lastly, some witnesses were concerned that SCISA authorizes the sharing of information that would have previously required a warrant.

5.5.1 The Interaction Between the *Security of Canada Information Sharing Act* and the *Privacy Act*

As stated previously, various witnesses raised concerns about the possibility that SCISA could have primacy over the *Privacy Act* and the potential impact on Canadians’ privacy should that be the case.

Subsection 5(1) of SCISA uses the following language: “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.” It therefore appears that the new information-sharing powers are subordinated to other applicable federal laws or regulations. Mr. Forcese and Mr. Mia nevertheless claimed that the meaning of these terms is vague and a source of confusion.¹⁸³

182 Ibid. (Mr. Tamir Israel).

183 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1150 (Mr. Ziyaad Mia).

5.5.1.1 The Perspective of Some Witnesses

Several witnesses indicated that there is ambiguity with regard to the interaction between SCISA and the *Privacy Act* and that it is not clear which takes precedence.¹⁸⁴ According to Mr. Forcese and Mr. Roach, it appears that SCISA must respect the provisions of the *Privacy Act*.¹⁸⁵ “Section 5 of the new act says that it’s subject to other existing acts that constrain or control the disclosure of information, which would suggest the *Privacy Act*.”¹⁸⁶ According to some witnesses, however, the *National Security Green Paper, 2016*¹⁸⁷ appears to offer a different interpretation.¹⁸⁸ Mr. Forcese gave the following explanation: “They say that because the new *Security of Canada Information Sharing Act* authorizes disclosure, it satisfies a lawful authority exception to the *Privacy Act*, effectively trumping it.”¹⁸⁹ The *Privacy Act* authorizes a federal institution to disclose personal information about an individual without that person’s consent when it is “for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure.”¹⁹⁰ Mr. Forcese explained as follows:

The *Privacy Act* itself has an exception saying that where some other active statute authorizes disclosure, then the *Privacy Act* rules don’t apply, so you get into a bit of a circle. The new act says subject to other laws, the *Privacy Act* says subject to permission in new laws, so which prevails?¹⁹¹

The CBA outlined in its brief the consequences of this confusion:

The *Privacy Act* does not address when information ‘received’ or ‘shared’ by another government institution is considered necessary, or automatically subject to the requirements that apply to information that is ‘collected’. It is unclear that personal information shared under SCISA would continue to be covered by the remaining protections under the *Privacy Act*.¹⁹²

The CBA therefore “recommends clarifying the interaction between the *Privacy Act* and SCISA.”¹⁹³ During his appearance, Mr. Elder commented that “[t]he *Privacy Act* would generally be presumed to govern, but the *Privacy Act* has explicit exceptions for situations

184 Ibid. (Mr. Craig Forcese); 1115 (Mr. Kent Roach); Ibid. (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Elder).

185 Ibid., 1105 (Mr. Craig Forcese); 1115 (Mr. Kent Roach).

186 Ibid., 1225 (Mr. Craig Forcese).

187 Public Safety Canada, [Our Security, Our Rights: National Security Green Paper, 2016](#).

188 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1105 and 1225 (Mr. Craig Forcese); 1115 (Mr. Kent Roach); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1150 (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

189 Ibid., 1105 (Mr. Craig Forcese).

190 *Privacy Act*, Paragraph 8(2)(b).

191 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1225 (Mr. Craig Forcese).

192 Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

193 Ibid.

in which another law is applicable.”¹⁹⁴ Mr. Karanicolas of the CLD indicated that “we believe this should be resolved by clarifying that the *Privacy Act* does indeed apply to the *Security of Canada Information Sharing Act*.”¹⁹⁵

5.5.1.2 The Perspective of Federal Institutions

Mr. Davies of the Department of Public Safety and Emergency Preparedness explained the interpretation given to the expression “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” as it relates to the *Privacy Act*:

[I]f there is a legal restriction or prohibition on disclosing information, SCISA does not apply.

The *Privacy Act* includes a general restriction on disclosing personal information without the consent of the related individual. However, as noted in section 8 of the *Privacy Act*, it also includes a list of situations in which personal information can be disclosed despite this general restriction. For example, personal information may be disclosed for the purpose for which the information was collected. In addition, personal information may be disclosed in accordance with disclosure authorities in other acts of Parliament, such as SCISA.

When they receive information disclosed under SCISA’s authorities, as noted in section 4 of the *Privacy Act*, departments and agencies must still ensure that personal information “relates directly” to an operating program or activity before they collect it.¹⁹⁶

5.5.1.3 The Committee’s Recommendations

In light of the evidence, the Committee recommends:

Recommendation 5

That the Government of Canada amend the *Security of Canada Information Sharing Act*:

a) to clarify that the *Privacy Act* takes precedence over the *Security of Canada Information Sharing Act*.

b) to stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the *Security of Canada Information Sharing Act*.

194 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Elder).

195 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

196 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1215 (Mr. John Davies).

5.5.2 Broadening the Mandate of Federal Institutions and Requiring a Warrant to Obtain Certain Information

5.5.2.1 Broadening the Mandate of Federal Institutions

Some witnesses indicated that SCISA could serve to broaden the mandate of the institutions listed in Schedule 3 to that Act.¹⁹⁷ Indeed, the standard of “relevance” to the recipient institution’s mandate as the threshold for sharing information could lead to an expansion of institutions’ mandates.

Mr. Roach and Mr. Forcese therefore make the following recommendation: “Amend s.5 to make crystal clear that receiving recipients must operate within their existing mandates and legal authorities.”¹⁹⁸

Ms. Vonn of the BCCLA also mentioned “the seriousness of the disruption caused by SCISA’s blurring of the mandate of critically important federal institutions.”¹⁹⁹ For example, she said that “FINTRAC [Financial Transactions and Reports Analysis Centre of Canada] itself has long maintained that one of its primary safeguards for privacy is its independence from law enforcement,”²⁰⁰ but that from now on because of “the almost unfettered access to information sharing authorized by SCISA, the independence of FINTRAC in this regard is essentially fictional.”²⁰¹ CSE Commissioner Jean-Pierre Plouffe,²⁰² as well as Mr. Evans²⁰³ of the CRCC, said they were in favour of an amendment to SCISA to clarify that the Act does not change the mandate of federal institutions.

Several representatives of federal institutions nevertheless maintained that SCISA does not modify their mandate in any way, and that they always operate within their mandate.²⁰⁴

197 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 5 November 2016; ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1100 (Ms. Micheal Vonn).

198 Ibid., Craig Forcese and Kent Roach.

199 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1100 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association).

200 Ibid.

201 Ibid.

202 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1245 (Mr. Jean-Pierre Plouffe).

203 Ibid., 1245 (Mr. Richard Evans).

204 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1720 (Mr. Gérald Cossette, Director, Financial Transactions and Reports Analysis Centre of Canada); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1230 (Ms. Tricia Geddes); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1630 (Mr. Donald Roussel); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1110 (Mr. Terry Jamieson).

5.5.2.2 The Requirement for a Warrant to Obtain Certain Information

During his appearance, Commissioner Therrien made reference to the recent decision²⁰⁵ of Justice Noël of the Federal Court, which mentioned that “since the adoption of Bill C-51, CSIS is now obtaining information from the Canada Revenue Agency that previously required a warrant.”²⁰⁶ According to Mr. Therrien, “At this time, CSIS is obtaining the information without a warrant because the *Security of Canada Information Sharing Act* makes this activity possible. ... Some cases used to require warrants, but they don’t anymore.”²⁰⁷ It therefore appears that there are instances where information shared under SCISA could involve interests protected by the *Canadian Charter of Rights and Freedoms*, such as the expectation of privacy.²⁰⁸ In its brief to the Committee, the International Civil Liberties Monitoring Group indicated that “it is not clear how SCISA affects the need for agencies to obtain warrants to access certain forms of information that would otherwise require judicial approval.”²⁰⁹

Mr. Wark explained the situation as follows:

[I]f an entity in SCISA possesses information under its own lawful mandate, and it has the grounds, which according to the act are as overly broad as these grounds might be, to share that information with another entity, then the receiving entity — in this case, perhaps, CSIS or the RCMP — would be receiving that information under the lawful authority of the original collector. From its perspective, as long as those receiving agencies had an appropriate mandate to receive that information, then they wouldn’t require a secondary warrant to acquire it.²¹⁰

Mr. Israel of CIPPIC also proffered an explanation:

[I]f it received it through SCISA legitimately, then it now has legitimately received that information, and it doesn’t need to rely on its authority within the CSIS Act, which already has a necessity limitation built into it. I think it’s subject to interpretation either way, but SCISA could be seen as overturning that decision in a way that would allow CSIS to legitimately receive metadata, which it could not collect on its own footing, and to then retain it indefinitely.²¹¹

According to witnesses, it appears therefore that SCISA would enable federal institutions to obtain indirectly what they do not have a right to obtain directly. As such, Mr. Kapoor indicated that there should be an amendment “to preserve section 8 rights in

205 [X \(Re\)](#), 2016 FC 1105.

206 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1155 (Mr. Daniel Therriena).

207 Ibid

208 Ibid.

209 International Civil Liberties Monitoring Group, [Brief on the Security of Canada Information Sharing Act](#), 1 February 2017.

210 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1230 (Mr. Wesley Wark).

211 Ibid., 1230 (Mr. Tamir Israel).

the criminal prosecution realm, and there should be a requirement that a warrant be obtained.”²¹²

Mr. Wark, on the other hand, does not believe that SCISA affects the collection powers of federal institutions.²¹³ Likewise, Ms. Sheppard from the Department of Justice pointed out that SCISA “does not affect collection. It only deals with disclosure. If, for example, you need a warrant to collect information, SCISA would not interfere with that. That would prevail in circumstances where it would be required.”²¹⁴ She added:

As long as the threshold in SCISA is met — as long as it’s relevant to the national security jurisdiction or responsibilities of the recipient institution — it can be disclosed, but it always operates subject to any other law that limits disclosure. For example, if there was something in the disclosing institution’s operating legislation that prevented that, SCISA does not override it. It only deals with disclosure, and the threshold has to be met for disclosure to occur. It’s up to the recipient. Whether it’s proactively disclosed or by request, they have to make sure that they are authorized to collect it.²¹⁵

Mr. Forcese pointed out, however, that although from the government’s point of view, SCISA does not create new collection powers, everything depends on how collection is defined:

Sufficiently broad information sharing allows for the pooling of information within the hands of one agency. The information that would not legally have been able to accrue in one agency is now available to it. Technically that’s not collection in the sense that it’s not been extracted from outside of government from an individual, but rather it’s the amalgamation of information in a database in the hands of an agency.²¹⁶

5.5.2.3 The Committee’s Recommendations

In light of the evidence, the Committee recommends:

Recommendation 6

That the Government of Canada amend section 5 of the *Security of Canada Information Sharing Act* to clearly stipulate that the recipient institution must respect its mandate and current legislative and collection powers.

212 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1240 (Mr. Anil Kapoor, Barrister).

213 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1235 (Mr. Wesley Wark).

214 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1240 (Ms. Ann Sheppard).

215 Ibid.

216 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1225 (Mr. Craig Forcese).

CHAPTER 6: OVERSIGHT

6.1 The Importance of Oversight

Several witnesses stressed the importance of independent oversight²¹⁷ over how federal institutions use the new information-sharing powers established by SCISA, and of national security in general.²¹⁸ Indeed, of the 17 recipient institutions listed in Schedule 3 to SCISA, only 3 are subject to independent oversight: CSIS, the CSE and the RCMP. Numerous witnesses highlighted the importance of creating oversight and accountability mechanisms for the new powers established by SCISA, and for information sharing in the context of national security in general:

- “[I]ndependent review of information-sharing activities is incomplete, given that 14 of the 17 receiving institutions under SCISA don’t have dedicated review bodies. ... All departments involved in national security also need to be reviewed by independent experts.”²¹⁹ **Commissioner Therrien, Privacy Commissioner of Canada**
- “[I]nsofar as there is always a level of interpretation, an important emphasis must be on review as a safeguard against unreasonable exchanges.”²²⁰ **Mr. Blais, Chair, SIRC**
- “[T]here is a need for expert review for the 14 institutions not currently subject to review.”²²¹ **Mr. Plouffe, Commissioner, Office of the CSE Commissioner**
- “[T]his is information sharing with inadequate or non-existent review structures. ... [I]ncreased and integrated information collection and sharing powers are not matched in this act by increased and integrated

217 Note that several witnesses made a distinction between oversight and review. In this report, however, it is understood that the terms oversight and review both refer to an examination of an agency’s activities after the fact by an independent body.

218 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1120 (Ms. Sukanya Pillay); 1130 (Mr. Kent Roach); 1125 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1125 (Mr. Daniel Therrien); 1245 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia); 1130 and 1135 (Mr. Anil Kapoor); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe); 1115 (Hon. Pierre Blais); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1135 (Ms. Lisa Austin); 1135 (Ms. Micheal Vonn); 1110 (Mr. Michael Karanicolos); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1540 (Ms. Laura Tribe); 1550 (Mr. David Elder); 1605 (Mr. David Fraser).

219 Ibid., (Mr. Daniel Therrien).

220 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1115 (Hon. Pierre Blais).

221 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe).

review structures, and this is a serious concern for CCLA.”²²² **Ms. Pillay, CCLA**

- “SCISA must include a robust oversight and accountability mechanism to enforce these principles. In the CBA’s view, any oversight body should have independence from the government institutions that will be sharing information under the act in order to avoid any potential conflicts of interest.”²²³ **Mr. Elder, CBA**
- “[E]ven with the best legal language in the world, you’re still dependent on people construing it, which means that you need independent review to ensure that those construals are reasonable.”²²⁴ **Mr. Forcese, Professor**
- “The notion of an independent reviewer is necessary, as well, as part of the framework of oversight and review in the national security environment.”²²⁵ **Mr. Kapoor, Barrister**
- “We also broadly support the Privacy Commissioner’s recommendation that in addition to parliamentary review, institutions permitted to receive information for national security purposes should be subject to expert or administrative independent review. We noted with alarm that 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight.”²²⁶ **Mr. Karanicolas, CLD**
- “[T]here is no common oversight of any of these 17 organizations, and all of them, apparently, are instrumental in our national security. All those functions should be overseen...”²²⁷ **Mr. Fraser, Lawyer**
- “I think it is really critical to have oversight over information sharing.”²²⁸ **Ms. Tribe, OpenMedia**

Witnesses provided a variety of explanations for why it is important to establish oversight and accountability mechanisms in SCISA.

