Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

MAR 0 5 2018

The Honourable John McKay, M.P.
Chair, Standing Committee on Public Safety and National Security
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Chair:

I am writing today to share my views on Bill C-59, *An Act Respecting National Security Matters*, which introduces a wide range of measures intended to strengthen Canada's national security framework in a manner that safeguards the rights and freedoms of Canadians.

As I indicated in my appearance before the Standing Committee in December, on the whole, I find it represents a step in the right direction but, particularly as it relates to information sharing provisions, it is insufficient to meet the standards that I believe are needed to ensure that national security activities are undertaken and overseen in a way that respects Canadians' privacy rights. I will take this opportunity to elaborate on my remaining concerns, and address outstanding questions I was asked during my appearance. I am also taking the opportunity to provide an updated list of recommendations, which includes recommendations related to the parts of the Bill I did not address during my appearance.

In previous Parliamentary submissions on Bill C-51, the *Anti-Terrorism Act, 2015*, and in a submission I made with my provincial and territorial colleagues on the federal government's national security consultation, I highlighted the need for rigorous legal standards around the collection and sharing of personal information, effective oversight, and minimization of risks to the privacy of ordinary, law-abiding Canadians (in part through prudent retention and destruction practices). Specifically, I indicated that the "law should prescribe clear and reasonable standards for the sharing, collection, use and retention of personal information, and compliance with these standards should be subject to independent and effective review mechanisms, including the courts." It is with this analysis in mind that I offer the following comments and recommendations.

Effective review and oversight

As I noted in December, Bill C-59 would create a new expert review body with a broad mandate to examine the activities of all departments and agencies involved in national security. Recently, Parliament also created through Bill C-22 a new National Security and Intelligence

.../2

Committee of Parliamentarians. Both of these bodies will be able to share confidential information and generally cooperate so as to produce well informed and comprehensive reviews that reflect considerations by experts and elected officials.

These developments are most welcome but they are clearly insufficient. In my view, effective review of national security activities must include both parliamentary and expert review, and the latter must include both national security and privacy experts. Why privacy experts? Because the work of national security agencies depends in large part on personal information; it is their "lifeblood"[1]. The OPC is the federal centre of expertise in privacy and personal data protection. Canadians are concerned that anti-terrorism efforts in government not unduly impede their privacy rights, and they expect my Office to play a role in ensuring balance.

Bill C-59 does not amend the *Privacy Act*, so my existing authorities appear to be untouched, but the only body with explicit authority to play a role in relation to Part 5, the renamed *Security of Canada Information Disclosure Act*, is the National Security and Intelligence Review Agency (NSIRA), as articulated in section 9 of Part 5 and section 39 of Part 1. C-59 is completely silent about my role, which leads to issues around interpretation.

The May 2017 Report of the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on *Safeguarding Canada's National Security While Protecting Canadians' Privacy Rights: Review of The Security of Canada Information Sharing Act (SCISA)* called for clarity with respect to the interplay between SCISA and the *Privacy Act* and recommended amendments to "stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the *Security of Canada Information Sharing Act*."[2] The Canadian Bar Association[3] echoed that call and I would agree. However, ETHI further recommended amendments to clarify that the *Privacy Act* takes precedence over SCISA[4]. That is, in effect, saying that privacy trumps security. I do not agree with this recommendation as the longstanding position of my Office is that privacy and security can and must co-exist, in a balanced fashion.

.../3

[1] Kevin Brosseau, Deputy Commissioner, RCMP, SECU meeting 88 (November 30, 2017); Wesley Wark, Professor, Public and International Affairs, SECU meeting 89 (December 5, 2017); Anil Kapoor, Barrister, ETHI meeting 39 (December 6, 2016)

[2] Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Safeguarding Canada's National Security While Protecting Canadians' Privacy Rights: Review of The Security of Canada Information Sharing Act* (SCISA) – Recommendation 5 (b)
https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP8899455/ethirp05/ethirp05-e.pdf

[3] Canadian Bar Association, Submission on the ETHI Study of the *Security of Canada Information Sharing Act* (SCISA), January 2017 (http://www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR8718954/br-external/CanadianBarAssociation-e.pdf)

[4] Recommendation 5 (a).

Therefore, I recommend the following:

RECOMMENDATION 1: That Part 5 be amended to stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the *Security of Canada Information Disclosure Act.*

RECOMMENDATION 2: That Part 1 be amended to clarify any ambiguity regarding the role of the Privacy Commissioner and add a provision to the following effect: "Nothing in this Act or any other Act of Parliament should be construed as limiting the powers of the Privacy Commissioner to conduct an investigation to ensure compliance with sections 4 to 8 of the *Privacy Act*."

