April 23, 2018

Proposed *Security of Canada Information Sharing Act* Amendments

By: Ben Allison, Lindsay Kvellestad, and Wajeeha Sattar

Policy Commented On: Bill C-59, An Act Respecting National Security Matters

Executive Summary

On August 1st, 2015, the *Security of Canada Information Sharing Act*, SC 2015, c 20 (*SCISA*) came into force by Bill C-51, 2nd Sess, 41st Parl, 2015 (assented to 18 June 2015). *SCISA* gave Government of Canada Institutions the power to share information in their possession with listed receiving institutions. Bill C-59, *An Act Respecting National Security*, 1st Sess, 42nd Parl, 2017 (first reading 20 June 2017) is currently in Committee (SECU). Among a host of other national security changes, this Bill proposes to make amendments to *SCISA*, which will become the *Security of Canada Information Disclosure Act* (*SCIDA*), Bill C-59, s 114. Experts in the field of national security law in Canada have pointed to weaknesses that are not being addressed in the *SCISA* (see Craig Forcese and Kent Roach, A report card on the national security bill). The majority of the criticisms that are associated with Bill C-59 and *SCISA/SCIDA* in particular are the threshold for sharing information, the overbreadth of the exception, circularity, and a lack of review. This post does not intend to canvass the issues afresh. Rather, our focus is on novel problems with the *SCISA* and the proposed amendments in Bill C-59 that have largely gone unaddressed. Beyond the existing critiques, the proposed amendments in Bill C-59 still do not address significant problems. We discuss some of these problems in three parts. Part I argues that treating all types of information as the same, as the *SCISA* does, is problematic. Part II addresses concerns related to disclosing institutions and how they function with regard to information sharing. Similar areas of concern are mentioned in Part III relating to recipient institutions. Each part of this post includes not only critiques but also proposed solutions to the various problems surveyed.

Part I: Types of Information

The *SCISA/SCIDA's* treatment of different types of information is problematic. This part introduces key concerns that follow sharing information, reviews the current and proposed regime, and suggests an alternative. There are three main concerns about information sharing within government bodies that we have identified. First, information obtained by disclosing government institutions (*SCISA*, s 1) is often personal in nature. Personal information triggers section 8 of the *Charter*, which protects the individual's right to be secure against an unreasonable search and seizure by the government. The Supreme Court's reasoning in *R v Wakeling*, 2014 SCC 72 (CanLII), is particularly salient to when shared information will be protected by the *Charter*. *Wakeling* also indicates that section 8 privacy interests persist when the information is no longer in the individual's possession. In that decision, the Court held that disclosing to a foreign body information that had already been lawfully obtained by a search warrant nevertheless raised s 8 privacy concerns. Justice Moldaver stated that, "there is a residual

and continuing expectation of privacy in wiretap information that persists even after it has been lawfully collected" (at para 40). Privacy interests do not evaporate once in the possession of a third party. This means that a plethora of private information that the Canadian government possesses about individuals must be protected even when it is no longer in the individual's possession.

Second, review and oversight of what information is being collected by receiving institutions is difficult (see Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015) at 140). The amount of information that the government collects on citizens is substantial and raises concerns for the meta-analysis of data. If a receiving institution amasses everything that is known by the government about an individual, regardless of how that information was obtained, that same institution will have the capacity to piece together the bits of seemingly unrelated pieces of information to create an invasive profile of Canadian citizens.

Finally, intelligence-to-evidence has been a historic concern for national security agencies (see Craig Forcese, Intelligence Swords and Shields in Canadian Law). The intelligence-to-evidence problem is how to lawfully create viable evidence for trial from intelligence sources without harming on-going investigations. This concern has contributed to institutional policies that caution against disclosure for fear that it will be disclosed to third parties. Intelligence-to-evidence is not just a concern with whether or not intelligence will be admissible. A major concern for national security agencies like CSIS is that intelligence regarding ongoing investigations will become a part of the mandatory disclosure requirements made by the prosecution in a criminal trial. By distinguishing between types of information, we believe the above concerns can be addressed where they are actually problematic.