222 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1120 (Ms. Sukanya Pillay).

223 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder).

224 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1215 (Mr. Craig Forcese).

225 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1135 (Mr. Anil Kapoor).

226 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

227 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Fraser).

228 Ibid., 1700 (Ms. Laura Tribe).

According to Mr. Roach, national oversight of information-sharing activities would enhance Canadians' confidence in government institutions:²²⁹

The absence of credible review for all of the institutions, combined with the fact that the government appears in the green paper to at least be seriously considering getting more data from metadata and other things feeds into what I would say is a justifiable lack of confidence that many Canadians have about how this information, once it is collected by one part of government, is going to be shared, stored, and accessed by other parts of government.²³⁰

Commissioner Therrien also stressed that effective oversight is essential for maintaining public confidence in agencies involved in national security.²³¹ Mr. Fraser commented along those same lines:

[M]ost national security and intelligence activities are obviously top secret. ... [T]he only way you can make sure they conduct themselves in accordance with our expectations in a democratic society is to have confidence in the oversight, confidence that somebody is watching and keeping an eye on them, somebody who can keep the secrets but who can also blow the whistle when necessary.²³²

Commissioner Therrien added that although he can investigate potential complaints regarding SCISA, "in this type of area, the people who may complain don't know what's happening, so it's unlikely that there will be complaints raised to my office."²³³ Ms. Pillay of the CCLA made similar comments, noting that "violations can occur without the knowledge of an affected person, and even if there is knowledge, without an appropriate review structure there's nowhere to bring a complaint, given the absence of any one review structure with jurisdiction to review all the agencies empowered to share information."²³⁴ Mr. Mia of the CMLA also indicated that there will be no way for people to know whether information about them has been disclosed.²³⁵ Mr. Roach mentioned that

damages cannot be a substitute for effective review, because as Justice O'Connor stressed, most people do not know if information is being shared about them. Mr. Arar and other Canadians who were tortured in Syria, in part because of Canadian information sharing, knew because of the devastating consequences that they experienced, but you or I would not know right now if information about us is being shared.²³⁶

229 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1130 (Mr. Kent Roach).

230 Ibid.

231 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

232 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1705 (Mr. David Fraser).

233 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1125 (Mr. Daniel Therrien).

234 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1120 (Ms. Sukanya Pillay).

235 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1135 (Mr. Ziyaad Mia).

236 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Mr. Kent Roach).

6.2 Currently Existing Oversight Agencies

6.2.1 The Office of the Communications Security Establishment Commissioner, the Security Intelligence Review Committee and the Civilian Review and Complaints Commission for the RCMP

As previously mentioned, only 3 of the 17 institutions listed in Schedule 3 to SCISA are currently subject to independent expert review. Mr. Plouffe, Communications Security Establishment Commissioner, explained that these are: “CSE, which I review; CSIS, which is reviewed by my colleagues from SIRC [Security Intelligence Review Committee]; and the RCMP, reviewed by my colleagues from the Civilian Review and Complaints Commission.”²³⁷ SIRC and the CRCC have undertaken a study of SCISA.²³⁸

These three organizations have broad powers for fulfilling their oversight mandate.²³⁹ According to Mr. Blais, Chair of SIRC, however, “there remain blind spots.”²⁴⁰

He mentioned that his powers are subject to certain constraints:

Although SIRC has great powers to review CSIS, this ability does not extend beyond CSIS. This means that SIRC cannot assess the source, validity or reliability of the information provided to CSIS by its domestic partners, nor how CSIS information or advice is used by these partners. In short, SIRC cannot follow the thread of information to allow for a more comprehensive review of CSIS’s interactions and exchanges with domestic partners.²⁴¹

He further added that SIRC, the Office of the CSE Commissioner and the CRCC “cannot carry out joint work as their legislation extends only to the respective organizations they review.”²⁴²

In fact, we can share some information on our results generally and on operating practices, but we cannot share information, even if our relationship is very close.²⁴³

Mr. Plouffe, the CSE Commissioner, seconded these comments, saying that “it would be desirable to give the existing review bodies explicit authority to co-operate.”²⁴⁴

237 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe).

238 Ibid., 1115 (Hon. Pierre Blais); 1125 (Mr. Richard Evans).

239 Ibid., 1100 (Mr. Jean-Pierre Plouffe); (Hon. Pierre Blais); (Mr. Richard Evans).

240 Ibid., 1120 (Hon. Pierre Blais).

241 Ibid.

242 Ibid.

243 Ibid.

244 Ibid., 1135 (Mr. Jean-Pierre Plouffe).

Mr. Forcese also stressed that the three oversight agencies “are constrained in their ability to coordinate.”²⁴⁵ Mr. Wark and Mr. Mia referred to them as “these siloed mechanisms” of national security institutions.²⁴⁶

6.2.2 The Privacy Commissioner of Canada

Furthermore, the “Privacy Commissioner has a mandate to review personal information policies and practices of all federal government institutions. In this context, Commissioner Therrien is examining the Schedule 3 institutions’ use of SCISA and privacy protections.”²⁴⁷

Commissioner Therrien mentioned one problem in the context of his mandate relating to national security:

Currently, the confidentiality provisions of the *Privacy Act* prevent the OPC [Office of the Privacy Commissioner] from sharing information with other review bodies, such as the Security Intelligence Review Committee (SIRC), the Office of the Communications Security Establishment Commissioner (OCSEC) or the Civilian Review and Complaints Commission.²⁴⁸

Mr. Forcese commented that the Privacy Commissioner “has a limited subject matter jurisdiction across all of government.”²⁴⁹ Ms. Pillay of the CCLA also indicated that “[i]n the past, government has stated that the Privacy Commissioner and the Auditor General have review powers, but their mandates and resources do not provide the jurisdiction and powers that would be required to properly review the information sharing that exists under the SCISA.”²⁵⁰

6.2.3 The Importance of Cooperation

Several witnesses commented that regardless of the oversight model determined by the government, cooperation among the agencies responsible for that oversight is essential.

Commissioner Therrien indicated in his brief that “review bodies must be able to share information, including classified and personal information, so that their respective reviews can be performed in a collaborative and effective manner rather than in silos as is

245 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1155 (Mr. Craig Forcese).

246 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1245 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia).

247 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe).

248 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

249 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1155 (Mr. Craig Forcese).

250 *Ibid.*, 1120 (Ms. Sukanya Pillay).

currently the case.”²⁵¹ The Commissioner also stressed the drawbacks of a lack of cooperation:

The detriments to siloed review include duplication of effort with resulting effects on resources, but above all less informed and therefore less effective review by all relevant bodies. Given the OPC’s extensive and ongoing work in this area, it should be included among the review bodies granted the authority to share and receive information.²⁵²

According to Mr. Blais, Chair of SIRC, “In the absence of a body with jurisdiction over the broader national security community, or to a lesser extent an ability for review bodies to work together, there will be clear accountability gaps regarding domestic information sharing.”²⁵³

6.3 The Best Oversight Model

6.3.1 The Need for Expert Oversight

For Mr. Plouffe, the CSE Commissioner, it is important that the 14 institutions listed in Schedule 3 to SCISA “be subject to expert review.”²⁵⁴ Likewise, Mr. Galbraith of the CSE Commissioner’s office stressed the importance of reviews being conducted by experts.²⁵⁵

According to Commissioner Therrien, “All departments involved in national security also need to be reviewed by independent experts.”²⁵⁶

In that same spirit, Mr. Roach commented that “[o]ne of the reasons we mentioned dedicated national security review is that, particularly with the foreign information sharing and also with the evolving nature of security threats, you need to have some specialized expertise to really judge the information sharing.”²⁵⁷ Mr. Kapoor and Mr. Mia also stressed the importance of expert oversight.²⁵⁸

6.3.2 The Choice of One “Super-Agency” or Several Agencies for Oversight

Some witnesses indicated that several different oversight models exist, but did not advocate for any one in particular. Commissioner Therrien indicated that

251 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

252 Ibid.

253 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1120 (Hon. Pierre Blais, Chair).

254 Ibid., 1135 (Mr. Jean-Pierre Plouffe).

255 Ibid., 1155 (Mr. J. William Galbraith, Executive Director, Office of the Communications Security Establishment Commissioner).

256 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1100 (Mr. Daniel Therrien).

257 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1155 (Mr. Kent Roach).

258 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1235 (Mr. Ziyaad Mia); 1230 (Mr. Anil Kapoor).

in some countries, expert review takes the form of a consolidated model, meaning one review body is responsible for all relevant government institutions – a so-called “Super-SIRC” – whereas in others, different bodies are limited to reviewing one institution or one aspect of national security activities. We have no strong preference between the two models, so long as all government institutions involved in national security are covered. Furthermore, if there is more than one review body, all bodies must be able to collaborate in their review activities, and no longer operate in silos.²⁵⁹

Commissioner Therrien did nevertheless indicate that it is preferable to have “the activities of national security agencies reviewed both by the OPC and one or more dedicated national security review bodies.”²⁶⁰ He said:

This creates some overlap, but it ensures that both national security and privacy can be examined by experts with deep and broad knowledge of both privacy and national security law. Among other factors, there is value in having the privacy impact of the work of national security agencies reviewed by an institution that also reviews the work of other government departments, so that best practices and developments in privacy law can apply across government.²⁶¹

As for creating a single office, Mr. Plouffe indicated that Justice O’Connor’s report looked closely at the issue of creating one super-agency to replace the current agencies: “As an example, with regard to CSE or the Office of the CSE commissioner, Justice O’Connor has stated that it should not be included in this so-called super-agency because of its uniqueness. As you know, CSE is the foreign intelligence agency, or the electronic agency, and it’s unique in itself.”²⁶² Mr. Plouffe commented that Justice O’Connor’s report described the advantages and disadvantages of a single oversight body. It suggested that having only one agency could lead to more superficial reviews, whereas an agency that oversees only one institution might conduct more in-depth reviews.²⁶³

Mr. Plouffe feels it is up to the government to decide on the most appropriate oversight model.²⁶⁴ He added that

if the government feels that a super-agency is not in order, at least we should have a coordinating committee of some sort — and this was suggested by my colleague Justice O’Connor 10 years ago — where all the heads of review agencies meet and discuss problems in common. The committee of parliamentarians would be a practical solution, because they would have to deal with one body and not with 14, 15, or 17 institutions.²⁶⁵

259 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

260 Ibid., 5 December 2016.

261 Ibid., 5 December 2016.

262 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1150 (Mr. Jean-Pierre Plouffe).

263 Ibid.

264 Ibid., 1135.

265 Ibid.

Several witnesses commented that real-time oversight is not very realistic, and that timely review after the fact is a more effective option.²⁶⁶ Other witnesses felt that the government could look to oversight models that have been established elsewhere, such as in Australia or the United Kingdom.²⁶⁷

A number of witnesses shared their general opinion with regard to the best independent oversight model:

- “We recommend matching information-sharing powers with amendments that give independent review body(s) review over all of the government of Canada’s information sharing activities under the new Act. As suggested by the Privacy Commissioner, review should be facilitated by agreements between governmental entities that share information. Especially, ensure that this body has the power to compel deletion of unreliable information from all the agencies to which it has been distributed.”²⁶⁸ **Mr. Forcese and Mr. Roach, Professors**
- “[W]e’ve called for an integrated review.”²⁶⁹ **Ms. Pillay, CCLA**
- “I’m an advocate of a unified, independent, national security review agency, the Canada national security review agency.”²⁷⁰ **Mr. Mia, CMLA**
- “I think the one of the solutions is to have a sort of centralized control over it. I recommended in the submission that there needs to be some centralized control of information sharing. The departments could do their piece, but somewhere in government—maybe in Public Safety—there would be someone overseeing all of this. The Privacy Commissioner and SIRC and everybody will do their audits, and we’re calling for a national security review agency.”²⁷¹ **Mr. Mia, CMLA**
- “There’s a broad and specialized basket of issues that come up, and I think they should be dealt with by a dedicated oversight body.”²⁷² “It’s important to have an oversight body that has access and can view the full picture. There can be a danger in terms of stovepipe oversight ... so it’s important to allow an oversight body to get the full picture and to have access to classified information that would let them fully see if the

266 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1245 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1235 (Mr. Ziyaad Mia).

267 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1230 (Mr. Anil Kapoor).

268 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 5 November 2016.

269 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Ms. Sukanya Pillay).

270 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1125 (Mr. Ziyaad Mia).

271 Ibid., 1205 (Mr. Ziyaad Mia).

272 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1135 (Mr. Michael Karanicolas).

measures that are being taken are appropriate to the needs of the security agencies.”²⁷³ **Mr. Karanicolas, CLD**

- “Consistent with the other efforts that are going on related to oversight of national security generally and across the board, there is no common oversight of any of these 17 organizations, and all of them, apparently, are instrumental in our national security. All those functions should be overseen, probably by a parliamentary committee that has the ability to summon any information they want, and that committee should have absolute visibility into this. There should probably also be an additional committee, like the Security Intelligence Review Committee currently, that has the ability to go in and routinely do audits. It goes in and double-checks that all this is being done, because a parliamentary committee doesn’t necessarily have the manpower to do that on a regular basis.”²⁷⁴ “I would be broadly in favour of oversight over the entire national security and intelligence functions within the Government of Canada, which would include the law enforcement components as well.”²⁷⁵ **Mr. Fraser, Lawyer**
- “OpenMedia hasn’t put forward a formal proposal on what we think the oversight mechanisms should look like. ... To your question of whether there should be oversight within each individual agency, I think there can be that as well in making sure that each department is operating within its purview and making sure the information it receives and shares is being handled appropriately. There is a bigger picture, which Mr. Elder is getting to, which is understanding the big picture and how they all work together, particularly with such top secret information being shared.”²⁷⁶ **Ms. Tribe, OpenMedia**
- “At least from a SCISA perspective, for the 17 institutions that are listed—and for many more, because if put on the disclosing end, it could be any institution that is permitted under SCISA to disclose—I think there needs to be a single body that looks at all of that. I don’t think that takes away from responsibilities within each of those institutions, however. I think there still has to be a clear accountability within each of those institutions to comply as well. We do need an oversight body that can look at the whole picture.”²⁷⁷ **Mr. Elder, CBA**

273 Ibid.

274 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1700 (Mr. David Fraser).