There is, however, no ambiguity on whether my Office would be able to share confidential information with the NSIRA and the new committee of parliamentarians. It is clear that we would not, and actually we would be prohibited by existing provisions in the *Privacy Act* from sharing such information. This means that the comprehensive review process offered in Bill C-59 as a fundamental element to bring balance between security and respect for rights would stop short of the objective, by leaving privacy experts out of integrated review. I am at a loss to understand why. If the fear is of duplication between our work and that of other review bodies, let me explain how bringing the OPC firmly within the family of review bodies would not only bring required expertise but would enhance efficiency and reduce overlaps.

We, as the federal centre of expertise for privacy, do not see ourselves as overseeing *all* aspects of national security activities, far from it. Nor is it our position that review and oversight bodies proposed in C-59 will have no knowledge of privacy law. However, because we have deep and extensive expertise in the area of privacy and personal information, derived from our review of programs government wide, we think we have value to add and we believe other review bodies, and national security agencies, could benefit from that experience.

In practical terms, that means being able to discuss files with other oversight bodies, including their classified information, so that review is fully integrated and grounded in relevant facts, as opposed to the theoretical discussions divorced from factual details that we currently have. Being granted the authority to share classified information with other oversight bodies would also enhance efficiency by allowing us to determine up front who is best placed to review a given issue and how an efficient division of roles can be defined. This would have the added benefit that national security agencies may not have to answer redundant questions from oversight bodies.

An example of what I mean can be found in our review of the measures taken by CSIS to comply with Justice Noel's October 2016 decision regarding CSIS' Operational Data Analysis

.../4

Centre or ODAC.[5] Justice Noel had ruled that CSIS acted without authority when it retained third party, non-threat related metadata belonging to individuals who were not targets of CSIS investigations. Minister Goodale mandated Security Intelligence Review Committee (SIRC) to review whether the measures taken by CSIS to give effect to Justice Noel's ruling were adequate. But we at the OPC also decided to review these measures, as the judgment clearly involved privacy issues. In fact, we were invited to examine these issues by the then-Director of CSIS.

Knowing there was a potential for inefficiencies between our work and that of SIRC, the two review agencies discussed, at the beginning of the process, whether we could find a way to share our respective approaches, define roles and reduce overlap, but we concluded we could not lawfully do this. At the end of our review process, we then met to see whether we could compare notes and avoid contradictions in findings. That led to a circuitous discussion, where we both spoke at high levels of abstraction so as not to breach our confidentiality obligations.

It is critical that existing prohibitions on information sharing between oversight bodies be lifted in order to ensure review mechanisms operate effectively and to meet the objective of bringing balance between security and respect for rights. Consequently, I recommend OPC be given the legal flexibility to share information and to determine when and how to cooperate to avoid duplication and bolster efficiency of reviews. Furthermore, information exchange should be allowed to flow both ways between OPC and NSIRA as well as other relevant review and oversight agencies.

RECOMMENDATION 3: That the OPC should be among the review bodies having the legal authority and flexibility to share confidential information obtained in the course of their work and to determine when and how to cooperate to avoid duplication, increase efficiency and produce more comprehensive reports. Sections 22 and 23 of the *National Security Committee of Parliamentarians Act* could be used as a model to provide all review bodies with similar authority to share information "related to the fulfillment of the mandate" of the other review bodies. These provisions could be transposed in the form of parallel amendments to:

i. the *Privacy Act*;
ii. Part 1 of C-59, which creates and empowers the NSIRA, and;
iii. the *National Security Committee of Parliamentarians Act*.

Need for rigorous legal standards

.../5

[5] X (Re), [2017] 2 FCR 396, 2016 FC 1105

SECURITY OF CANADA INFORMATION DISCLOSURE ACT (SCIDA)

When Bill C-51 enacted SCISA, I indicated that among my concerns was the fact that the relevance standard for sharing was set too low, and that there was an absence of clear data retention and recordkeeping requirements and a lack of information-sharing agreements and privacy impact assessments.

The relevance test is too permissive because it casts too wide a net and creates undue risks for ordinary citizens who pose no threat to national security. The government seems to recognize that a relevance standard does not sufficiently protect privacy because it is suggesting changes to section 5 of SCIDA. In its response to ETHI, the government said: "The key issue regarding the threshold is the need to establish specific decision making parameters for the discloser of information that will protect individual privacy but not cause undue delays in the information sharing process."[6] The proposed new section 5, particularly paragraph 5(1)(b), incorporates some aspects of a necessity threshold for disclosures but falls short of adopting what officials refer to as "strict necessity".