There is no present or future distinction in *SCISA* between the types of information that are being shared between government institutions. Once the information meets a broad threshold of "[undermining] the security of Canada" (*SCISA*, s 5) and is not excluded, it may be disclosed to other recipient institutions listed in the *Act* (Schedule 3). This means that it will be relatively easy for recipient institutions to collect large amounts of otherwise private information from various government sources. There are various critiques with the current and new threshold and exception requirements that have already been discussed (see, for example, Craig Forcese and Kent Roach, Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience; Kent Roach, "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations" in Andrew Lynch, Nicola McGarrity & George Williams, *Counter-Terrorism and Beyond: The Culture of Law and Justice After 9/11*, (Abington: Routledge, 2010) at 46-68; Leah West, The Problem of 'Relevance': Intelligence to Evidence Lessons from UK Terrorism Prosecutions). We agree with these criticisms but have additional concerns with the broad type of information that will be shared.

Not all of the material received by a government institution has the same privacy concerns or methods of collection. For example, the Canada Revenue Agency (CRA) may use *SCISA* as legislative authority to share private information with Canadian Security Intelligence Service (CSIS) for the purposes of a criminal investigation if the broad threshold requirement is met. CSIS would be able to receive private information from the CRA without a warrant. This

disclosure is drastically different from the RCMP passing along the results of a lawfully obtained wiretap to CSIS. They are both personal in nature where an individual will likely retain an expectation of privacy. However, the latter has already undergone some review and oversight process while the former has not. Private information can be lawfully collected if warrant procedural requirements are followed. Not all of the information already in the possession of the government is as invasive or personal as banking information. Information from relatively minor organizations such as a Port Authority or the Department of Fisheries and Oceans do not raise the same degree of concern. While it is feasible that an individual may retain an expectation of privacy in the information obtained from these institutions, it has a much lower risk of infringing privacy rights than information held by financial institutions or national security agencies. Although Bill C-59 introduces changes to how the threshold of information sharing will be met, none of the proposed amendments distinguish between the type of information being collected by the various government institutions. Some of those changes are addressed later in this post.

The issue of treating all information the same is not a new concept. In 2004, the Supreme Court considered different types of information as a means for determining what, if any, privacy interest an individual might have (*R v Tessling*, 2004 SCC 67 (CanLII)). Justice Binnie held that there were three broad categories of information: personal, territorial, and informational (para 19-24). This distinction was made for the purpose of determining which kinds of information should be protected over others. The Court stated that the "biographical core of personal information" that reveals "intimate details of the lifestyle and personal choices of the individual" should be protected (para 25). *SCISA* includes an even broader concept of information than what *Tessling* considered, which was trying to determine when a warrant is necessary. *SCISA* applies to information already in the possession of the government, some of which is lawfully obtained through a warrant while some is obtained out of force or necessity. For example, we have little choice about whether or not to report our income every year in order to avoid tax penalties. We also do not have a choice about whether or not our medical information will be collected by the government if we wish to receive medical care. This is part of the problem with having the same rules for various types of information from sources that include the Department of National Defence and the Veterans Review and Appeal Board. The type of information received can be fundamentally different.

Distinguishing between types of information has real advantages. This is different from distinguishing between sources of information, which will be discussed later. Not all of the concerns mentioned earlier are applicable for every kind of information. Review and oversight will not be as crucial for information already obtained through a warrant because it has already been subjected to judicial oversight. Repeating the review process for the same piece of information is inefficient and unnecessary. This means that the review and oversight bodies can prioritize their efforts towards data that has not yet been vetted by a judicial body. This would increase the efficiency for disclosure and may encourage agencies to disclose pertinent information faster. Intelligence-to-evidence issues will exist for only some of the information received from various sources. Generally, national security agencies that are building a case against an individual will have information that they will not want disclosed to defence counsel. Only some of the data that can be shared will have evidentiary problems for admissibility. Information will affect the biographical core of personal information to varying degrees. Medical history is far more private than information from Parks Canada. This holds true for the threat of

metadata-type analysis. Risks associated with metadata analysis and long-term storage do not hold true for every piece of information obtained by the government. Conversely, some types of data may, by their nature, pose a more serious concern than others. However, there must also be some restraint despite these advantages. Too much delineation on the types of information that is shared will become complex and counterproductive. Although it may be useful to treat a wiretap differently from banking information, the broad concept of information should not be broken down into overly narrow categories.