275 Ibid., 1705.

276 Ibid., 1710 (Ms. Laura Tribe).

277 Ibid., 1710 (Mr. David Elder).

6.4 The Role of the Privacy Commissioner

Several witnesses stressed the importance of the work performed by the Privacy Commissioner. Some nevertheless maintained that oversight related to national security should be the responsibility of an agency with solid national security expertise, because there are very specific considerations involved.

CSE Commissioner Plouffe believes that “there is a need for expert review for the 14 institutions not currently subject to review,” and the oversight currently provided by the Privacy Commissioner is inadequate.²⁷⁸

As for the Privacy Commissioner’s role, Mr. Forcese commented that “information sharing is going to be intertwined with operational considerations that are specific to national security, and having a dedicated national security reviewer looking at the information sharing probably is more advantageous than using the Privacy Commissioner.”²⁷⁹ Mr. Roach explained the need for training in the event that the Privacy Commissioner is given the mandate of overseeing information sharing under SCISA:

One of the Arar commission’s recommendations was that some of the people in the RCMP who were sharing information were not adequately trained in national security. If the Privacy Commissioner were to be the sole reviewer of the information sharing, I would also want to see the Privacy Commissioner develop expertise in the particularities of national security sharing, particularly its foreign dimension.²⁸⁰

Likewise, Ms. Pillay commented that “the current mandate of the Privacy Commissioner, while extremely laudable, means that he is constrained, and there is only so much that he can do. To change that mandate would have other implications, and I would rather see an independent reviewer.”²⁸¹ Likewise, Mr. Mia indicated that the Privacy Commissioner “plays an important role because of the privacy protections, but the Privacy Commissioner is not a national security expert.”²⁸² Mr. Karanicolas made similar comments, saying that “there needs to be an independent civilian oversight rather than bundling this into the Privacy Commissioner.”²⁸³

Ms. Austin indicated that her hesitation in “leaving it all up to the Privacy Commissioner is that there are very specific considerations that come up in a national security context that some of these other bodies might have more contextual information on and that would be very useful in reviewing this.”²⁸⁴ She also commented that “the

278 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe).

279 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1155 (Mr. Craig Forcese).

280 Ibid., 1155 (Mr. Kent Roach).

281 Ibid., 1155 (Ms. Sukanya Pillay).

282 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1225 (Mr. Ziyaad Mia).

283 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1135 (Mr. Michael Karanicolas).

284 Ibid., 1135 (Ms. Lisa Austin).

Privacy Commissioner's office has not had a strong mandate with respect to Charter issues."²⁸⁵

6.5 A Parliamentary Review

Several witnesses felt that a parliamentary committee reviewing national security elements, including information sharing, would be useful, but should not replace a specialized oversight agency with expertise in national security.

The Commissioner felt that a parliamentary review would be helpful, but insufficient: "All departments involved in national security also need to be reviewed by independent experts."²⁸⁶ Commissioner Therrien added the following in his brief:

We note that other countries have implemented an oversight model which includes review by a Committee of Parliamentarians, while maintaining review by experts. While the former provides democratic accountability, the latter ensures that in-depth knowledge of the operations of national security agencies and of relevant areas of the law are applied so that rights are effectively protected.²⁸⁷

Mr. Karanicolas of the CLD supported Commissioner Therrien's recommendation.²⁸⁸

Ms. Pillay also felt that the creation "of a parliamentary committee ... is not a substitute for an independent reviewer of national security issues, so the two have to work together."²⁸⁹ Mr. Mia indicated that "other than the committee of parliamentarians, we need to have one unified, arm's-length, well-resourced review agency."²⁹⁰ Mr. Kapoor commented as follows:

There has to be an expert component to it — that is, people who are expert in the area of national security — and there has to be what I would characterize as a parliamentary review, which is the committee of parliamentarians. The committee of parliamentarians is very important because it has democratic legitimacy. It can bring concerns from constituencies to the agencies and can conduct closed hearings as well.²⁹¹

6.6 Resources, Independence of Oversight Agencies and Access to Information

The Privacy Commissioner stressed that adequate resources and independence from the government are two elements that are essential to effective oversight:

In order to be fully effective, review bodies must also be properly resourced. Greatly enhanced national security activities and initiatives in recent years have resulted in much

285 Ibid.

286 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1100 (Mr. Daniel Therrien).

287 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

288 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1110 (Mr. Michael Karanicolas).

289 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1220 (Ms. Sukanya Pillay).

290 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1225 (Mr. Ziyaad Mia).

291 Ibid., 1230 (Mr. Anil Kapoor).

heightened public concerns about privacy, including mass surveillance, but without any consequential increase in funding for the oversight bodies. For the OPC's part, it has been forced to risk manage its limited resources, moving efforts from other mandated activities. This is less than ideal. It is also insufficient to produce effective review and privacy oversight, which are essential to maintain trust in national security activities.

The OPC's research on oversight of security and intelligence agencies has led it to determine that, beyond resourcing, effective review requires meaningful independence from the executive, non-partisanship and institutional expertise, with knowledge of both domestic and international standards and law.²⁹²

Several other witnesses also stressed the importance of the oversight agency being independent and having adequate resources.²⁹³

Mr. Forcese explained that even if an oversight agency is well resourced, it cannot fully audit all the activities of an institution. There will have to be a triage in order to determine priorities.²⁹⁴

Finally, several witnesses indicated that the independent oversight agency must have access to information to fulfill its oversight mandate.²⁹⁵

6.7 Record-Keeping

On the one hand, the Office of the Privacy Commissioner of Canada noted that

record-keeping is an essential prior condition to effective review. The OPC's advice to Public Safety in the context of the SCISA Deskbook was clear on this point: it called for guidance on the content of records that should be kept, including a description of the information shared and the rationale for disclosure.²⁹⁶

Likewise, Mr. Elder of the Canadian Bar Association stated as follows:

Whatever oversight mechanism is pursued, in order to better facilitate the review of activities carried out under SCISA, the CBA submits that regulations should be introduced requiring disclosing institutions to keep a record of all disclosures made under SCISA and requiring receiving institutions to maintain records of subsequent use and disclosure of information received pursuant to SCISA. If such records do not exist, it will be nearly impossible for any oversight body to determine whether the guiding principles of the Act are indeed being respected.²⁹⁷

292 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety](#), 5 December 2016.

293 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1225 (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder); 1700 (Ms. Laura Tribe).

294 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1240 (Mr. Craig Forcese).

295 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1645 (Mr. David Elder); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1140 (Mr. Michael Karanicolas).

296 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

297 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder).

Ms. Tribe of OpenMedia pointed out that “all government institutions should be required to keep thorough records of when they disclose our private information, including to foreign governments.”²⁹⁸

Similarly, when he appeared before the Committee, Mr. Evans of the CRCC mentioned that the O’Connor report contained recommendations on record-keeping: “For example, Justice O’Connor’s report stressed that information-sharing agreements or arrangements pertaining to integrated national security operations should be reduced to writing. This is important, and the Commission will be examining whether the RCMP adheres to this recommendation with respect to information sharing relating to the *Security of Canada Information Sharing Act*.”²⁹⁹

Moreover, as mentioned previously in the report, the manner of consigning what constitutes a “disclosure” within the meaning of SCISA does not seem to be defined. In fact, there did not seem to be an established standard determining whether a disclosure could involve information pertaining to more than one individual.³⁰⁰

6.8 The View of Federal Institutions

According to Mr. Burt of DND, mechanisms already exist that govern his institution in the exercise of its powers:

We’re subject to the oversight of the Commissioner himself, the Office of the Information Commissioner and the Auditor General. We also have an ombudsman in the Department of National Defence. In terms of counter-intelligence, we have a judge advocate general committee consisting of lawyers who work internally and of external organizations that specifically monitor our counter-intelligence capacity. I’m fairly confident about the mechanisms that govern us to ensure compliance with the legislation and policies under which we operate.³⁰¹

Similarly, Mr. Roussel of Transport Canada told the Committee that his institution was “already subject to a complete set of extremely strict verifications by both the Auditor General and the Privacy Commissioner.”³⁰²

Ms. Whelan of the RCMP specified that her organization “has also established processes to maintain statistics on disclosures made to and by the RCMP under the Act, including what was disclosed, who disclosed it, and when it was disclosed,”³⁰³ and that “all

298 Ibid., 1540 (Ms. Laura Tribe).

299 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1125 (Mr. Richard Evans).

300 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1645 (Mr. Glen Linder); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1130 and 1145 (Hon. Pierre Blais); 1100 and 1145 (Mr. Richard Evans).

301 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1655 (Mr. Stephen Burt).

302 Ibid., 1655 (Mr. Donald Roussel).

303 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1215 (Ms. Alison Whelan).

correspondence related to SCISA must be documented in the RCMP's secure records management system as well."³⁰⁴

6.9 The Committee's Recommendations

In light of the evidence, the Committee recommends:

Recommendation 7

That the Government of Canada strengthen the oversight of information sharing by Government of Canada institutions, by considering the following options:

a) establishing a super-agency to provide expert oversight that would review all information-sharing activities by federal national security institutions;

b) establishing new oversight bodies, where there are existing gaps, such as the Canada Border Services Agency, capable of cooperating to review information sharing between federal institutions pursuant to the *Security of Canada Information Sharing Act*;

c) conferring new powers upon the Security Intelligence Review Committee, the Office of the Communications Security Establishment Commissioner, the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police, and the Privacy Commissioner of Canada that would enable them to:

- i. oversee information sharing among the 14 Government of Canada institutions listed in Schedule 3 to the *Security of Canada Information Sharing Act* as well as their use of information; and**
- ii. cooperate with other agencies and conduct joint investigations;**

d) establishing a parliamentary review mechanism³⁰⁵ that, on a complementary basis with one or several other expert oversight

304 Ibid.

305 At the time of writing of the report, [Bill C-22, An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts](#), was at the report stage in the House of Commons. Several witnesses made reference to this bill. See: ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1200 (Ms. Sukanya Pillay); 1220 and 1245 (Mr. Craig Forcese); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1245 (Mr. Wesley Wark); 1250 (Mr. Tamir Israel); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1235 (Mr. Ziyaad Mia); 1240 (Mr. Anil Kapoor); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1550 (Mr. David Elder); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1100 (Mr. Daniel Therrien).

agencies, would review the information-sharing activities of federal national security institutions;

e) conferring upon the Privacy Commissioner of Canada the role of overseeing the information sharing of the 14 Government of Canada institutions listed in Schedule 3 to the *Security of Canada Information Sharing Act* as well as their use of information, and that the Privacy Commissioner report his or her findings to Parliament.

Recommendation 8

That the Government of Canada amend the *Security of Canada Information Sharing Act* to impose on federal institutions and on the recipient institutions listed in Schedule 3 to the Act a legal duty to keep records in order to report on any use or subsequent sharing of information provided to them under the Act.

CHAPTER 7: PRIVACY SAFEGUARDS

During the study, several witnesses indicated that there is no binding provision in SCISA to protect the privacy of Canadians.³⁰⁶ Several witnesses felt that the Act should include a number of privacy safeguards, particularly with respect to information reliability, information-sharing agreements, privacy impact assessments (PIAs), and the retention and deletion of personal information.³⁰⁷ In fact, several witnesses told the Committee that errors in information sharing can cause grave injustices and serious harm to Canadians.³⁰⁸

SCISA does, however, contain guiding principles which are set out in section 4 as follows:

4 Information sharing under this Act is to be guided by the following principles:

- (a) effective and responsible information sharing protects Canada and Canadians;
- (b) respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing;
- (c) entry into information-sharing arrangements is appropriate when Government of Canada institutions share information regularly;
- (d) the provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing; and
- (e) only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive information that is disclosed under this Act.

Privacy Commissioner Therrien, however, pointed out that there is nothing binding about these principles:

There is a reference in the preamble to SCISA that says, among other things, that information sharing should occur responsibly. That's advice given by Parliament to departments, and I'm sure this advice in the preamble will lead to certain actions within the public service. However, it's left completely to the public service to determine what kind of controls or governance structure they will put in place to live by this principle of responsible information sharing. We don't need to be overly prescriptive, but I think there

306 Ibid., 1125 (Ms. Sukanya Pillay); Ibid., 1210 (Mr. Wesley Wark); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1120 (Ms. Lisa Austin); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1125 (Mr. Craig Forcese); Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

307 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1110 (Mr. Jean-Pierre Plouffe).

308 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1125 (Ms. Sukanya Pillay).

need to be some high-end controls, safeguards, and governance mechanisms to ensure that this broad authority given by Parliament is exercised responsibly.³⁰⁹

In this regard, the “[Canadian Bar Association] recommends that SCISA include effective mechanisms to enforce the principles outlined in section 4.”³¹⁰

In his appearance before the Committee, Mr. Davies stated that “each institution is responsible for how they implement SCISA.”³¹¹ He added, however, that

Public Safety's role is to help institutions understand the Act. To that end, we create guidance on SCISA. We've conducted information sessions for government officials and we released a framework to guide SCISA's implementation. We continue to provide support to government departments and agencies, as required, and are looking to improve the guidance we provide, including addressing the issues raised recently by the Privacy Commissioner in his annual report.³¹²

Moreover, several representatives of federal institutions explained to the Committee the various privacy safeguards that had been put in place within their organizations, such as policies and directives, as well as training.³¹³

In light of the testimony, the Committee recommends:

Recommendation 9

That the Government of Canada amend the *Security of Canada Information Sharing Act* in order that the guiding principles listed in section 4 become legal obligations.

7.1 Reliability of Shared Information

As mentioned above, the reliability of information can have severe implications for individuals. According to Mr. Roach, SCISA should put more emphasis on information reliability:

Justice O'Connor in the Arar commission report stressed that there need to be assurances that the reliability of the information is discussed, and also the respect for caveats, which is mentioned in section 4.

309 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1125 (Mr. Daniel Therrien); *Ibid.*, 1110 (Mr. Kent Roach).

310 Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

311 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1215 (Mr. John Davies).

312 *Ibid.*

313 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1605 (Mr. Stephen Burt); 1605 (Mr. Dominic Rochon); 1610 (Ms. Marie-France Paquet, Director General, Intermodal Surface, Security and Emergency Preparedness, Safety and Security Group, Department of Transport); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1600 and 1605 (Mr. David Drake); *Ibid.*, 1230 (Mr. Robert Mundie).

