THE CANADIAN BAR ASSOCIATION

L'ASSOCIATION DU BARREAU CANADIEN

Security of Canada Information Sharing Act (SCISA)

CANADIAN BAR ASSOCIATION

JANUARY 2017

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc :** 613.237.0185 | info@cba.org | **www.cba.org**

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the CBA.

TABLE OF CONTENTS

The Security of Canada Information Sharing Act (SCISA)

The Security of Canada Information Sharing Act (SCISA)

I. INTRODUCTION

The Canadian Bar Association appreciates the opportunity to appear before the Access to Information, Privacy and Ethics Committee in its study of the *Security of Canada Information Sharing Act* (SCISA).

The CBA is a national association of over 36,000 members, including lawyers, notaries, academics and law students, with a mandate to seek improvements in the law and the administration of justice.

In December 2016, we offered our views on SCISA to the federal government as part of our response to the National Security Green Paper, 2016. The CBA supports information sharing for the purpose of national security that is necessary, proportionate and accompanied by adequate measures against abuse.

Information sharing is necessary to ensure the efficient and effective operation of government institutions as they work together to safeguard Canadians. However, sharing too much information – or information that is not reliable, as illustrated by the case of Maher Arar – or not sharing enough information to protect national security can lead to harmful consequences. An appropriate balance must be achieved in SCISA between protecting the safety and security of Canadians and preserving individual privacy rights and freedoms.

SCISA has significantly expanded intra-governmental information sharing for national security purposes in Canada, including personal information, without precise definitions, basic privacy protections or clear limitations on the purpose for sharing. While some helpful changes were made to SCISA before its final passage into law in 2015, the statute still causes concern on several fronts.

II. INDEPENDENT OVERSIGHT

The CBA supports the principles guiding information sharing in section 4 of SCISA. However to be effective, SCISA must include a robust oversight and accountability mechanism to enforce

them. This mechanism should have independence from the government institutions that will be sharing information.

The guiding principles for information sharing in section 4 include:

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;
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 the act.

A number of oversight models could potentially work. The current proposal in Bill C-22, *National Security and Intelligence Committee of Parliamentarians Act* would allow that committee to review 'any activity carried out by a department that relates to national security or intelligence.'[1] If created, this committee might be an appropriate body to ensure that information sharing by government institutions under SCISA is carried out appropriately, not only under section 4, but the Act as a whole.

In addition, to better facilitate review of activities carried out under SCISA – whether by a Committee of Parliamentarians, another designated general oversight body or the Privacy Commissioner of Canada – regulations should be introduced requiring institutions to keep a record of disclosures made under SCISA, as well as, for recipient institutions, records of subsequent use and disclosure of information received pursuant to SCISA.

RECOMMENDATIONS

1. **The CBA recommends that SCISA include effective mechanisms to enforce the principles outlined in section 4.**

[1] Bill C-22, section 8(b).

2. **The CBA recommends that regulations be enacted under SCISA requiring records to be kept of disclosures made under SCISA, as well as records of subsequent use and disclosure of information received pursuant to SCISA.**

III. BALANCED INFORMATION SHARING

Section 5(1) of SCISA permits disclosure among the 17 government institutions in Schedule 1 of the Act 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. [Emphasis added]

Mere relevance is a very low standard for what should be an exceptional sharing of information between departments. As others, including the Privacy Commissioner, have commented, a simple test of relevance to the recipient's mandate could allow unnecessary and overbroad sharing of information. A preferable threshold would combine relevance with an additional test of necessity to filling the receiving institution's statutory responsibilities relating to national security. As the Privacy Commissioner has pointed out, the standard under the *Canadian Security Intelligence Service Act* to permit CSIS to collect information is where collection is 'strictly necessary'. This may also be an appropriate and symmetrical standard under SCISA.

In the same vein, several institutions in Schedule 3 to SCISA have broad mandates that go well beyond national security. At a minimum, information should be shared under section 5 only if clearly relevant to a specific statutory authority that relates to national security. Schedule 3 should 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 might relate to national security concerns. Greater specificity would assist both disclosing and receiving institutions, as well as any oversight body in assessing whether disclosure to another institution might be appropriate.