In light of this risk, there are three reasonable classifications of information that should be distinguished from each other in *SCIDA*. By differentiating types of information from one another, the review and oversight process can be targeted to address the problems inherent within the information type. First, information that has been obtained through a warrant should be considered on its own. Review and oversight may be limited in this classification because it has already undergone a degree of review. Currently, *SCISA* states that government institutions *may* disclose information to recipient institutions, but this should be amended to *require* government institutions to disclose information obtained through a warrant to recipient institutions (*SCISA*, s 5). A culture of secrecy has been a historic problem for most Canadian national security agencies in the past (see Craig Forcese, Staying Left of the Bang: Fixing Canada's Dysfunctional System of Parallel CSIS/RCMP Anti-Terror Investigations). Authoritative "shall" language will ensure essential disclosure is made for this class of information. National security agencies must begin to talk to each other efficiently in order to be effective in protecting Canadian interests. Non-national security agencies tend not to generate intelligence. Information from the CRA is not likely to threaten ongoing investigations like information from the Communications Security Establishment. The concern with intelligence-to-evidence should be relegated to the kinds of information that may pose a threat to national security if it were made part of a criminal disclosure.

The second classification should be for information with a low risk of affecting the "biographical core" of personal information. There is a low risk that disclosing this information would infringe upon a person's *Charter* rights, such as their right against an unreasonable search and seizure. Because of this lower risk, this kind of information should not be subject to the review and oversight concerns mentioned above. Limited judicial resources can then be dedicated to more sensitive kinds of information, which will also make the global process of information sharing more efficient. It may still be possible that information obtained for one purpose will violate a person's privacy expectations when it is used for a different purpose by another agency. It would then fall to the disclosing institution to ensure that privacy interests are protected by seeking judicial oversight.

This leads to a third classification: information that has a high risk of affecting an individual's "biographical core." Medical records, banking, and international travel are all examples of the kinds of private information that may necessitate a heightened review or oversight process. Therefore, when this classification of information is shared, a warrant should be issued before sharing the information to ensure privacy interests are protected.

Finally, there must be more consideration for the threat of a metadata analysis than what is currently in place. Metadata is information about information (Ann Cavoukian, A Primer on

Metadata: Separating Fact from Fiction at 3). A single piece of innocuous data could be harmless on its own but the combination of that same data point with hundreds of others to create grounds for more intrusive searches must attract a heightened level of oversight. This kind of analysis has the potential to derive information about an individual that is deeply personal. The potential for metadata analysis is not a category on its own. Rather, it is a concern that must be considered whenever information is pooled from various institutions. Precisely how to deal with metadata concerns is beyond the scope of this proposal; however, we recognize that it is a valid danger that must be considered.

Recommendation: Classify information using three categories – information obtained via a warrant, information with a low risk of impacting an individual's "biographical core," and information with a high risk of impacting the "biographical core."

Part II: Disclosing Institutions

A. Broad Disclosers

SCISA applies to a broad array of potential disclosing institutions, specifically to any "Government of Canada institution" (*SCISA*, ss 2 and 5(1)). *SCISA/SCIDA* defines "Government of Canada institution" as an institution listed in Schedule 2 (including the Communications Security Establishment) and a "government institution" under s 3 of the *Privacy Act*, RSC 1985, c P-21. The *Privacy Act* defines "government institution" as any parent Crown corporation or their wholly-owned subsidiary, as defined by s 83 of the *Financial Administration Act*, RSA 2000, c F-12, and "any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule," which includes a list of 147 entities (s 3). This list ranges from the Department of Health to Statistics Canada to various Port Authorities. Bill C-59 will not amend the definition of "Government of Canada institution" (Bill C-59, s 115).