The problem with section 4 right now is simply that principles are placed out there, but there are no teeth, unless there's a requirement for protocols through regulations or through amendments of the statutes.³¹⁴

Similarly, Mr. Elder of the CBA argued:

The Arar commission stressed the importance of precautions to ensure that information is accurate and reliable before it is shared. Omitting safeguards in SCISA ignores lessons learned through the Arar saga and the recommendations of the Arar commission, and risks repeating the same mistakes.³¹⁵

Indeed, Mr. Elder specified that the CBA's concern "stems from the tragic case of Maher Arar. From information that turned out to be inaccurate and that may not have been adequately vetted before being handed off to foreign governments, we wound up with a Canadian citizen being detained and tortured, with all kinds of horrible things. That's really the worst-case scenario, and it's a great reason for being really careful with the information we're sharing."³¹⁶ Hence, the "CBA recommends that SCISA include safeguards to ensure that any shared information is reliable."³¹⁷

For Mr. Mia and Mr. Kapoor, the test of whether information is "necessary" would make it possible to obtain more-reliable information.³¹⁸ Mr. Kapoor indicated that "the 'necessary' test would impose some rigour that at least has the prospect of doing so more efficiently than a relevancy test would."³¹⁹ Mr. Mia added that this would reduce the risk of making mistakes.³²⁰ In addition, Mr. Mia feels that controls also have a role to play in ensuring the reliability of shared information.³²¹

In light of the evidence, the Committee recommends:

Recommendation 10

That the Government of Canada amend the *Security of Canada Information Sharing Act* by creating a legal obligation to ensure the reliability of any shared information.

314 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1110 (Mr. Kent Roach).

315 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1555 (Mr. David Elder).

316 Ibid., 1645.

317 Canadian Bar Association, [Security of Canada Information Sharing Act \(SCISA\)](#), January 2017.

318 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1205 (Mr. Ziyaad Mia); 1200 (Mr. Anil Kapoor).

319 Ibid., 1200 (Mr. Anil Kapoor).

320 Ibid., 1205 (Mr. Ziyaad Mia).

321 Ibid.

7.2 Retention, Deletion and Correction of Information

As mentioned above, Privacy Commissioner Therrien is of the opinion that SCISA should include “some high-end controls, safeguards, and governance mechanisms”³²² to ensure that this new information-sharing authority is exercised responsibly. More specifically, with regard to the retention of information, the Commissioner feels that “[i]t should not be for the bureaucracy to decide how long they are going to keep the information”³²³ and that “[t]here should be rules of law on this.”³²⁴ The Commissioner explained that this means the recipient institutions listed in Schedule 3 to SCISA should be required to delete information:

If the government maintains that the sharing of information about ordinary citizens (such as travellers or taxpayers) to one or more of the 17 recipient institutions under SCISA is necessary to undertake analyses meant to detect new threats, national security agencies should be required to dispose of that information immediately after these analyses are completed and the vast majority of individuals have been cleared of any suspected terrorist activities. This would be in keeping with the recent judgment of the Federal Court which held that retention of “associated data” for people who are not a threat to national security was illegal.³²⁵

Mr. Therrien also pointed out that a “receiving institution must determine whether it has the authority to collect [information], to receive it,” and that if it receives information it does not have the authority to collect, it should be required to delete the extra information.³²⁶

Several witnesses also noted the importance of clear rules on information retention, in particularly with respect to how long information should be retained before it must be deleted.³²⁷ To support their arguments, some also made reference to the recent Federal Court decision³²⁸ in which CSIS was found to have retained data illegally.³²⁹

Mr. Israel of CIPPIC stated that his organization “would suggest that the remedying of this lack of retention obligation would be best achieved through overarching amendments to the *Privacy Act* that would apply across all of government and impose an overarching retention obligation.”³³⁰ Mr. Israel noted that several institutions set their own limits on information retention while others have limitations set for them by law, “but an

322 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1125 (Mr. Daniel Therrien).

323 Ibid.

324 Ibid.

325 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

326 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1115 (Mr. Daniel Therrien); [X \(Re\)](#), 2016 FC 1105.

327 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1125 (Mr. Craig Forcese); Ibid., 1225 (Mr. Tamir Israel).

328 [X \(Re\)](#), 2016 FC 1105.

329 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1225 (Mr. Tamir Israel).

330 Ibid.

overarching retention limitation in the *Privacy Act* would provide for a more principled and across-the-board process.”³³¹

Mr. Mia of the CMLA also argued that when the government gathers information as part of a national security investigation, that information should be expunged as soon as the government determines that the individual under investigation is not a suspect.³³² He added that this would help reduce the size of databases and avoid errors.³³³ However, Mr. Kapoor disagreed with Mr. Mia on this point for the following reason:

To the extent that the service [CSIS] properly receives — and I underscore “properly” — information about national security threat information, I don't think it's wise for the service to destroy it. I don't think it's wise. Today it may not mean much, but 10 years from now or five years from now, when circumstances change and you're continually revising your analytics, you need to have a rich environment to be able to stay on top of the threat environment.”³³⁴

Currently at CSE, information gathered that does not meet the criteria set out in the *National Defence Act* is destroyed.³³⁵ Mr. Blais, Chair of SIRC, told the Committee that the recent decision by the Federal Court indicated “that they have to review all the documents on a regular basis to make sure that they don't keep that data too long, or for a period that will not be considered strictly necessary.”³³⁶ Mr. Roussel of the Department of Transport stated that his organization did not gather personal information as such, but rather used information from other institutions and that a policy governed the retention of information.³³⁷ Mr. Linder specified that as far as IRCC is concerned, “[I]f we receive information in error or information that's not relevant, the guidelines we have within the department are that the information must be destroyed immediately.”³³⁸

Mr. Picard of the Department of Foreign Affairs, Trade and Development indicated that, to his knowledge, the standard for retention of information that is collected legitimately is “a minimum of two years.”³³⁹ Mr. Burt of the Department of National Defence pointed out that the information gathered by his institution did not necessarily touch on individuals and sometimes needed to be databased for quite a long time to allow for cross-checking.³⁴⁰ He added that “there is no formal process around how long you can keep [operational information]. The goal is to database it usefully so that you have good information to look

331 Ibid., 1255.

332 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1205 (Mr. Ziyaad Mia).

333 Ibid.

334 Ibid., 1210 (Mr. Anil Kapoor).

335 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1155 (Mr. Jean-Pierre Plouffe).

336 Ibid., 1200 (Hon. Pierre Blais).

337 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1615 (Mr. Donald Roussel).

338 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1700 (Mr. Glen Linder).

339 Ibid., (Mr. Patrick Picard, Director, Access to Information and Privacy, Department of Foreign Affairs, Trade and Development).

340 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1620 (Mr. Stephen Burt).

back upon.”³⁴¹ Mr. Rochon of CSE specified that his organization has “retention periods for most of the collection of information that we have. We have ministerial directives that impose those retention periods. We follow them and they are reviewed by our commissioner to make sure that we adhere to them.”³⁴²

Mr. Wark pointed out that retention mechanisms currently exist, sometimes in the form of ministerial directives.³⁴³ He stated that “some of those ministerial directives around retention of information could be made public without endangering national security to reassure the Canadian public that information is not being kept in an abusive and overly long way.”³⁴⁴

Regarding the correction of information and problems linked to the sharing of inaccurate information, CSE Commissioner Jean-Pierre Plouffe indicated that one of the ways to reduce risks associated with the inaccuracy of shared information “would be to incorporate into the Act a provision that any information that is not relevant, which is the threshold used presently in the Act, should be destroyed. This is not built into the act right now. In my view, that's a problem.” Mr. Plouffe went on to state that it would be possible to add to section 10 of SCISA, “which talks about regulations that could be made by the Governor in Council. They have three ways to make regulations. I would add a fourth one, which should read ‘destruction of information that is not relevant.’ If you have a built-in provision to the effect that if it's not relevant, it is to be destroyed within a certain time, I think you would avoid the problem you just raised.”³⁴⁵ Mr. Evans of the CRCC noted that one way to reduce risks associated with the sharing of inaccurate information would be to institute better practices and have internal oversight mechanisms.³⁴⁶ Lastly, Mr. Blais, Chair of SIRC, specified that CSIS uses corroboration to verify the accuracy of information.³⁴⁷

Regarding oversight of the new information-sharing powers conferred by SCISA, CSE Commissioner Plouffe and Mr. Blais, Chair of SIRC, both felt that “review bodies” should not have the power to compel the 17 recipient institutions listed in Schedule 3 to delete information.³⁴⁸

In light of the evidence, the Committee recommends:

341 Ibid.

342 Ibid., 1620 (Mr. Dominic Rochon).

343 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1250 (Mr. Wesley Wark).

344 Ibid.

345 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1140 (Mr. Jean-Pierre Plouffe).

346 Ibid., 1145 (Mr. Richard Evans).

347 Ibid., 1145 (Hon. Pierre Blais).

348 Ibid., 1245 (Hon. Pierre Blais); 1245 (Mr. Jean-Pierre Plouffe).

Recommendation 11

That the Government of Canada amend section 10 of the *Security of Canada Information Sharing Act* to confer upon the Governor in Council the power to make regulations concerning the correction and deletion of information and that the Governor in Council make regulations regarding the correction, deletion and retention of information.

7.3 Information-Sharing Arrangement

One of the guiding principles set out in section 4 of SCISA is as follows: “entry into information-sharing arrangements is appropriate when Government of Canada institutions share information regularly.”

According to the Privacy Commissioner, there is a “need for an explicit requirement for written information agreements.”³⁴⁹ He added that

[e]lements addressed in these Agreements should include, as a legal requirement, the specific elements of personal information being shared; the specific purposes for the sharing; limitations on secondary use and onward transfer; and other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures.³⁵⁰

Commissioner Therrien also specified that “OPC should also be given explicit authority to review and comment, and the right to review existing agreements on request by OPC to assess compliance. Finally, departments should be required to publish the existence and nature of information-sharing agreements between departments or with other governments.”³⁵¹

Ms. Pillay explained that if there are no information-sharing agreements between the institution disclosing information and the recipient institution regarding limitations on how information can be used and who it can subsequently be shared with, the institution disclosing such information loses all control over it.³⁵² Ms. Tribe of OpenMedia also emphasized that information sharing under SCISA should be done within the context of arrangements.³⁵³ Ms. Austin pointed out that written agreements “were very key to the Arar commission report.”³⁵⁴ Mr. Forcese also indicated that putting in place information-sharing protocols “that mitigate the spread of information through government agencies is

349 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

350 Ibid.

351 Ibid.

352 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1125 (Ms. Sukanya Pillay).

353 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1540 (Ms. Laura Tribe).

354 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1120 (Ms. Lisa Austin).

probably the best we can do, coupled with effective auditing thereafter to ensure compliance and conformity with those dictates.”³⁵⁵

Mr. Pierre Blais, Chair of SIRC, underscored the importance of information-sharing agreements, noting that, in reviewing such agreements, his organization “will be attentive to these formalized agreements, where much of the work of determining the precise balance of security and privacy concerns will inevitably take place.”³⁵⁶

Mr. Burt of the Department of National Defence told the Committee that his organization did not have any formal information-sharing agreements under SCISA.³⁵⁷ However, other institutions did indicate that new arrangements had been entered into since SCISA was enacted. For instance, Ms. Geddes of CSIS specified that CSIS has signed a new arrangement with Global Affairs Canada that integrates SCISA.³⁵⁸ Mr. Drake of Global Affairs Canada also indicated that his organization had concluded an information-sharing arrangement with CSIS pursuant to SCISA.³⁵⁹

In light of the evidence, the Committee recommends:

Recommendation 12

That the Government of Canada amend the *Security of Canada Information Sharing Act* so as to:

- a) make it a duty for recipient institutions to enter into information-sharing arrangements with disclosing institutions; and**
- b) confer upon the Privacy Commissioner of Canada the power to review and comment on all existing or future information-sharing arrangements.**

7.4 Privacy Impact Assessments

During the hearings, various witnesses emphasized the importance of PIAs as a means of protecting privacy.

In his submission, Commissioner Therrien emphasized the importance of PIAs:

An additional tool to determine whether government initiatives involving the use of personal information raise privacy risks is the Privacy Impact Assessment (PIA), which describes and quantifies these risks, and proposes solutions to eliminate or mitigate them to an acceptable level. At the federal level, the obligation to conduct PIAs is currently at

355 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1125 (Mr. Craig Forcese).

356 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 8 December 2016, 1115 (Hon. Pierre Blais).

357 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 2 February 2017, 1700 (Mr. Stephen Burt).

358 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1230 (Ms. Tricia Geddes).

359 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 7 February 2017, 1605 (Mr. David Drake).

the policy level, and is triggered by a new or substantially modified program or activity. Despite this policy obligation, the OPC was concerned to see how few PIAs were undertaken in relation to SCISA.³⁶⁰

In fact, a survey conducted by the OPC on the implementation of SCISA revealed that 12 of the 17 institutions authorized to collect information under the Act “had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary,”³⁶¹ and two of these institutions determined that PIAs were necessary and had begun to develop them.³⁶²

Mr. Davies of the Department of Public Safety and Emergency Preparedness told the Committee that “departments and agencies must also continue to abide by government requirements. These include the Treasury Board Directive on Privacy Impact Assessment.”³⁶³ He added that the “Minister of Public Safety has also written to his colleagues regarding the importance of completing PIAs when required.”³⁶⁴

Commissioner Therrien indicated that he was concerned by the results of his survey regarding PIAs. He was “encouraged by what the Minister said [concerning PIAs], but it has not translated into [OPC] receiving anything [in the way of PIAs] at this point.”³⁶⁵

Mr. Israel of CIPPIC suggested that “other overarching safeguards that could be adopted within the *Privacy Act* could provide additional safeguards and a better framework for legitimate information within a modified and reduced SCISA. These safeguards could include the adoption of privacy impact assessments and a more robust enforcement of the *Privacy Act*.”³⁶⁶

360 Office of the Privacy Commissioner of Canada, [Submission of the Office of the Privacy Commissioner of Canada to the National Security Policy Directorate of Public Safety Canada](#), 5 December 2016.