In order to adequately protect privacy rights, this limited progress in increasing the threshold for disclosure would have to be accompanied by more complete changes to the standard applicable to receiving institutions. However, rather than imposing rigorous standards for receiving institutions, Bill C-59 removes them from the application of SCISA. This has implications not only for the threshold issue but also for retention, record-keeping and other privacy safeguards. Information sharing involves two parties and, to protect rights, rules are also required for receiving institutions. If relevance is not adequate for disclosing institutions, it is also inadequate, even more so, for receiving agencies because: they are aware of the parameters of their mandates; they often will have more time to assess necessity than sending institutions, given the analytical work done in receiving institutions can take time, time that sending institutions may not have in an emergency situation. These institutions are perfectly capable of applying the classic, internationally established necessity test, and should be required to do so.

We understand that the government intention is for receiving institutions to continue to be governed by the *Privacy Act*, or their specific enabling legislation where applicable. The current *Privacy Act* uses the wording "relates directly". As your committee recommended in its May 2017 report on Canada's national security framework, we also recommend that a dual

.../6

[6] Government Response to the Report by the Standing Committee on Access to Information, Privacy and Ethics, *Safeguarding Canada's National Security while Protecting Canadians' Privacy Rights: Review of the Security of Canada Information Sharing Act (SCISA)*: https://www.ourcommons.ca/content/Committee/421/ETHI/GovResponse/RP9066704/421_ETHI_Rpt05_GR/421_ETHI_Rpt05_GR-e.pdf , p.3.

threshold be adopted for information sharing, with necessity and proportionality applying to receiving institutions.

I note that CSIS has a standard of strict necessity under the *CSIS Act*, and that Part 3 of Bill C-59 incorporates essentiality. Therefore, I see no reason why a necessity standard cannot be imported into Part 5, which would also be consistent with international norms. Therefore, I reiterate my recommendation:

> **RECOMMENDATION 4:** That Bill C-59 be amended to require the necessity and proportionality threshold to apply to receiving institutions, either by way of an amendment to SCIDA or by way of a consequential amendment to section 4 of the *Privacy Act*. In this way, a dual threshold would apply to national security information sharing: the new s.5 of SCIDA would apply to disclosing institutions and receiving institutions would be governed by a necessity and proportionality threshold.

Retention and Destruction

The issue of thresholds leads directly to the ancillary question of retention and destruction of personal information that does not meet, or no longer meets, the recipient's threshold, particularly as it relates to law-abiding citizens who pose no threat. If the threshold for collection is higher than the threshold for disclosure (which is currently the case at least for CSIS), then retention rules are required to ensure recipient institutions discard without delay information that does not meet their criteria.

Similarly, even if one accepts that government sharing of information related to law-abiding citizens may lead to the identification of new threats to national security, once that information is analyzed and leads to the conclusion that someone is not a threat, it should no longer be retained. Otherwise national security agencies will be able to keep a profile on all of us. This is consistent with the decision of the European Court of Justice in the Passenger Name and Record case involving Canada, decided in July 2017.[7] In that case, the highest court in the European Union held that retention of information of individuals found to pose no threat to national security did not meet legal requirements of necessity and proportionality and were incompatible with fundamental human rights.

A recent example of this problem was illustrated in our *Audit of Canada Border Services Agency – Scenario Based Targeting of Travelers* (2017)[8], summarized in my latest annual report

.../7

[7] *Decision of the Court of Justice of the European Union, Opinion 1/15 of the Court (Grand Chamber)*, 26 July, 2017: http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=EN

[8] OPC *Audit of Canada Border Services Agency – Scenario Based Targeting of Travelers* (2017): https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/#toc_0_2.

to Parliament. The objective of this program is, through the use of algorithms, to identify people and goods bound for Canada that may pose a threat to security and safety. Scenario Based Targeting (SBT) uses advanced analytics to evaluate the data of all travelers, collected from air carriers, against a set of conditions or scenarios, such as age, gender and nationality using database and open-source checks.