This application of *SCISA*'s disclosure regime to such a large number of disclosing institutions could be problematic. Kent Roach and Craig Forcese have voiced concerns about the amount of information so many institutions could convey, particularly, as discussed above, in the age of Big Data, metadata analysis, and improved data storage technologies (see *False Security* at 157 & 166). We echo their concern for the following reasons. First, *SCISA*'s application to so many disclosing institutions increases the risk of violating Canadians' privacy rights by unnecessarily or accidentally sharing their information. In fact, in the first year that *SCISA* was in force, the Office of the Privacy Commissioner of Canada (OPCC) found instances where information was disclosed about family members of individuals under investigation, despite not meeting *SCISA*'s relevance threshold for disclosure (see OPPC, 2016-2017 Annual Report at 58). Second, there is the risk of information overload, where recipient institutions receive more information than they can reasonably process. This is a concern because if all information is deemed important, then effectively, none of it is. If too much information is shared, it would take longer to analyse and would make determining what is significant more difficult, while making it easier to miss something, much like the proverbial "needle in a haystack". Although information sharing is important, it must occur in a controlled way to ensure not only protection of privacy rights but also minimal risk of information overload and related inefficiencies.

One way to address this problem is to classify disclosing institutions as sources based on the type and quantity of information they collect that is relevant to national security and that may impact privacy interests. As explained in Part I, some organizations are more likely to have certain types of information than others. Institutions like CSIS and the RCMP would be in the "top" category because they collect large quantities of information relevant to national security and to privacy interests, while institutions like the Canadian Museum for Human Rights and the National Film Board would be in the "bottom" category because they collect little of that type of information. Institutions like Port Authorities would fall in the middle because they are likely to have some of that information – such as information gathered when leasing port operations to private terminal operators – but not as much as an institution like CSIS.

Classifying disclosing institutions like this would help make the number of disclosing institutions more manageable. Classification would help recipient institutions streamline what information should be given the highest priority for processing and indicate to disclosing institutions which of them has a larger burden to disclose and to be more careful about privacy interests. The purpose is not to create more bureaucracy, but to create a basic "flagging" system to assist institutions in reducing inefficiencies and being mindful of civil liberties.

Recommendation: Classify disclosing institutions based on the type and quantity of information they collect that is relevant to national security and may impact privacy interests.

B. Operationalizing *SCISA/SCIDA*

The operative provision of *SCISA*, section 5, has received critiques about its threshold for disclosure. Because those arguments have been addressed by others, including the Canadian Civil Liberties Association and Professor Kent Roach, we will not address them further (see briefs provided to the Standing Committee on Public Safety and National Security).

To the government's credit, though, the amendments in Bill C-59 seem to take some of those critiques to heart because the new *SCIDA* will require disclosing institutions to complete several internal assessments prior to disclosure. They will need to assess the information's usefulness to national security and its contribution to the jurisdiction or responsibilities of the recipient institution (Bill C-59, s 118 (proposed *SCIDA*, s 5(1)(a))), as well as ensure that it does not affect privacy interests more than reasonably necessary (Bill C-59, s 118 (proposed *SCIDA*, s 5(1)(b))) and that it is accurate and was reliably obtained (Bill C-59, s 118 (proposed *SCIDA*, s 5(2))). While these changes are a step in the right direction, this is a significant amount of assessment, and the legislation does not provide support for any of it, other than encouraging information sharing agreements between institutions that regularly share information (*SCISA*, s 4(c); Bill C-59, s 117(2)).

After studying the first six months of *SCISA* being in force, the OPCC concluded that government-wide guidance is important to operationalize *SCISA* (see OPCC 2015-2016 Annual Report at 20). Unfortunately, the OPCC also found that the DeskBook (link not available, but see *Security of Canada Information Sharing Act*: Public Framework) prepared by Public Safety Canada to support *SCISA*'s implementation in government institutions lacked specificity about how to share information while respecting privacy rights (2015-2016 Annual Report at 18). The

quality of the training government employees received about information sharing is also a concern. Furthermore, out of the five institutions that had collected or disclosed information under *SCISA*, only three had related policies or guidance documents, but they also lacked enough specificity to meaningfully help staff determine whether *SCISA*'s thresholds had been met (2015-2016 Annual Report at 19-20). In the second phase of this review, the OPCC also found a lack of internal procedures for operationalizing *SCISA* (2016-2017 Annual Report at 58). Guidance is particularly important in relation to privacy interests because government privacy violations are unlikely to come before a court for review, and institutions should not be tempted to use disclosure as an end-run around the *Charter* to obtain information for which they would otherwise need a warrant (see Craig Forcese, Intelligence Sharing).