361 Ibid., [2015–2016 Annual Report to Parliament on the Personal Information and Electronic Documents Act and the Privacy Act](#), September 2016.

362 Ibid.

363 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1215 (Mr. John Davies).

364 Ibid.

365 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 22 November 2016, 1135 (Mr. Daniel Therrien).

366 Ibid., 1225 (Mr. Tamir Israel).

CHAPTER 8: PROTECTION FROM CIVIL PROCEEDINGS PROVIDED UNDER SECTION 9 OF THE SECURITY OF CANADA INFORMATION SHARING ACT

During the study, several witnesses drew the attention of Committee members to section 9 of SCISA, which reads as follows: “No civil proceedings lie against any person for their disclosure in good faith of information under this Act.”³⁶⁷ Some felt that the implications of this section were worrisome.³⁶⁸ To illustrate the consequences of immunity from civil proceedings, some witnesses drew a parallel between section 9 of SCISA and the case of Maher Arar, a Canadian who was subjected to torture, in particular because of inaccurate shared information.³⁶⁹ In fact, some witnesses pointed out that section 9 of SCISA actually prevented Canadians who suffered harm because of information shared under SCISA from obtaining compensation.³⁷⁰

Ms. Austin stated that a “provision that there is no recourse for those who are abused undermines the trust of Canadians.”³⁷¹ Mr. Fraser added that if “a statute has to provide immunity for otherwise unlawful conduct, we should be very careful about authorizing that conduct in the first place and we should be very careful about granting that immunity.”³⁷² Also, according to Mr. Mia, “[s]ection 9 says that when someone shares information and it harms a Canadian or some person — but let's say a Canadian, as in the Arar case — they're immune from paying out compensation or being sued for it.”³⁷³ Similarly, Mr. Roach noted in reference to section 9 of SCISA:

Not only does this raise the spectre of allowing the sort of information sharing that harmed Maher Arar and many other people, but it also puts yet another barrier to getting civil compensation should information sharing — and in particular I would stress information sharing about security threats — impose harm on people who may very well want to seek compensation for it and who may very well want to restore their reputation.³⁷⁴

In her appearance before the Committee, Ms. Sheppard of the Department of Justice explained why section 9 was included in SCISA:

367 SCISA, s. 9.

368 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1115 (Mr. Kent Roach); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1145 and 1225 (Mr. Ziyaad Mia); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1155 (Ms. Micheal Vonn); 1200 (Ms. Lisa Austin); ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1605 (Mr. David Fraser).

369 Ibid. (Mr. Kent Roach); Ibid., 1145 and 1225 (Mr. Ziyaad Mia); Ibid. 1225 (Ms. Lisa Austin).

370 Ibid. (Mr. Kent Roach); Ibid. (Mr. Ziyaad Mia); Ibid. (Ms. Lisa Austin).

371 Ibid. 1200 (Ms. Lisa Austin).

372 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 31 January 2017, 1605 (Mr. David Fraser).

373 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1145 (Mr. Ziyaad Mia).

374 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1115 (Mr. Kent Roach).

When we decided to include it, we consulted with operating agencies and departments, which revealed that some civil servants were reluctant to lawfully share information because they were afraid they would be found personally liable in terms of committing a criminal act for disclosing information. It was really done to help allay anxiety and to encourage responsible disclosure, charter-compliant disclosure.

The provision is there to inform public servants that they will be protected from civil liability if they disclose information in good faith, and that's why it was included. It shields individuals. It was not ever intended to shield the crown from immunity, and that may be something that people don't understand.

Individuals who are adversely affected by sharing could begin civil liability proceedings against the crown, which could be found vicariously liable for the actions of its employee, but it wouldn't protect them from criminal liability if they maliciously shared information.³⁷⁵

For his part, the Privacy Commissioner, in a written response to the Committee dated 5 December 2016, stated the following:

While you may wish to consult with the Department of Justice, which has the most relevant expertise in this area, it is our view that the Crown would likely be protected from civil suit by section 9. The Crown can only be liable in tort through the tortious acts of its servants. If a statutory immunity clause relieves individual Crown servants of liability, the Crown cannot be vicariously liable for their actions unless the immunity clause expressly preserves the Crown's potential liability.

Mr. Mia noted that the immunity provided under section 9 included the Crown, and he was concerned about the fact that “you can be negligent and act in good faith as well.”³⁷⁶ As well, Ms. Vonn specified that she “certainly read the clause as one in which the Crown was waiving its own liability, and not civil servants,”³⁷⁷ and that “[i]f failure to achieve clarity in that clause was evident to us,”³⁷⁸ she believed it would “be evident to most Canadians.”³⁷⁹ Ms. Austin also told the Committee, “I would add that because the word ‘person’ is there, I would automatically assume it includes the Crown. If it's not meant to include the Crown, it would be a useful amendment to say that the Crown can be liable.”³⁸⁰ She also added that “it seems useful to keep some provision to say that a good-faith interpretation of this isn't going to get you into trouble,”³⁸¹ as for example in the case of a “civil servant who is worried about misjudging that line in terms of sharing information.”³⁸²

For Mr. Kapoor, section 9 “is just an indemnification issue. The government has to be responsible for mistakes. ... Just by indemnification, the government can solve this

375 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 17 November 2016, 1240 (Ms. Ann Sheppard).

376 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1145 (Mr. Ziyaad Mia).

377 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1225 (Ms. Micheal Vonn).

378 Ibid.

379 Ibid.

380 Ibid., 1225 (Ms. Lisa Austin).

381 Ibid.

382 Ibid.

problem so that they're not hung out to dry. From my perspective, we can get rid of this provision and have proper indemnification agreements.”³⁸³

Mr. Roach said he “would favour simply deleting section 9 of SCISA.”³⁸⁴ He added that it would be preferable to leave it up to the courts to decide whether a person can obtain compensation.³⁸⁵

In light of the evidence, the Committee recommends:

Recommendation 13

That the Government of Canada amend section 9 of the *Security of Canada Information Sharing Act* to make it clear and unequivocal that:

- a) only employees acting in good faith in the performance of their duties are immune from civil proceedings; and**
- b) the Crown remains liable for the actions of its employees.**

383 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1225 (Mr. Anil Kapoor).

384 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1145 (Mr. Kent Roach).

385 *Ibid.*, 1110.

CHAPTER 9: CONSIDERATION OF THE COMMISSION OF INQUIRY INTO THE AIR INDIA BOMBING

Mr. Forcese, Mr. Roach, Mr. Kapoor and Ms. Austin³⁸⁶ pointed out that SCISA fails to implement a key recommendation of the report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, which had brought to light the serious consequences that can arise when not enough information is shared.³⁸⁷ In fact, as Mr. Roach and Mr. Forcese noted in their brief:

The Air India commission recognized this, and urged that the CSIS Act “should be amended to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor.”

The government ignored this recommendation — and despite the occasional puzzling government claims to the contrary, Bill C-51 did not honour it. Instead, Bill C-51 responded to legitimate concerns about siloed information, so evident in the Air India investigation, by throwing wide open the barn doors on information-sharing but in such a complex and unnuanced way that the only certain consequence will be less privacy for Canadians.³⁸⁸

Mr. Kapoor, who served as counsel to the Air India commission, told the Committee that “[t]he infrastructure problems and the lack of coordination that we saw in Air India have to a large extent been ameliorated by changes in the way in which the RCMP and [CSIS] deal with each other on a regular basis.”³⁸⁹ Mr. Forcese explained the reason why CSIS was reluctant to share information with the RCMP:

That has to do with what is known as “intelligence to evidence”. CSIS is concerned that if it shares information with the RCMP, that sensitive information will be disclosable in court because of the scope of our *Criminal Code* and charter disclosure rules. It has nothing to do with this law. It has to do with the way we’ve structured this intelligence-to-evidence conundrum.

That is the reason the Air India commission recommended that there be a proviso putting in place a system for CSIS to disclose to a third party — they proposed a national security adviser — who would decide whether that information should be prioritized for intelligence purposes or for evidentiary purposes in a criminal trial. CSIS would not be making the decision at the end of the day. Someone outside CSIS would ensure that if there was a need for use in a criminal trial, it would be available.³⁹⁰

386 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 13 December 2016, 1150 (Ms. Lisa Austin).

387 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 3 November 2016; ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1130 (Mr. Anil Kapoor).

388 Ibid., Craig Forcese and Kent Roach.

389 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1245 (Mr. Anil Kapoor, Barrister).

390 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 3 November 2016, 1200 (Mr. Craig Forcese).

Mr. Roach and Mr. Forcese made a clear recommendation in this regard: “Implement Recommendation 10 of the Air India inquiry to establish legislated rules in the *CSIS Act* requiring CSIS to ‘report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor.’”³⁹¹ Mr. Mia of the CMLA also told the Committee that “we maybe need to look at new legislation ... and some requirement for the agencies to work together.”³⁹²

In light of the evidence, the Committee recommends:

Recommendation 14

That the Government of Canada implement recommendation 10 made by the Commission of Inquiry into the Air India tragedy by amending the *Canadian Security Intelligence Service Act* to require the Canadian Security Intelligence Service to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the national security advisor.

391 Craig Forcese and Kent Roach, Brief, [Analysis and Proposals on the Security of Canada Information Sharing Act](#), 3 November 2016.

392 ETHI, [Evidence](#), 1st Session, 42nd Parliament, 6 December 2016, 1240 (Mr. Ziyaad Mia).

APPENDIX A CORRESPONDENCE



Canada Revenue Agency Agence du revenu
du Canada

Commissioner Commissaire

Ottawa, Canada
K1A 0L5

JAN 20 2017

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
6th Floor
131 Queen Street
Ottawa ON K1A 0A6

Dear Mr. Calkins:

I would like to thank you for your letter dated December 13, 2016, concerning the Standing Committee on Access to Information, Privacy and Ethics' study of the Security of Canada and Information Sharing Act (SCISA).

You have indicated that the Committee is seeking clarification on the role of the Canada Revenue Agency (CRA) with regards to the SCISA, including how its mandate relates to national security and how it views its responsibilities under the SCISA as a recipient institution.

Through its role as the federal regulator of charities, the CRA is responsible for ensuring that the tax incentives reserved for charities are only made available to organizations that operate for exclusively charitable purposes and that charitable funds and services reach intended, legitimate beneficiaries. This includes protecting the integrity of the charity registration system from the risk of terrorist abuse. It is because of this national security mandate that the CRA has been listed as a recipient institution.

As a recipient institution, the CRA may only receive charity related information in support of its national security mandate to protect the charity registration system from abuse by individuals or groups with links to terrorism. This information is solely used to assist the CRA in assessing the level of risk posed by applicant or registered charities, and in choosing the most appropriate course of administrative action, such as refusing to register an organization as a charity, imposing sanctions and penalties, or revoking charitable status. The CRA abides by government and legal

.../2

Tel. – Tél. : 613-957-3688
Fax – Télécopieur : 613-952-1547
www.cra-arc.gc.ca

Canada

requirements governing the security and confidentiality of the information it receives and has comprehensive internal systems in place to protect it. The CRA has updated policies and procedures to provide clear guidelines on the usage, storage, retention, and recordkeeping of the information it receives.

In addition to receiving information as a recipient institution, the CRA is also permitted to share any taxpayer information, for national security purposes, with other recipient institutions within the limits set out in the Income Tax Act (ITA), the Excise Tax Act (ETA) and the Excise Act, 2001 (EA, 2001).

While the CRA was previously authorized to share certain charity related information with the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and the Financial Transactions and Reports Analysis Centre, amendments to the ITA, the ETA, and the EA, 2001 resulting from Bill C-51 (assented to on June 18, 2015) now allow it to disclose any taxpayer information to any of the recipient institutions listed in Schedule 3 of the SCISA. As per the ITA, the ETA, and the EA, 2001, information may only be disclosed when it is relevant to an investigation of a threat to the security of Canada or an investigation of a terrorism offence. In addition, as per the intent of the SCISA, the CRA will only share information when it is also relevant to the receiving institution's national security responsibilities. The CRA retains control over the decision to share information.

Should you require additional information, please do not hesitate to contact me or Mr. Geoff Trueman, Assistant Commissioner, Legislative Policy and Regulatory Affairs Branch, at 613-670-9550.

Sincerely,



Bob Hamilton



Canadian Food
Inspection Agency
President
Ottawa, Ontario
K1A 0Y9

Agence canadienne
d'inspection des aliments
Président
Ottawa (Ontario)
K1A 0Y9

JAN 19 2017

PRC 017973

Mr. Blaine Calkins, MP
Chair, Standing Committee on Access to
Information, Privacy and Ethics
House of Commons
Ottawa, Ontario

Dear Mr. Calkins:

Thank you for your letter of December 13, 2016 regarding the interests of the Standing Committee on Access to Information, Privacy and Ethics with respect to the Canadian Food Inspection Agency (CFIA) and its role under the administration of the *Security of Canada Information Sharing Act* (SCISA). I am happy to provide the Committee with clarification of the CFIA's mandate in regards to national security.

First, I would like to stress that the CFIA is committed to carrying out its responsibilities to Canadians while protecting the privacy rights of individuals, including safeguarding the confidentiality of information provided by individuals and institutions consistent with our obligations under the *Privacy Act* and related Treasury Board policies and directives.

With respect to the CFIA's mandate, the Agency is an integral part of the federal government's capacity to respond rapidly and effectively to national security in the event of a food safety emergency or a threat to agricultural or forest biosecurity. These threats might include bioterrorism or agro-terrorism (terrorism directed towards Canada's agricultural resource base). The CFIA surveillance, detection and inspection programs are designed to identify these threats and detect the presence of hazards such as contaminants, diseases or pests whether in food, animals and plants or their products. As well, the CFIA provides early warning to Canadians of risks arising from the presence of these hazards.

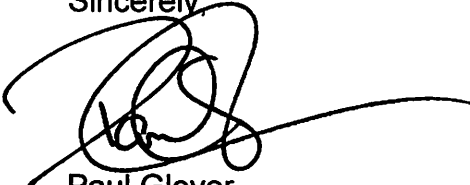
While the CFIA's mandate is to protect Canadians (human health) and Canada's natural resources (animal and plant health), it does so in partnership with federal institutions from which it might receive information to identify a risk or manage a threat. The sharing of information assists the CFIA in fully delivering its mandate. The information shared with federal institutions (i.e. collect, use, retain and further disclose) may include personal information to which the CFIA has obligations under the *Privacy Act*.