We found that large numbers of travelers – approximately 60,000 a year – are identified by scenarios as deserving extra scrutiny and therefore being potential security threats at the beginning of the process. And while CBSA has processes in place, including information sharing with domestic and international partners, to limit the number of individuals for whom targets are eventually issued, we also found that agreements with these partners do not limit retention and therefore do not mitigate against potential for ongoing suspicion of people who have been determined to not be a threat. We recommended that CBSA should ensure that only the personal information which is directly related to and demonstrably necessary for the purposes of administering the SBT program is collected and retained, and that CBSA should revise its MOUs with domestic and international partners to ensure they contain specific provisions to limit retention and use of data that is obtained from CBSA for purposes of database checks.

I therefore recommend:

RECOMMENDATION 5: That Bill C-59 be amended to impose on recipient institutions retention and destruction rules in respect of personal information that does not meet or no longer meets the recipient's threshold for collecting the information. More specifically, we recommend an explicit provision for record disposal by receiving institutions in these three instances:

i) any personal information that does not meet the collection threshold;
ii) any personal information that the recipient institution does not believe "will contribute to the exercise of its jurisdiction or the carrying out of its responsibilities"; and,
iii) any personal information which, after analysis, leads to the opinion that the individual concerned is not a threat to national security.

Record-keeping

As for the record-keeping rules for *disclosing* institutions, we are generally pleased with the elements set out in subsection 9(1) of SCIDA. These elements are consistent with the record-keeping elements we recommended in the context of our submission on Bill C-51, as well as our

.../8

review of information-sharing practices under SCISA (the results of which were tabled in our most recent Annual Report).[9] The inclusion of the requirement suggests the government accepts the view that record-keeping is required for effective review. In our opinion, these same record-keeping obligations should apply equally to *receiving* institutions given that their actions may directly affect individual rights.

Therefore, we recommend:

> **RECOMMENDATION 6:** That SCIDA be amended so that the record keeping obligations found in subsection 9(1) apply not only to disclosing institutions but also to recipient institutions.

I note that subsection 9(2) of SCIDA requires that copies of these records be shared only with the NSIRA. In order to enable my Office to play a meaningful concurrent role in overseeing the sharing of personal information in a national security context, institutions should likewise be obligated to provide copies of these records to OPC, on request. Consistent with recommendations 1 and 2, this would confirm the continued application of the *Privacy Act* and the jurisdiction of the OPC.

> **RECOMMENDATION 7:** That a new subsection be added to section 9 of SCIDA: "For greater certainty, the Government of Canada institution must also, on request by the Privacy Commissioner under s.34 of the *Privacy Act*, provide the Commissioner with a copy of any record requested that it prepared under subsection (1)."

Information-Sharing Agreements (ISAs) and Privacy Impact Assessments (PIAs)

In order to give effect to the enhancements on governance and accountability around Canada's national security framework proposed by C-59, it is essential that ISAs and PIAs be viewed as an integral part of this framework.

The requirement to prepare PIAs, which describe and quantify risks to privacy, and propose solutions to eliminate or mitigate them to an acceptable level, remains at the level of policy which (as we have seen through past investigations and reviews) is inconsistently followed across government, if at all. Indeed, we have received very few PIAs from government institutions whose mandate is primarily the protection of national security.[10] It is remarkable that,

.../9

[9] OPC Annual Report, "Review of the Operationalization of the *Security of Canada Information Sharing Act" (2017):* https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-4-2

[10] Since 2009, we have received one each from CSIS and CSE related to their national security activities and none from DND

almost three years after the law's adoption, we have not received any SCISA-specific PIAs. This law, after all, was the subject of extreme scrutiny and concern, from a privacy perspective, yet the government did not see fit to follow its own policy and formally assess the privacy risks of that legislation. If this law was not the subject of a PIA, why have a PIA policy at all?

Information sharing agreements (ISAs) are also key to effective privacy protection and transparency. ISAs would provide more specificity than the core standards set out in legislation, and, if crafted properly, would go a long way to ensure that only appropriate and accurate information is shared. During our audit of SCISA, we found that although ISAs were, for the most part, in place, most lacked specific privacy provisions that we would expect to see in such agreements. As noted in a submission to Public Safety Canada's Green Paper *Our Security, Our Rights* and our appearance before this Committee[11], we continue to call for inclusion of the following data elements in information-sharing agreements, as a legal requirement: the specific elements of personal information being shared; the specific purposes for sharing; limitations on secondary use and onward transfer, and other measures to be prescribed by regulations, such as specific safeguards, retention periods (beyond those covered by recommendation 5) and accountability measures.[12]

We maintain our recommendation that these important mechanisms be elevated to legal requirements if they are going to be truly effective in enabling information-sharing activities from an operational perspective, while mitigating serious privacy risks, particularly to law-abiding citizens.