For these reasons, the government should provide guidance for how to operationalize *SCISA/SCIDA*. Although it is impractical to have oversight for every disclosing institution, there should be guidance or processes in place to assist institutions in making the assessments needed to disclose information. For example, this could mean creating a more comprehensive DeskBook or implementing a training program. Classifying both the information, as mentioned in Part I, and the disclosing institutions could be helpful to streamline development of policies and guidance documents by developing policies specific to each category, rather than for each institution. For example, more guidance would be necessary for higher category institutions that have more information to share, like CSIS, but less would be needed for lower category institutions that have less information to share, like the National Film Board. Implementing guidance documents or policies about how to make the above assessments would help to alleviate civil liberties concerns, as well as reduce efficiency problems and encourage institutions to actually use *SCISA/SCIDA.*

Finally, despite concerns about information overload, it seems that institutions have been underutilizing *SCISA*'s powers. As mentioned above, the OPCC found that only five institutions used *SCISA*'s authority in its first six months (2015-2016 Annual Report at 17). It also found that thirteen of the seventeen recipient institutions used pre-existing authorities for sharing information (at 18) and that most disclosures were made in response to requests for information about individuals who were already being investigated (2016-2017 Annual Report at 58). Although OPCC's reviews focused on the early days of *SCISA* being in force, they seem to indicate a reluctance to utilise *SCISA*. Of course, cultural barriers to information sharing exist, but perhaps if appropriate policies were created to inform institutions how information sharing should work, they would be more inclined to use *SCISA* and to use it properly. Alternatively, if policies prove ineffective in that regard, Ministerial Directives could be issued outlining expectations for information sharing.

Recommendations: 1) Create policies or guidance documents for disclosing institutions about how to make the assessments required under *SCIDA*. If necessary, utilise Ministerial Directives. **2)** Use classifications of information and disclosing institutions to help streamline the creation of policies and guidance documents.

C. Review

Bill C-59 will amend *SCISA* to require record keeping for disclosed information, and these records will be sent to the National Security and Intelligence Review Agency (NSIRA) annually for review (Bill C-59, s 119(1) and (2)). This is an improvement to the absence of review in *SCISA* currently, but realistically, NSIRA will have limits to its review capacity, given its broad mandate (Bill C-59, s 8). This is a concern shared by Kent Roach, given the potential breadth of information sharing under *SCISA/SCIDA* (Brief to the Standing Committee on Public Safety and National Security on Bill C-59 at 6). Again, classification of disclosing institutions could be used to help streamline review. For instance, "top" category institutions could have their disclosure records reviewed annually because they encounter more information impacting privacy interests, whereas "bottom" category institutions could have their disclosure reviewed every five years because they encounter less privacy-sensitive information.

Additionally, adding an express requirement to document the weighing of privacy interests would help NSIRA do its job more efficiently. In the disclosure records, institutions will have to describe the information used to determine whether disclosure was authorized under *SCIDA* (Bill C-59, s 119(1)), and one of the required assessments in authorizing disclosure will be that privacy interests are not affected "more than is reasonably necessary in the circumstances" (Bill C-59, s 118). Although this implies that consideration of privacy interests should be included in the disclosure records, we agree with the Canadian Bar Association that there should be an express requirement (see Bill C-59 – *National Security Act, 2017* at 33) – specifically, in *SCIDA* s 9(e), which currently states: "a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act" (Bill C-59, s 119(1)). By ensuring NSIRA will have information about how privacy interests were considered, rather than hoping institutions include specifics, NSIRA will be able to review disclosure records more efficiently and effectively.

Recommendations: 1) Use classifications of disclosing institutions to streamline the review process. **2)** Amend s 9(e) in *SCIDA* to read: "a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act, including details about how privacy interests were weighed against security interests."