Canada

It is clear to the Agency that being identified as a recipient institution under SCISA does not preclude the CFIA of its obligations under the *Privacy Act*. To that effect, the CFIA has assessed that it will not be necessary to undertake a Privacy Impact Assessment as it does not foresee changes or modifications to its systems or initiatives, nor does it foresee an increase in the collection, use or disclosure of personal information under SCISA.

With respect to the CFIA's responsibilities under the SCISA, the President of the CFIA is responsible to receive information of national security interest. I have decided to effectively administer use of the authority under SCISA and delegate my power to two positions: 1) Vice-President of the Policy and Programs Branch; and 2) Agency Security Officer. As prescribed under SCISA, the CFIA has the responsibility to ensure that it receives only information relevant to its mandate and jurisdiction with respect to an activity that undermines the security of Canada. The delegated positions will determine whether information received is relevant and of national security interest. In the same manner, the delegated positions will determine if the CFIA can share information with another institution listed under SCISA or further disclose within the Agency by applying the same criteria of relevancy and of national security interest. In addition, to ensure its accountability, the CFIA will keep records of all information received and shared under SCISA, and will retain such records as per the Agency's Recorded Information Management Policy.

Sincerely

A handwritten signature in black ink, appearing to read 'Paul Glover', with a long horizontal line extending to the right.

Paul Glover
President
Canadian Food Inspection Agency



JAN 18 2017

eDoc: 5157933
ccm 2016-000802

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
131 Queen Street, 6th Floor
House of Commons
Ottawa, ON K1A 0A6

Dear Mr. Calkins:

This letter is in response to your December 13, 2016 letter (enclosed) requesting clarification on the Canadian Nuclear Safety Commission's (CNSC) mandate and role with regard to the *Security of Canada Information Sharing Act* (SCISA).

The CNSC's national security mandate is two-fold. Under the *Nuclear Safety and Control Act* (NSCA), the CNSC is responsible for:

- preventing unreasonable risk to national security by regulating the development, production and use of nuclear energy, nuclear substances, prescribed equipment and prescribed information
- implementing Canada's international obligations respecting the control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive devices

While the risks associated with the theft or sabotage of nuclear materials in Canada have a low probability, the potential impacts are very high. The CNSC has not used SCISA so far; however, it could be a useful instrument in ensuring the effective and timely receipt of information.

As a recipient organization under SCISA, the CNSC considers the protection of national security information and the personal information handling provisions of the *Privacy Act* to be of the highest priority. The CNSC has a process in place, aligned with Public Safety Canada's guidance, to ensure the appropriate collection, retention, and further disclosure of personal information received under SCISA.



Subsequent to your letter, the Clerk of the Committee has contacted the CNSC and extended an invitation to appear at a Committee meeting in early February 2017. We look forward to the opportunity to discuss these matters with you and your colleagues. In the meantime, please do not hesitate to contact us should you require further information.

Yours sincerely,

A handwritten signature in blue ink that reads "M. Binder". The signature is fluid and cursive, with the first letter of "M" and "B" being large and prominent.

Michael Binder

Encl: (1)

STANDING COMMITTEE ON ACCESS TO
INFORMATION, PRIVACY AND ETHICS



COMITE PERMANENT DE L'ACCES A
L'INFORMATION, DE LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS ET DE L'ETHIQUE

[BY EMAIL]

2016-12-13

Michael Binder, President
Canadian Nuclear Safety Commission
280 Slater Street, POB 1046, Station B
Ottawa, Ontario
K1P 5S9

Dear Mr. Binder,

In the context of its study of the *Security of Canada Information Sharing Act (SCISA)*, the Standing Committee on Access to Information, Privacy and Ethics is seeking clarification on your organization's mandate and its role with regards to the Act.

As you know, you are listed as a recipient institution as per Schedule 3 of the Act.

More precisely, the Committee wishes to know how your organization's mandate relates to national security, and how your organization views its responsibilities under the Act as a recipient institution, with respect to the collection, retention, and further disclosure of personal information.

The Committee would appreciate receiving this information by Friday, January 20, 2017, so that it can consider your response when it resumes sitting in late January. A representative of your organization may be invited to appear before the Committee to discuss the subject matter further, if required.

Best regards,



Blaine Calkins, MP
Chair



Communications Security
Establishment

Centre de la sécurité
des télécommunications

UNCLASSIFIED

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

Our file Notre référence
CERRID # 32847528

JAN 19 2017

Dear Mr. Calkins:

Thank you for your December 13, 2016 letter regarding the study of the *Security of Canada Information Sharing Act* (SCISA) by the Standing Committee on Access to Information, Privacy and Ethics.

CSE is one of Canada's key security and intelligence organizations. CSE's mandate and authorities are defined in the *National Defence Act* (NDA), which requires CSE to do three things: 1) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; 2) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and 3) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

As you highlighted in your letter, SCISA lists CSE as an entity that can receive information from another Government of Canada institution. SCISA does not supersede or expand CSE's authorities to collect or receive information from our domestic partners. To date, CSE has not received or disclosed information under SCISA. CSE relies on authorities under the NDA and the provisions of the *Privacy Act*, as well as information sharing arrangements with our domestic security and intelligence partners, when sharing information.

To ensure that information is collected in accordance with its statutory obligations, CSE has policies and systems in place to allow for the validation, tracking and auditing of information received. Such information exchanges involve specific guidelines to ensure that the information is relevant to CSE-mandated activities, and provided to appropriate personnel. Disclosing institutions are encouraged to contact CSE before disclosing any information in order to ensure that CSE's mandate allows for the lawful collection of the information. The implemented process further leverages existing information sharing mechanisms to ensure that information disclosed to CSE is appropriately tracked.

More widely, I would like to highlight that CSE has a responsibility to protect privacy, and we take that responsibility very seriously. Protecting Canadian privacy is a fundamental part of our organizational culture and is embedded within our operational structures, policies and processes. CSE's strong privacy framework includes detailed operational policies, with specific retention periods, and regular training and testing of staff on privacy and compliance knowledge, as well as internal review and independent external review by the Office of the CSE Commissioner. These measures contribute to ensuring that CSE's activities are conducted in a way that protects Canadian privacy interests.

Sincerely,

Greta Bossenmaier
Chief



FEB 02 2017

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to
Information, Privacy and Ethics
House of Commons
Ottawa ON K1A 0A6

Dear Colleague:

Thank you for your correspondence of December 13, 2016, addressed to my predecessor, the Honourable John McCallum, concerning the role and mandate of Immigration, Refugees and Citizenship Canada (IRCC) in the context of your study of the *Security of Canada Information Sharing Act* (SCISA).

Under its mandate, IRCC is responsible for determining the admissibility of applicants for temporary and permanent residence in Canada, which ensures that individuals who pose a threat to national security do not enter or acquire status in Canada. While these responsibilities require collaboration with other federal institutions, the final decision on all applications rests with IRCC.

IRCC is also responsible for citizenship grant decisions as well as promoting the rights and responsibilities of Canadian citizenship. The Department works to prevent fraud, including revoking citizenship in cases where the person obtained citizenship by false representation, or fraud with respect to matters related to national security. Furthermore, IRCC is responsible for the passport program domestically and abroad and safeguards the security, value and integrity of Canadian passports and travel documents, through entitlement reviews and administrative investigations.

Further specific information pertaining to IRCC's mandate in relation to national security can be found in the enclosed Annex.

Given its key role related to national security and the large volumes of personal data it holds, IRCC views its responsibilities pertaining to SCISA very seriously. The objective of SCISA is to improve the effectiveness and timeliness of information sharing among government institutions for national security purposes, while respecting the rights of individuals under the *Privacy Act* and the *Canadian Charter of Rights and Freedoms*.

Canada

To ensure the responsible and effective use of SCISA across all listed institutions, Public Safety Canada has developed a deskbook to guide institutions in their implementation of the Act. At IRCC, an internal policy was developed to further support employees with the implementation of the Act, while providing guidelines adapted to IRCC's particular context. The policy covers matters such as delegation of authority, provides guidelines concerning collection, disclosure and retention of information, as well as caveats restricting secondary disclosure of information. Moreover, it introduces a reporting process and establishes recordkeeping requirements. Finally, training has been provided on the use of SCISA and is continuously available, together with functional support and guidance from privacy and policy experts.

Given its mandate, IRCC plays a crucial role in ensuring the security and safety of Canadians and SCISA supports this role by encouraging collaboration between government institutions on matters related to national security.

I trust that this information will be useful to better understand the Department's mandate in relation to national security.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Ahmed Hussen', written in a cursive style.

Ahmed Hussen, P.C., M.P.
Minister of Immigration, Refugees and Citizenship

Enclosure

ANNEX

Detailed description of Immigration, Refugees and Citizenship Canada's mandate in relation to national security

Immigration, Refugees and Citizenship Canada (IRCC) is responsible for facilitating the arrival and integration of migrants into Canada, while protecting the health, safety and security of Canadians, as well as managing the citizenship program, and the issuance of Canadian passports and travel documents. These mandates and responsibilities place IRCC as a critical link in the Government of Canada's national security regime. IRCC's support for national security priorities focuses on ensuring the integrity of the citizenship, immigration, refugee and passport processes and programs.

IRCC works closely with its security and enforcement partners to proactively identify applicants who are inadmissible to Canada due to security concerns, to remove or revoke the status of those who engage in activities deemed to undermine Canada's national security, and may refuse and revoke the passport of persons posing a threat to national security based on decisions rendered by the Minister of Public Safety and Emergency Preparedness. More specifically:

- IRCC conducts entitlement reviews and may launch an administrative investigation to collect further information to determine a subject's eligibility to passport services. The Minister of Public Safety and Emergency Preparedness has the authority to cancel, refuse or revoke the passport of individuals of concern to national security and communicate these decisions to IRCC to take the required action.
- IRCC ensures that individuals are not admitted to Canada who are deemed inadmissible for criminality, organized criminality, human or international rights violations, security, misrepresentation and other grounds defined in the *Immigration and Refugee Protection Act*.
- IRCC conducts assessments and issues ministerial opinions on whether protected persons¹ who have been found to be inadmissible for security reasons, human rights violations, serious criminality, or organized crime represent a danger to the public in Canada or danger to the security of Canada.
- IRCC processes pre-removal risk assessment applications, which may include those submitted by persons who are inadmissible on grounds of security, violating human or international rights, organized criminality or serious criminality. In some cases, this involves an assessment of whether the applicant is a danger to the public in Canada or a danger to the security of Canada.
- IRCC is responsible for conducting revocations of citizenship which include grounds related to national security. More specifically, citizenship can be revoked if a person has obtained his or her citizenship by false representation, fraud or knowingly concealing material circumstances with

¹ A protected person is defined as a person on whom refugee protection is conferred and whose claim or application has not subsequently been deemed to be rejected under the *Immigration and Refugee Protection Act*.

respect to facts which may render persons inadmissible to Canada on grounds of security, human rights violations, and organized crime.

- IRCC can make referrals to the Security Intelligence Review Committee for individuals who should be prohibited from obtaining Canadian citizenship for reasons that they have engaged, are engaging or may engage in activities that constitute a threat to the security of Canada.

Minister of Finance



Ministre des Finances

Ottawa, Canada K1A 0G5

2016FIN447571

JAN 11 2017

Mr. Blaine Calkins, MP
Chair
Standing Committee on Access to Information, Privacy and Ethics
6th Floor, 131 Queen Street
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Calkins:

Blaine,

Thank you for your letter dated December 13, 2016 requesting information regarding my role under the *Security of Canada Information Sharing Act (SCISA)*.

As the Minister of Finance, I have a number of responsibilities related to national security. These responsibilities include the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which establishes measures to detect and deter money laundering and the financing of terrorism. I also have broad responsibility over the stability of Canada's financial sector. It is therefore important that my Department and I have access to information regarding potential threats to the critical infrastructure, stability and cyber security of Canada's financial sector and to the stability of the global economic and financial system.

Under SCISA, the Head of each Government Institution and those delegated by the Head are listed as the recipient of SCISA disclosures. Therefore, as the Minister of Finance, those who I have named as delegates¹ and I are accountable and responsible for receiving or collecting information under SCISA, should it be required. The Department of Finance and I take these responsibilities under SCISA very seriously. That is why prior to the

¹ The Assistant Deputy Ministers of the Financial Sector Policy Branch and International Trade and Finance Branch.

August 1, 2015, coming into force of SCISA, in line with the Public Safety SCISA Deskbook, the Department of Finance established guidelines to govern the receipt and disclosures under SCISA.

The guidelines require:

- that only information relevant to the Department of Finance's jurisdiction or responsibility may be received;
- that disclosures can only be made to the Assistant Deputy Ministers of the Financial Sector Policy Branch and International Trade and Finance Branch, respectively;
- that the Department of Finance should be contacted before receiving the information; and,
- proper storage and tracking of the information received, based on classification.

We look forward to supporting the Committee as part of its study on SCISA.

Yours sincerely,

A handwritten signature in blue ink, appearing to read "Bill Morneau", with a long, sweeping horizontal stroke extending to the right.

The Honourable Bill Morneau, P.C., M.P.



Thank you for your letter requesting a description of Global Affairs Canada's mandate as it relates to national security, and on how the Department views its responsibilities under the *Security of Canada Information Sharing Act (SCISA)* as a recipient institution with respect to the collection, retention, and further disclosures of personal information.

As outlined in the *Department of Foreign Affairs, Trade and Development Act*, Global Affairs Canada manages diplomatic and consular relations with foreign governments and international organizations, advancing Canada's political, security and economic interests and the values of freedom, democracy, human rights and the rule of law.

In this capacity, Global Affairs Canada contributes to a number of national security-specific activities, a selection of which are outlined below. The designation of Global Affairs Canada as a Canadian federal institution eligible to receive information shared under SCISA allows the Department to better address its mandated national and international security responsibilities and fulfill its role in protecting Canadian national security.

Global Affairs Canada is the lead federal department for identifying, co-ordinating and facilitating the response to national security-related incidents occurring outside Canada, involving Canadians or Canadian interests. For example, the Department leads Canada's response to national security-related hostage-takings abroad through a coordinated effort drawing on the special skills of the federal national security community. Global Affairs Canada missions and diplomats also play an important role when Canadian citizens are imprisoned or accused of terrorist activity abroad.