> **RECOMMENDATION 8:** That information-sharing agreements and privacy impact assessments be made into legal requirements either by way of amendment to Bill C-59 in the national security context, or more generally, by way of amendments to the *Privacy Act*.

Rules and Standards Beyond SCIDA

It is important to note that not all information sharing for national security purposes takes place under SCISA/SCIDA. SCISA seeks to fill gaps in information sharing authorities in what the government referred to in its green paper as the "national security framework" (the whole body of law governing national security activities), but it is equally important to fill gaps in that framework's information sharing safeguards. It is well recognized that SCISA/SCIDA represents

.../10

[11] Appearance before the Standing Committee on Public Safety and National Security (SECU) on Public Safety's Green Paper, October 4, 2016: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20161004/

[12] OPC Submission, *Canada's National Security Framework* (December 2016) – URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205/

only a fraction (probably much less than 1 per cent) of all information-sharing activities for national security purposes. In fact, in our review of the operationalization of SCISA tabled in our recent annual report, we found that during the examination period, only five of the 17 institutions listed in Schedule 3 of SCISA had been engaged in information-sharing activities under the Act.[13] The bulk of information-sharing occurs outside of SCISA/SCIDA's provisions. If SCIDA is intended to strike the right balance from a policy perspective, these same principles should apply to all information-sharing. I would therefore recommend:

> **RECOMMENDATION 9:** That the rules and standards under SCIDA, amended as proposed above, should be extended to all domestic intra-governmental national security information sharing.

PRIVACY PROTECTION MEASURES AT THE COMMUNICATIONS SECURITY ESTABLISHMENT AND THE NOTION OF "PUBLICLY AVAILABLE INFORMATION"

By establishing its mandates in a stand-alone statute, Part 3 of Bill C-59 brings some much-needed clarity around the activities of CSE, in connection with foreign intelligence, cyber security and information assurance. The proposed authorization regime, which involves the approval of the Intelligence Commissioner, a retired judge independent from the executive branch of government, represents an important improvement. Furthermore, I recognize that C-59 includes the general requirement at section 25 that measures be put in place to protect the privacy of Canadians and persons in Canada regarding the use, analysis, retention and disclosure of information collected by CSE. This is bolstered by later provisions (sections 35 and 44) which incorporate elements of essentiality and necessity, which are strong privacy protection standards.

Paragraph 24(1)(a) permits CSE to acquire, use, analyze, retain or disclose publicly available information. Although CSE must ensure there are privacy-protective measures regarding the use, analysis, retention and disclosure of publicly available information, there do not appear to be restrictions on the collection of such information. We are of the view that, while the reasonable expectation of privacy attached to publicly available information is reduced, there remains a residual reasonable expectation of privacy that requires protection. Consequently, I recommend:[14]

.../11

[13] OPC Annual Report, "Review of the Operationalization of the *Security of Canada Information Sharing Act" (2017):* https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_scisa_2017/#toc3_1

[14] This echoes the recommendation by the Canadian Civil Liberties Association in its Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*, p. 10, Recommendation 18.

RECOMMENDATION 10: That section 24 be amended to add a limit to the activities listed in 24(1) namely: the measures shall be reasonable and proportional in the circumstances, having regard to the reasonable foreseeable effects on Canadians and people in Canada including on their right to privacy;

A further measure that could improve privacy protection concerns the definition of publicly available information. Part 3 defines this term as including information that is "published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise, or is available to the public on request by subscription or purchase". I believe this to be very broad[15], and while I appreciate the importance of that information for national security agencies, I have concerns regarding the legality of means that other actors may use to make information publicly available. For instance, while we acknowledge CSE's explanation that it will not purchase stolen information, will publicly available information always be lawfully obtained or created by a vendor, including in compliance with Canada's private sector privacy law (PIPEDA), notably its requirement for meaningful consent? It is important in a country governed by the rule of law that national security agencies not be able to use the fruits of activities that may not be criminal but are still unlawful. We therefore recommend as follows:[16]

RECOMMENDATION 11: That the definition of "publicly available information" in section 2 of Part 3 be amended to specify that information is published or broadcast lawfully, and that information obtained through purchase or subscription was legally obtained or created by the vendor.

We note that, in his brief provided to the Committee on December 6, 2017, the Commissioner for CSE recommended that the Intelligence Commissioner "should approve the active cyber operations in addition to the defensive cyber operations that are authorized by the Minister pursuant to subsections 30(1) and 31(1) of the proposed *Communications Security Establishment Act*."[17] We agree with this recommendation, as it addresses a gap in the Intelligence Commissioner's authority to approve activities under all CSE mandates.