Part III: Receiving Institutions

A. Necessity Standard

Neither *SCISA* nor Bill C-59 contains any obligations on recipient institutions; in fact, there is no mention of recipient institutions in *SCISA* or the proposed *SCIDA* at all. The absence of provisions in *SCIDA* relating to recipient institutions means that they are governed by the *Privacy Act*, which has negative consequences. For instance, this implies that recipient institutions would be held under the relevancy standard of the *Privacy Act* for collecting information rather than a necessity standard. The *Privacy Act* allows a government institution to collect personal information belonging to Canadian citizens as long as it "relates directly to an operating program or activity of the institution" (s 4). This relevancy standard is not only too low for disclosing institutions but even more so for recipient institutions as they are the ones who would be in possession of the disclosed information. Although Bill C-59 somewhat elevated the standard of disclosure for disclosing institutions from relevancy to whether the disclosure will

"contribute to the exercise of the recipient institution's jurisdiction…in respect of activities that undermine the security of Canada" (Bill C-59, s 118 (proposed *SCIDA*, s 5(1)(a))), it fails to provide a standard for recipient institutions at all. There would be two separate standards for government institutions covered under *SCIDA*: a standard that incorporates some aspects of a necessity threshold for disclosing institutions and a relevancy standard for recipient institutions.

Disclosing institutions would not be in the best position to determine whether disclosure will truly contribute to the exercise of the recipient institution's jurisdiction in respect of activities that undermine the security of Canada or whether disclosure will affect any person's privacy interest more than is reasonably necessary in the circumstances, as stipulated by s 5 of *SCIDA*. The recipient institutions could be obligated to share enough information with the disclosing institutions so as to allow them to make an informed decision about whether the information requested would affect a person's privacy interest more than is reasonably necessary. Since this seems unlikely, as the Privacy Commissioner of Canada points out, under the newly proposed *SCIDA*, it would make more sense for recipient institutions to be held to a higher standard and to place more obligations on them for proper handling of personal information (see Letter to the Chair of Standing Committee on Public Safety and National Security at 5). They are in the best position to ensure that the information they have requested does not affect a person's privacy interest more than is reasonably necessary and they are also the ones who end up in possession of this information. The burden should, therefore, fall more on the recipient institutions as they would have all the details about the investigation that they would be conducting. We agree with the British Columbia Civil Liberties Association (BCCLA) that a standard higher than relevancy needs to apply to information collection under *SCISA* by recipient institutions in order to sufficiently protect privacy rights (see Written Submission of the British Columbia Civil Liberties Association to the Standing Committee on Public Safety and National Security on Bill C-59 at 18).

Another inevitable issue for recipient institutions under *SCISA* is handling the vast amount of information that would be collected by them under the relevancy standard. This would end up slowing down the process in an emergency situation and would make it more difficult to identify real security threats. Simply having an excess amount of information is meaningless and potentially harmful unless there is a system in place to properly analyze that information and produce results efficiently. If only a relevancy standard is applied to collect personal information, recipient institutions may end up collecting mass information about Canadian citizens that could be broadly relevant to their investigation but could impact a person's privacy interests more than reasonably necessary.

A standard of relevancy places too much power in the hands of recipient institutions, who would be able to keep a profile on almost all Canadians by justifying the information as relevant. Relevancy is a much lower standard than necessity and should not be applied when dealing with privacy of Canadians as it would lead to excessive information collection.

Recommendation: Amend s 5 in *SCIDA* to require a necessity threshold to be imposed on recipient institutions.

B. Privacy Safeguards

Since *SCIDA*'s preamble expressly refers to the need for government institutions to share information in a manner that respects the *Privacy Act*, it means that once information is shared, it is subject to limitations on its use, retention and destruction. Without having specific record-keeping rules in *SCIDA*, it would be impossible to determine whether the recipient institutions are in compliance with *SCIDA*, the *Privacy Act* and other legal obligations. These rules are needed to hold recipient institutions accountable for the information they receive from disclosing institutions. It would be impossible to know whether they are meeting *SCIDA*'s requirements, and would make governance, oversight and evaluation of *SCIDA*'s effectiveness challenging (see OPCC 2016-2017 Annual Report at 58).

Another reason for record-keeping provisions for recipient institutions in *SCIDA* is to have consistency among all seventeen listed institutions and have the same retention rules to prevent confusion when time comes to share that information with other agencies. It would make little sense if some recipient institutions retained information for longer than other institutions and simply shared that information with them at a future time. Therefore, to maintain consistency and effectiveness of information collection by the various agencies implicated by *SCIDA*, it is crucial to add the proper record-keeping, retention and destruction rules for recipient institutions in *SCIDA.*

Furthermore, without clear retention and destruction rules, information collected by recipient institutions can potentially be retained for an unlimited amount of time and be used completely out of context along with new information obtained in the future. There are concerns around unauthorized and excessive collection and retention of personal information. The absence of clear policies may result in inadequate information-handling by recipient institutions that may pose a threat to privacy (see OPCC 2016-2017 Annual Report at 58). Without explicit record-keeping provisions for recipient institutions in *SCIDA*, we will continue to have privacy concerns for Canadians. Having these provisions will allow Canadians to better understand how their information is being shared within government (see BCCLA submission at 19).