As an overarching comment, The CBA is concerned about how the restrictions in section 5 would work in practice. Before disclosing information to another Schedule 3 institution, the disclosing institution would have to determine the relevance of that information to the recipient institution's jurisdiction or responsibilities. Even if references to specific statutory provisions that relate to national security were to be included for each listed institution in

Schedule 3 (as we recommend), section 5 of the Act still places an implicit burden on a disclosing institution to be sufficiently familiar with a recipient institution's mandate to determine whether any given information will be relevant to the fulfillment of that mandate. If the test for disclosure is strengthened to permit disclosure only where strictly necessary, as we also recommend, the disclosing institution would be faced with an even more difficult assessment.

Accordingly, it may be preferable for all information of potential value to national security to be disclosed to a single, centralized expert authority for distribution – where relevant and strictly necessary – to the institutions listed in Schedule 3. Having MPs involved in this clearinghouse activity, which is more in the nature of an administrative function, would likely not be appropriate. If a new body is created to review and facilitate interdepartmental sharing, it should report directly to Parliament, as a way of ensuring independence from departments that might be exchanging information under SCISA.

RECOMMENDATIONS

3. **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.**

4. **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.**

IV. RESTRICTIONS ON SUBSEQUENT USE AND DISCLOSURE

A remaining concern with SCISA is the lack of restrictions around subsequent use and disclosure of information disclosed to an institution under section 5. While this was amended before Bill C-51 was passed, we remain concerned that it places insufficient restrictions on subsequent use and disclosure of information received under that section. The current provision seems to allow for the subsequent disclosure by a recipient institution to other, non-designated government institutions, to individuals, to foreign governments, or even to the private sector.

The CBA is particularly concerned about subsequent use and further disclosures where information has been obtained by a disclosing institution through the exercise of extraordinary powers, such as powers to compel production of information or enter premises. It would be inappropriate for an institution that lacked similar powers to make further use of information disclosed to it under section 5(1). Otherwise, the receiving institution would benefit from investigation and enforcement powers not conferred on it by Parliament. SCISA should not allow receiving institutions to obtain indirectly that which they could not obtain directly.

Section 6 says that subsequent disclosures are neither authorized nor prohibited by SCISA, but must be done in accordance with the law, including any legal requirements, restrictions and prohibitions. It is unclear what 'in accordance with the law' means here, but one might reasonably infer that it could reference the *Privacy Act* and the laws supervised or implemented by the recipient institutions.

About the latter, to the extent that the laws supervised or implemented by the designated potential recipient institutions would provide few restrictions on use or disclosure, this would create a loophole in the scheme of SCISA that could allow significant and inappropriate 'purpose creep' – including potential disclosure to third parties. In The CBA's view, the information sharing between government institutions contemplated by SCISA should be seen as an extraordinary measure, designed to fulfil an explicit, narrow purpose. It is incumbent on the federal government to explicitly restrict subsequent use and disclosure of that information. It is not enough to leave further disclosures to be governed by existing, sector-specific statutes that may govern the activities of designated potential recipient institutions.

On the *Privacy Act*, section 5 of SCISA says that a government institution's information sharing is, "subject to any provision of any other Act of Parliament, or any regulation made under such an Act, that prohibits or restricts the disclosure of information." Among the stated purposes of SCISA is to facilitate information sharing between government institutions to protect Canada against activities that undermine its security. That goal is different from the purpose in the *Privacy Act*, but there is some overlap.

The intersection of the two Acts is most clear under the collection, use and disclosure provisions. While SCISA is theoretically subordinate to the *Privacy Act* as a result of section 5(1) of SCISA, the *Privacy Act* explicitly allows disclosure authorized by *any other Act of*

Parliament,[2] which would permit any disclosure under SCISA that might otherwise be prohibited.