The Department also manages Canada's membership in bilateral or multilateral defence and security organizations including the United Nations, the North Atlantic Treaty Organization, the North American Aerospace Defence Command, the Organization of American States, the Conference on Disarmament, and the Organization of Security and Cooperation in Europe. These organizations deal with traditional threats to security as well as non-traditional threats such as terrorism and threats to cyber and space security.

Global Affairs Canada is also a major consumer of intelligence reporting relating to foreign policy and international security which requires comprehensive coordination with the Canadian intelligence community on intelligence and information sharing issues. The Department is responsible for assessing threats to the security of missions abroad, providing appropriate protection, and managing any residual risks to life and property. Under the Global Security Reporting Program, the Department provides ongoing reporting to the Government of Canada on security and stability issues of strategic interest to Canada, and regular situational awareness reporting and threat dynamics in mission areas abroad.

Preventing terrorists from using the global financial system to further terrorist activity is essential for the suppression of international terrorism. Under the *United Nations Al-Qaida and Taliban Regulations* and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* Global Affairs Canada plays a key role in the listing of terrorist entities, as well as acting as the lead Canadian department on international treaty negotiations on terrorism.

The Department contributes to multilateral counter-proliferation efforts related to preventing the transit of weapons of mass destruction (WMD) and related materials among states and non-state actors of proliferation concern. These efforts include the Proliferation Security Initiative focused on the interdiction of WMD proliferation and UNSCR 1540 aimed at preventing the terrorist acquisition of WMD and related materials. Each of these initiatives call on States to take steps to enhance national legal authority to strengthen key counter-proliferation measures, including the rapid exchange of relevant information concerning suspected proliferation activity. SCISA will assist Canada in exchanging relevant information on suspected proliferation activity in a timely manner.

Global Affairs Canada carefully manages all of its obligations as a recipient institution under the SCISA. The retention of personal information by Global Affairs Canada, compliant with the *Privacy Act* and subject of Privacy Risk Assessments (PIA), remains unchanged. The disclosure of personal information by Global Affairs Canada is determined on a strictly individual case-by-case basis, on the merit of the case, in conformity with the threshold of relevance established in SCISA. All information contemplated for disclosure must be determined to be relevant to the recipient institution's jurisdiction or responsibilities with respect to an activity that undermines the security of Canada. No disclosure of information can be conducted without the clear, written authorization of an official at the Director-level or above.

In conclusion, Global Affairs Canada is a lead department shaping Canada's response to the majority of activities that undermine the security of Canada or the lives of the people of Canada. This letter has highlighted some key examples of the Department's national security mandate. If desired, further information on the Department's national security role pertaining to areas such as the *Investment Canada Act*, the *Export and Import Permits Act*, the *Chemical Weapons Convention Implementation Act*, international law and humanitarian assistance can be provided or found in the SCISA Deskbook (attached in PDF)

Minister of Health



Ministre de la Santé

Ottawa, Canada K1A 0K9

JAN 18 2017

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
ethi@parl.gc.ca

Dear Mr. Calkins:

Thank you for your letter of December 13, 2016, in which you seek clarification on Health Canada's mandate as it pertains to the *Security of Canada Information Sharing Act*.

I have shared your correspondence with Mr. Simon Kennedy, Deputy Minister of Health Canada, and Dr. Siddika Mithani, President of the Public Health Agency of Canada, and have asked each of them to provide you with a detailed response on this issue directly.

The work that the Standing Committee has accomplished so far in fulfilling its mandate is of great benefit. Please accept my best wishes for success as you move forward.

Again, thank you for writing.

Yours sincerely,

A handwritten signature in cursive script that reads "Jane Philpott".

The Honourable Jane Philpott, P.C., M.P.



Health
Canada

Santé
Canada

Deputy Minister Sous-ministre

Ottawa Canada
K1A 0K9

JAN 18 2017

Your file Votre référence

Our file Notre référence

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
ethi@parl.gc.ca

Dear Mr. Calkins:

I am writing in response to your letter of December 13, 2016, addressed to the Honourable Jane Philpott, Minister of Health, in which you seek clarification on Health Canada's mandate as it pertains to the *Security of Canada Information Sharing Act* (SCISA).

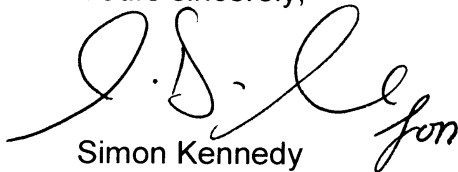
Health Canada has security responsibilities related to nuclear emergencies and nuclear non-proliferation. Responsibility for these activities falls under the purview of the *Department of Health Act* and the *Emergency Management Act*, which support the Federal Nuclear Emergency Plan. This includes responsibilities for management of the radiological consequences of a nuclear emergency and support for radiological and nuclear security during major events. As well, the Department has responsibilities for supporting nuclear non-proliferation under the *Comprehensive Nuclear Test-Ban Treaty Implementation Act*.

Health Canada's inclusion in Schedule III of the SCISA supports effective cooperation in response to real or potential threats involving nuclear facilities, radiological dispersal devices, radiological exposure devices, and the proliferation of nuclear weapons.

It is important to note that only information relevant to a recipient institution's security mandate can be shared under SCISA. As a recipient organization, the Department takes its responsibility to receive information under the SCISA and the protection of this information very seriously. Health Canada's processes to collect, retain, and disclose relevant personal information are done in a manner that is consistent with both the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.

Thank you for writing. I trust that the foregoing is helpful.

Yours sincerely,



Simon Kennedy

Canada



JAN 30 2017

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
House of Commons
Ottawa ON K1A 0A6

Dear Mr. Calkins:

Thank you for your correspondence of December 13, 2016, in which you sought clarification regarding Transport Canada's national security responsibilities under the *Security of Canada Information Sharing Act* (SCISA).

Transport Canada has yet to use the SCISA provisions to exchange personal information for national security purposes. The department discloses information under several other legal and regulatory authorities, such as the *Aeronautics Act*, the Canadian Aviation Security Regulations, the *Secure Air Travel Act*, the *Marine Transportation Security Act*, and the Marine Transportation Security Regulations.

Regarding the handling of personal information at Transport Canada, a ministerial delegation instrument identifies a limited number of departmental officials who are authorized to receive information under SCISA, and a similar document is being prepared for disclosures. Prior to the enactment of SCISA, Transport Canada developed guidelines for the exchange of information with other institutions.

Canada's national transportation system is vital to this country's economic prosperity. Threats to or interference with this vast and complex system can undermine the security of Canada. Transport Canada's mandate includes the promotion of a safe and secure, efficient and environmentally responsible transportation system in Canada. This being the case, the department's security responsibilities include identifying, tracking and responding to threats to the transportation modes. The nature of these threats range from, for example, terrorism, sabotage or other forms of unlawful interference, as well as hostile cyber activity. Criminal activities can also undermine the safety and integrity of transportation systems.

In order to fulfill its security mandate, Transport Canada must have access to information from domestic and international security and intelligence agencies to effectively and proactively identify and address threats to the transportation system. Any restriction or reduction in the quality and quantity of information originating from other Canadian institutions can undermine Transport Canada's ability to meet its legislated responsibilities and can negatively impact the security of Canada.

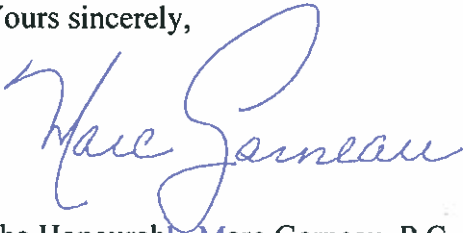
Currently, Transport Canada administers, in whole or in part, the following acts with a clear link to national security: the *Aeronautics Act*, the *Marine Transportation Security Act*, the *Railway Safety Act*, the *Transportation of Dangerous Goods Act* and the *International Bridges and Tunnels Act*.

If Transport Canada does not have access to relevant security information, the department and key transportation stakeholders with the proper security clearance would be unable to promptly (if not proactively) respond to attack-plotting by terrorists and others who seek to commit acts of unlawful interference against the transportation system or related infrastructure.

Transport Canada requires information and intelligence comprising, but not limited to, terrorist aspirations, intents and activities, malicious cyber activities, criminal elements operating in Canadian airports and ports in support of the established security screening regimes of workers and non-passengers accessing restricted areas.

I trust that this response meets your requirements. Thank you again for writing.

Yours sincerely,

A handwritten signature in blue ink that reads "Marc Garneau". The signature is fluid and cursive, with a large loop at the end of the name.

The Honourable Marc Garneau, P.C., M.P.
Minister of Transport



JAN 23 2017

Mr. Blaine Calkins, M.P.
Chair
Standing Committee on Access to Information, Privacy and Ethics
131 Queen Street, Sixth Floor
House of Commons
Ottawa, Ontario
K1A 0A6

Mr. Calkins,

Further to your letter of December 13, 2016, I am pleased to provide you with information on the mandate of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and its responsibilities under the *Security of Canada Information Sharing Act* (SCISA) as a recipient institution.

As Canada's financial intelligence unit, FINTRAC facilitates the detection, prevention and deterrence of money laundering and the financing of terrorist activities. Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), FINTRAC houses both supervisory and intelligence functions. And so while FINTRAC ensures that businesses subject to the PCMLTFA comply with their reporting obligations, it also analyzes the information it receives from those businesses to subsequently disclose financial intelligence to law enforcement and national security agencies.

The compliance function is responsible for ensuring that reporting entities comply with their obligations (record keeping, reporting certain financial transactions, etc.) as set out in Part 1 of the PCMLTFA. With the financial transaction reports that FINTRAC receives from reporting entities subject to the PCMLTFA, it is able to provide financial intelligence to assist Canada's law enforcement and national security agencies in combatting money laundering, terrorism financing and threats to the security of Canada. This case-specific financial intelligence is FINTRAC's core product. The Centre also develops strategic intelligence about trends and typologies of money laundering and terrorism financing.

In terms of intelligence, FINTRAC can disclose information related to a financial transaction (or an attempted financial transaction) specified under the PCMLTFA, to law enforcement agencies **only** when it has “reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering or a terrorism activity financing offence”. If this first threshold is met, FINTRAC is further required to disclose the same financial transaction information to the Canada Revenue Agency, the Canada Border Services Agency, and the Communications Security Establishment, as well as provincial securities regulators, according to different secondary thresholds that apply to each agency.

When FINTRAC has “reasonable grounds to suspect that the information would be relevant to threats to the security of Canada”, it is required to disclose the information to the Canadian Security Intelligence Service. If this first threshold is met, FINTRAC is further required to provide the same information to the appropriate police force and the Canada Border Services Agency, according to different secondary thresholds that apply to each partner.

Therefore, section 5 of the SCISA does not change in any way when, or to whom, FINTRAC discloses financial intelligence. FINTRAC can disclose financial intelligence **only** when the legislated thresholds have been met and **only** to recipients as prescribed in the PCMLTFA.

FINTRAC has not received or collected any information under the SCISA. The SCISA does not impact FINTRAC’s activities given that the provisions of the PCMLTFA take precedence over any provisions related to the reception and communication of information.

Enshrined in the PCMLTFA are clear principles for the protection of privacy, which respect the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, and are reinforced by FINTRAC’s own operational policies and security measures. Furthermore, the Office of the Privacy Commissioner of Canada conducts a statutory biennial review of how FINTRAC manages personal information, ensuring the appropriate measures are in place.

The Centre understands very clearly that in order to maintain the confidence of Canadians, it needs to continually demonstrate that it protects the private information under its control and that it takes the limits of its mandate seriously. To that effect, the PCMLTFA provides for severe penalties for any person or entity, including FINTRAC employees, that use or disclose information inappropriately, including a fine of up to \$500,000 and/or up to five years imprisonment.

Should you have any additional questions or require additional information, please do not hesitate to contact me at 613-995-9063.

Sincerely,



Gérald Cossette

cc. Hugues La Rue, Clerk, Standing Committee on Access to Information, Privacy and Ethics



Public Health
Agency of Canada

Agence de la santé
publique du Canada

President

Présidente

Ottawa, Canada
K1A 0K9

JAN 19 2017

Mr. Blaine Calkins, MP
Chair
Standing Committee on Access to Information, Privacy and Ethics
House of Commons
Ottawa, ON

Dear Mr. Calkins:

Thank you for your letter of December 13, 2016, seeking clarification of the Public Health Agency of Canada's (PHAC) mandate and role with regard to the *Security of Canada Information Sharing Act (SCISA)*.

I am pleased to provide information on how PHAC's mandate relates to national security and how PHAC views its responsibilities under SCISA as a recipient institution, with respect to receiving, retention, and further disclosure of personal information.

Under SCISA, PHAC is authorized to receive information concerning national security in order to protect Canada against activities that undermine the health security of Canada. PHAC has specific responsibilities related to national security that require responding rapidly to threats with direct public health consequences, such as pandemics or other emerging infectious disease outbreaks, and accidental or intentional release or misuse of pathogens or toxins, including bioterrorism. PHAC also supports Health Canada in the public health consequence management of chemical or nuclear events, and supports Public Safety in responding to the public health impacts of natural disasters such as fires, floods and earthquakes. Responsibility for these activities is derived from the *Department of Health Act*, the *Public Health Agency of Canada Act*, the *Emergency Management Act*, the *Human Pathogens and Toxins Act*, and the *Quarantine Act*.

Inclusion of PHAC in Schedule 3 of SCISA allows other Government of Canada institutions to share health security related information with PHAC on a priority and as-needed basis in support of these responsibilities. Receiving national security information under SCISA allows for PHAC to prepare for, monitor, and respond to health emergencies and health impacts of national security events.

.../2

While PHAC has not yet received or shared information under SCISA, as a recipient institution, the Agency takes its responsibility to receive information under SCISA and the protection of this information very seriously. Before receiving or sharing information, PHAC will first determine whether the information is relevant and of national security interest, as per the requirements of SCISA. PHAC is also committed to safeguarding the confidentiality of information provided by individuals and institutions, and our processes will be in accordance with Canadian law, including any legal requirements, restrictions and prohibitions.

If you have further questions, I would invite your office to contact Éleine Chatigny, A/Assistant Deputy Minister, Health Security Infrastructure Branch. She may be reached either by telephone at (613) 957-0316 or by email at Elaine.Chatigny@phac-aspc.gc.ca

Thank you for writing.