Recommendation: Amend s 9 in *SCIDA* to include recipient institutions under record-keeping, and add a limit of two years on retention of personal information collected by recipient institutions. After this time period, the information collected must be destroyed in a prescribed manner. An exception should be added for ongoing investigations in which the information is being used.

C. Review and Oversight

Since recipient institutions under *SCISA* collect personal information belonging to Canadians, it is highly important to have the proper review and oversight mechanisms in place to ensure that information does not end up being used improperly and in violation of the *Privacy Act.* Recipient institutions should conduct a review to ensure that the information received truly relates to the purpose of *SCISA*, which is to share information about an activity that undermines the security of Canada (*SCISA*, s 5(1)). Review of information received should be conducted by recipient institutions because they have the most complete information and are the ones who would be

retaining and using that information in their investigations. Also, if a disclosing institution shares information by mistake or because in that institution's opinion, the information was relevant to the recipient institution's investigation but it actually is not, then if it is not vetted by the recipient institution to ensure it meets the threshold for disclosure under *SCISA*, that institution would end up in possession of and retaining information that is not necessary or relevant to the jurisdiction of the recipient institution in respect of an activity that would undermine the security of Canada.

Recommendations: 1) Amend s 9(2) in *SCIDA* to include recipient institutions in the review obligations to the NSIRA. **2)** The disclosing and recipient institutions should provide a copy of every record to the Office of Privacy Commissioner. This will allow multiple checkpoints and provide enough oversight to ensure that the personal information shared and collected among government institutions meets the privacy thresholds.

D. Listed Institutions

Currently, there are seventeen listed recipient institutions in Schedule 3 to *SCIDA*. These institutions can collect vast amounts of personal information belonging to Canadians. Only four of the seventeen institutions have actually been involved in investigations and received information from disclosing institutions under *SCISA*. These four institutions are CSIS, RCMP, Canada Border Services Agency (CBSA), and Immigration, Refugees and Citizenship Canada (IRCC). A full review by the government is needed to ensure that only institutions directly relevant to Canada's national security matters are listed, as recommended in the Report of Standing Committee on Access to Information, Privacy and Ethics (see Report of the Standing Committee on Access to Information, Privacy and Ethics at 27). This will limit access of personal information to only those institutions who are actively involved in Canada's national security matters and would avoid future privacy issues.

Recommendation: Amend s 10(3) of *SCIDA* to require a review every two years to determine whether an institution should remain listed or be deleted from Schedule 3 to *SCIDA* in order to keep the institutions list very narrow. This review should take into account the number of investigations each recipient institution has conducted in the past years.

Conclusion

Overall, Bill C-59 will make some positive amendments to *SCISA*, but there are still areas that need improvements. In Part I, we recommended that information should be divided into three categories to streamline disclosure and bolster privacy protections. In Part II, we recommended requiring privacy considerations to be explicit in disclosure records and classifying disclosing institutions to streamline information processing, assist review, and aid in developing policies and guidance documents. In Part III, we recommended holding recipient institutions to account, similar to disclosing institutions, by imposing a necessity threshold for collecting information, adding record-keeping requirements, including recipient institutions in the review process, and regularly assessing the listed recipient institutions. As we know from the Air India Inquiry, information sharing is important to national security, but it must be executed in a way that both respects Canadians' privacy rights, while also balancing the efficiency and efficacy of our

national security organizations. We believe these recommendations strike this balance and would greatly improve *SCISA*.

This post may be cited as: Ben Allison, Lindsay Kvellestad, and Wajeeha Sattar "Proposed Security of Canada Information Sharing Act Amendments" (20 April, 2018), online: ABlawg, http://ablawg.ca/wp-content/uploads/2018/04/Blog_BA_LK_WS_SCISA.pdf