Since SCISA does not deal with collection of information by government institutions, the *Privacy Act* would presumably continue to govern, at least at first instance. It provides that personal information can be used for the reason it was collected, which must be relevant to the 'operating program or activity' of the collecting institution. Information may also be used for any purpose consistent with the initial purpose. Further, information can be used pursuant to a long list of specific purposes enumerated in section 8(2). This includes any purpose authorized by another Act of Parliament or regulation, and many more.

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*.

RECOMMENDATIONS

5. **The CBA recommends that section 6 of SCISA be narrowed to prohibit subsequent disclosure of information to the private sector and foreign governments and to limit subsequent use by recipient institutions for the purpose of ensuring national security.**
6. **The CBA recommends clarifying the interaction of the *Privacy Act* and SCISA.**

V. ADDITIONAL CHECKS AND BALANCES

SCISA includes few effective checks and balances on information sharing, or safeguards to ensure that shared information is reliable.

Maher Arar's experience illustrated the devastating consequences of sharing inaccurate or unreliable information.[3] The RCMP's decision to provide raw information to US authorities about his suspected al-Qaeda affiliation was the likely cause of his transport to and torture in Syria. The Arar Commission stressed the importance of precautions to ensure that information

---

2 *Privacy Act*, RSC 1985, c. P-21, section 8(2)(b).

3 Commissioner Dennis O'Connor, *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa: 2006).

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. By preventing civil proceedings for disclosures made in good faith, section 9 prevents individuals who suffer damages as a result of wrongful or inaccurate disclosure from seeking redress.

Section 5(1) of SCISA would only authorize disclosure of information 'relevant' to the recipient institution's jurisdiction or responsibilities for activities that undermine the security of Canada, "including in respect of their detection, identification, analysis, prevention, investigation or disruption." While the relevance requirement appears to limit the scope of information sharing, the broad definition of 'activities that undermine the security of Canada' would mean almost everything is relevant. The expression 'jurisdiction or responsibilities' is also so broad it could encompass almost anything.[4]

The other seemingly restraining feature of section 5(1) is that it is subject to any prohibitions or restrictions on disclosure in other Acts or regulations. As discussed above, we believe that restrictions on disclosure under existing laws will not effectively restrain the enhanced information sharing under SCISA.

While section 4(b) of SCISA states that information sharing should be guided by 'respect for caveats on and originator control over shared information', these principles are unenforceable.

Finally, section 6 of SCISA authorizes additional disclosure 'to any person, for any purpose', as long as the disclosure is 'in accordance with law'. This would be less problematic if it clearly applied only to sharing between Canadian agencies (which is not expressly stated).

RECOMMENDATION

7. **The CBA recommends that SCISA include safeguards to ensure that any shared information is reliable.**

VI. CONCLUSION

The CBA appreciates the opportunity to share our views on SCISA. We support balanced information sharing for the purpose of national security that is necessary, proportionate and accompanied by adequate safeguards to protect individual privacy rights and ensure that

4 Craig Forcese and Kent Roach, *Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience* (www.antiterrorlaw.ca) at 31.

information shared is reliable. These measures include robust independent oversight, restrictions around the subsequent use and disclosure of information disclosed to an institution under the Act, as well as effective checks and balances on information sharing. We trust that our comments will be of assistance, and would be pleased to provide any clarifications that the Committee requests.

VII. SUMMARY OF RECOMMENDATIONS

1. **The CBA recommends that SCISA include effective mechanisms to enforce the principles outlined in section 4.**

2. **The CBA recommends that regulations be enacted under SCISA requiring records to be kept of disclosures made under SCISA, as well as records of subsequent use and disclosure of information received pursuant to SCISA.**

3. **The CBA recommends that section 5(1) 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.**

4. **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.**

5. **The CBA recommends that section 6 of SCISA be narrowed so as to prohibit subsequent disclosure of information to the private sector and foreign governments and to limit subsequent use by recipient institutions for the purpose of ensuring national security.**

6. **The CBA recommends clarifying the interaction of the *Privacy Act* and SCISA.**

7. **The CBA recommends that SCISA include safeguards to ensure that any shared information is reliable.**