Sincerely,



Siddika Mithani, PhD

APPENDIX B LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
<p>As an individual</p> <p>Craig Forcese, Professor Faculty of Law, University of Ottawa</p> <p>Kent Roach, Professor Faculty of Law and Munk School, University of Toronto</p>	2016/11/03	33
<p>Canadian Civil Liberties Association</p> <p>Sukanya Pillay, Executive Director and General Counsel</p>		
<p>Canada Border Services Agency</p> <p>Robert Mundie, Director General and Chief Privacy Officer Corporate Secretariat</p> <p>Canadian Security Intelligence Service</p> <p>Tricia Geddes, Director General Policy and Foreign Relations</p> <p>Department of Justice</p> <p>Ann Sheppard, Senior Legal Counsel</p> <p>Department of Public Safety and Emergency Preparedness</p> <p>John Davies, Director General National Security Policy</p> <p>Royal Canadian Mounted Police</p> <p>Scott Doran, Director General Federal Policing Criminal Operations</p> <p>Alison Whelan, Executive Director Strategic Policy and External Relations, Federal Policing</p>	2016/11/17	34
<p>As an individual</p> <p>Wesley Wark, Visiting Professor Graduate School of Public and International Affairs, University of Ottawa</p> <p>Office of the Privacy Commissioner of Canada</p> <p>Patricia Kosseim, Senior General Counsel and Director General Legal Services, Policy, Research and Technology Analysis Branch</p> <p>Steven Morgan, Director General Audit and Review</p> <p>Daniel Therrien, Privacy Commissioner of Canada</p> <p>Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic</p> <p>Tamir Israel, Staff Lawyer</p>	2016/11/22	35

Organizations and Individuals	Date	Meeting
<p>Canadian Muslim Lawyers Association Ziyaad Mia, Member Legal Advocacy Committee</p> <p>Kapoor Barristers Anil Kapoor, Barrister</p>	2016/12/06	39
<p>Civilian Review and Complaints Commission for the Royal Canadian Mounted Police Richard Evans, Senior Director Operations Joanne Gibb, Acting Director Research, Policy and Strategic Investigations Unit</p> <p>Office of the Communications Security Establishment Commissioner J. William Galbraith, Executive Director Jean-Pierre Plouffe, Commissioner</p> <p>Security Intelligence Review Committee Pierre Blais, Chair Chantelle Bowers, Deputy Executive Director</p>	2016/12/08	40
<p>As an individual Lisa Austin, Associate Professor University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights</p> <p>British Columbia Civil Liberties Association Micheal Vonn, Policy Director</p> <p>Centre for Law and Democracy Michael Karanicolas, Senior Legal Officer</p>	2016/12/13	41
<p>As an individual David Fraser, Partner, McInnes Cooper</p> <p>Canadian Bar Association David B. Elder, Executive Member, Privacy and Access Law Section</p> <p>OpenMedia Laura Tribe, Executive Director</p>	2017/01/31	42
<p>Communications Security Establishment Dominic Rochon, Deputy Chief Policy and Communications</p> <p>Department of National Defence Stephen Burt, Assistant Chief of Defence Intelligence Canadian Forces Intelligence Command</p>	2017/02/02	43

Organizations and Individuals	Date	Meeting
<p>Department of Transport</p> <p>Marie-France Paquet, Director General Intermodal Surface, Security and Emergency Preparedness, Safety and Security Group</p> <p>Donald Roussel, Associate Assistant Deputy Minister Safety and Security Group</p>	2017/02/02	43
<p>Canadian Nuclear Safety Commission</p> <p>Terry Jamieson, Vice-President Technical Support Branch</p> <p>Lisa Thiele, Senior General Counsel and Director</p>	2017/02/07	44
<p>Department of Citizenship and Immigration</p> <p>Glen Linder, Director General International and Intergovernmental Relations</p> <p>Michael Olsen, Director General Corporate Affairs</p>		
<p>Department of Foreign Affairs, Trade and Development</p> <p>David Drake, Director General Counter-Terrorism, Crime and Intelligence Bureau</p> <p>Victoria Fuller, Director, Case Management Consular Operations</p> <p>Jeffrey K. McLaren, Director Mission Security Operations</p> <p>Patrick Picard, Director Access to Information and Privacy</p>		
<p>Financial Transactions and Reports Analysis Centre of Canada</p> <p>Gérald Cossette, Director</p> <p>Stéphane Cousineau, Deputy Director Corporate Management Services Sector and Chief Financial Officer</p>		

APPENDIX C LIST OF BRIEFS

Organizations and Individuals

Canadian Bar Association

Forcese, Craig

International Civil Liberties Monitoring Group

Roach, Kent

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* ([Meetings Nos 33, 34, 35, 39, 40, 41, 42, 43, 44, 45, 50, 51 and 56](#)) is tabled.

Respectfully submitted,

Blaine Calkins
Chair

The Privacy Impacts of the Security of Canada Information Sharing Act: A Premature Review

Introduction

1. On June 18, 2015, the 41st Parliament of Canada passed former Bill C-51, the Anti-Terrorism Act 2015. Included in this Act were new information sharing provisions for Canada's national security organizations. These provisions formed Canada's Security of Canada Information Sharing Act (SCISA).
2. During deliberations of the Standing Committee on Public Safety and National Security, various witnesses testified as to the necessity of these new information sharing tools and potential privacy concerns that may arise from their application. Given that these new tools were not yet in place during the initial review of the draft legislation, these concerns were based on theory and presumption, not fact.
3. On 18 October 2016, the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("the Committee") adopted the following motion:
That the Committee undertake a study of the Security of Canada Information Sharing Act, its impacts on privacy since its implementation, and whether there are any changes that should be proposed in the course of the Government's national security consultation and review.
4. The scope of this current review was not to re-examine potential privacy concerns of SCISA. Instead, the committee's mandate was to review the concrete privacy impacts that SCISA has had since it came into force less than two years ago.
5. This committee heard from many of the same witnesses that appeared before the Standing Committee on Public Safety and National Security during its review of Bill C-51¹. Although the Conservative Caucus appreciates the time and efforts of these witnesses, the testimony on the potential privacy concerns of SCISA was, again, largely based on theory and presumption.
6. In order to fulfill the mandate of this current study, the committee required factual testimony on how the new information sharing tools in SCISA are impacting the privacy rights of Canadians. To this end, the committee heard from Canada's national security organizations who have been using these new tools, the Canadian national security oversight bodies who review the application of these new tools, and the Privacy Commissioner who assess any impacts of new legislation on the privacy rights of Canadians.

¹ Canadian Bar Association, OpenMedia, British Columbia Civil Liberties Association, Canadian Muslim Lawyers Association, Wesley Wark, Craig Forcese, Kent Roach, Canadian Civil Liberties Association.

The Application of SCISA by Canada's National Security Organizations

7. The overarching goal of SCISA was to allow Canada's national security organizations to effectively protect Canadians. As indicated in section 3.1 of the majority report, this tool plays an important role in Canada's national security:

A number of officials from federal institutions described the benefits of SCISA and asserted that it gives them an important new tool for sharing information effectively and improves national security.

8. In addition to protecting Canadians, a vital goal of SCISA is to achieve this protection while also ensuring the privacy rights of Canadians. Determining whether this balance is being achieved is the central element of this current study. Although Canada's national security organizations agree that SCISA will help ensure our country's national security, it is difficult to concretely determine the privacy impact of these tools due to the short time the law has been enacted.

9. Indeed, although many of these national security organizations stated that there has been no abuse or misuse of these new information sharing provisions², they also stated that SCISA is relatively new legislation, and as a result, they have not yet had the opportunity to fully determine its effects and impacts³. Given the testimony received from Canada's national security organizations, it is our view that it is currently impossible to determine whether the application of the new information sharing laws has inappropriately impacted the privacy of Canadians.

The Review of SCISA's Application by Canada's National Security Oversight Bodies

² ETHI *Evidence*, 1st Session, 42nd Parliament, 7 February 2017, 1640 (Terry Jamieson, Vice-President, Technical Support Branch, Canadian Nuclear Safety Commission; David Drake, Director General, Counter-Terrorism, Crime and Intelligence Bureau, Department of Foreign Affairs, Trade and Development; Gérald Cossette, Director, Financial Transactions and Reports Analysis Centre of Canada; Glen Linder, Director General, International and Intergovernmental Relations Department of Citizenship and Immigration); ETHI *Evidence*, 1st Session, 42nd Parliament, 2 February 2017, 1605 1610 (Dominic Rochon, Deputy Chief, Policy and Communications, Communications Security Establishment; Stephen Burt, Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command, Department of National Defence), 1610 (Marie-France Paquet, Director General, Intermodal Surface, Security and Emergency Preparedness, Safety and Security Group, Department of Transport)

³ ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 February 2017, 1600 (Mr. Donald Roussel, Associate Assistant Deputy Minister, Safety and Security Group, Department of Transport); ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 February 2017, 1610 (Mr. Dominic Rochon, Deputy Chief, Policy and Communications, Communications Security Establishment); ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 February 2017, 1630 (Mr. Stephen Burt, Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command, Department of National Defence).

10. In order for this committee to determine the concrete impacts of SCISA on the privacy of Canadians, it is essential to examine the testimony of Canada's national security oversight bodies.

11. The committee heard from Mr. Jean-Pierre Plouffe, Commissioner for the Office of the Communications Security Establishment Commissioner. During his appearance, Mr. Plouffe indicated that, although he reviews the important work of the Communications Security Establishment (CSE), it is unlikely that CSE will share or receive any information under SCISA.⁴

12. In addition, the committee heard from both the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police and the Security Intelligence Review Committee for the Canadian Security Intelligence Service. Both of these oversight bodies indicated to the committee that they are currently undertaking their first reviews of the application and use of the new information sharing provisions in SCISA.⁵

13. Given the testimony received from Canada's national oversight bodies with regards to their on-going reviews of the application SCISA, it is impossible to determine whether there have been any concrete impacts to the privacy rights of Canadians since the enactment of SCISA.

The Review of Privacy Impact by the Office of the Privacy Commissioner of Canada

14. The Office of the Privacy Commissioner of Canada plays a critical role in determining the privacy impacts of SCISA. To this end, the Privacy Commissioner informed the committee that his office undertook a survey of Government of Canada institutions on the application and implementation of SCISA in the first six months since its coming into force, that is, from 1 August 2015 to 31 January 2016.

15. The Commissioner also informed the committee that his office will be conducting the second phase of his audit to further determine the impacts of SCISA on the privacy of Canadians.⁶ Given that the Privacy Commissioner's audit is still on-going, the committee is not in a position to fully determine the concrete impacts of SCISA's provisions on the privacy rights of Canadians.

Conclusion

⁴ ETHI *Evidence* 1st Session, 42nd Parliament, Thursday, December 8, 2016, 1105 (Mr. Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment Commissioner).

⁵ ETHI *Evidence* 1st Session, 42nd Parliament, Thursday, December 8, 2016, 1115 (Hon. Pierre Blais, Chair, Security Intelligence Review Committee), 1125 (Mr. Richard Evans, Senior Director, Operations, Civilian Review and Complaints Commission for the Royal Canadian Mounted Police).

⁶ ETHI, *Evidence*, 1st Session, 42nd Parliament, 22 November 2016, 1105 ((Mr. Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment Commissioner).

16. The Conservative members of the Standing Committee on Access to Information, Privacy and Ethics believe that there is no priority more important than protecting the safety and security of Canadians. Providing our national security organizations with the tools they required to achieve this and to allow them to work alongside our allies is critical. We also believe that it is important to ensure that our national security is balanced with the right to privacy of Canadians. Therefore, we believe that the mandate of this study – to review the concrete privacy impacts of the new information sharing tools in SCISA - is extremely important.

17. Although some witnesses have expressed concerns relating to SCISA, these views are the exact same ones shared during the review of Bill C-51 and are based on theory and presumption. The 41st Parliament considered the merits of these concerns and voted to enact Bill C-51 and the information sharing tools which now form SCISA. The mandate of our committee during this study was not to discuss whether SCISA should have been enacted. Our mandate was to determine: Have there been any impacts on the privacy rights of Canadians since SCISA has been enacted?

18. The testimony received from witnesses unfortunately does not allow the committee to answer this question. Given the relatively recent enactment of SCISA, Canada's national security organizations have not had the opportunity to fully utilize these new tools. Furthermore, Canada's national security oversight bodies and Canada's Privacy Commissioner have on-going reviews of the impacts of these new information tools.

19. For this reason, the Conservative members believe that it is premature and imprudent for this committee to suggest substantive amendments to SCISA.

20. To this effect, we recommend:

Recommendation 1: That the Standing Committee on Access to Information, Privacy and Ethics undertake a study of the Security of Canada Information Sharing Act and its impacts on privacy since its implementation in 3 years.

SCISA: One part of a larger problem
The New Democratic Party dissenting opinion

Through its Bill C-51, the previous government gave broad, far-reaching powers to Canada's security agencies. These powers unnecessarily comprise Canadians' civil liberties.

In order to protect the rights and freedoms of Canadians, we must turn away from the path laid out by C-51. Concentrating too much power in the hands of any one person or organization, no matter how well intentioned at the outset, is a recipe for abuse and injustice.

The *Security of Canada Information Sharing Act* (SCISA) is a foundational element of the regime envisioned in C-51 and should be repealed, as recommended by a number of witnesses, along with all the other elements of that bill.

New Democrats are open to conversations with our security agencies about how to better protect Canadians, while at the same time respecting their rights and freedoms.

Some of the committee's recommendations are laudable. They should be considered in a comprehensive review of our security practices and culture.

However, to endorse these recommendations for changes to SCISA in a context where the other elements of C-51 remain largely unaddressed would send the wrong message. It would suggest that C-51 largely got it right, and that a little tinkering could fix the problems it created.

In fact, Canada needs to affirm, in no uncertain terms, the value and integrity of Canadians' rights and freedoms by rejecting the C-51 regime and repealing its many elements. Such a repeal would set the context for a real, meaningful dialogue about rights, freedoms and security risks in Canada; one that could lead to important reform that does not run roughshod over the rights of Canadians.

Once the table is set for that dialogue, it may prove fruitful to return to some of the recommendations in this report. Until then, we need to prioritize critique of a security culture in Canada that does not provide enough protection to Canadians from arbitrary interference by the state.