.../12

[15] Under PIPEDA and its Regulations, there is a narrow definition of publicly available information - http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-7/page-1.html. Parliament may of course adopt a different definition in Bill C-59.

[16] This is consistent with Recommendation 17 by the Canadian Civil Liberties Association in its Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters,* p. 10.

[17] Brief submitted to SECU by the Office of the Communications Security Commissioner, December 6, 2017, http://www.ourcommons.ca/Content/Committee/421/SECU/Brief/BR9337287/br-external/CommunicationsSecurityEstablishmentCommissioner-e.pdf, p. 2.

CANADIAN SECURITY INTELLIGENCE SERVICE

Part 4 of C-59 introduces a new regime for the collection and use of datasets, largely in response to an October 2016 Federal Court ruling, in which the Court found that CSIS does not have the authority to retain associated data that has been assessed by CSIS as being non-threat related. At the same time, in that decision, the Court noted that Canadian intelligence agencies should be provided with proper tools for their operations[18], and that "evidence was produced establishing that the processing and analysis of associated data ha[d] yielded some useful intelligence results. In some cases, analysis of retained data in past cases indeed contributed to new investigative leads and other useful pertinent information."[19]

While this new regime will clearly extend the Service's authority to collect and use information, it includes independent review by the Intelligence Commissioner and, in the case of Canadian datasets, the Federal Court. In fact, Canadian datasets will be subject to various filters, including the Intelligence Commissioner for their creation, a short timeframe (90 days) for decision on retention by the Federal Court and ultimately, application of the "necessity" test for querying data, with IC approval required if under exigent circumstances. For their part, the retention of foreign datasets will require approval by the Intelligence Commissioner, which we believe meets the requirement for effective independent review.

YOUTH CRIMINAL JUSTICE ACT

During my appearance, I was asked whether I had concerns regarding the proposed changes to the *Youth Criminal Justice Act* vis-à-vis protecting the privacy rights of Canadian youth who are at risk of radicalization. I note that Part 8 of C-59 proposes, among other measures, to clarify the jurisdiction of youth justice courts, and to strengthen prohibitions against detention as a social measure. It also proposes to permit access to youth records for the purpose of administering the Passport Program, which allows for the revocation of passports in certain instances of criminality or national security concerns. Given the use of this information is restricted only to administration of the *Canadian Passport Order*, a case can be made that this represents an appropriate balance between privacy and security.

As to the larger issue of youth privacy, my Office has recently published a paper on online reputation[20] which examines the particular challenges for youth, who often have little or no option but to engage online (e.g. due to social pressures or requirements placed on them by

.../13

[18] X (Re) 2016 FC 1105, §264, p. 124 - http://cas-cdc-www02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20public%20judgment%20FINAL%20(ENG).pdf

[19] Ibid, §265

[20] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/

schools). They are also in a time of experimentation, in which boundaries are being tested. It is thus critical that youth be provided with a means of reinventing themselves as they mature and enter adulthood – a fact recognized by the existence of "clean slate" and other protective mechanisms in Canada and elsewhere.[21]

JUDICIAL REVIEW OF THE INTELLIGENCE COMMISSIONER'S DECISIONS

During my appearance before you in December, I was asked whether the decisions made by the Intelligence Commissioner (IC) should be subject to judicial review. After reflection, I am not convinced that this would be appropriate. For judicial review to come into play, the interests of an individual directly affected by a particular decision must be at stake; however, the IC's decisions under Part 2 of Bill C-59 are not of a nature that would directly affect the rights of an individual. It is also unclear how an individual would become aware of an IC decision, given the secrecy surrounding these decisions. That said, where acts authorized by the IC lead to consequences for individuals, the legality of those consequences would be subject to review as appropriate by the NSIRA, the National Security and Intelligence Committee of Parliamentarians, the courts, and my Office.

CONCLUSION

Bill C-59 is a step in the right direction in many aspects, notably with improvements in review and oversight. However, I maintain that the SCISA/SCIDA provisions are the weakest part and, on issues related to the sharing and retention of personal information, we do not believe Bill C-59 attains the standards of privacy that would adequately protect Canadians. We believe the adoption of our recommendations is necessary to achieve the balance between privacy and security that Canadians expect and to which they are entitled. I would be happy to elaborate on any of the issues mentioned above.

Sincerely,

Daniel Therrien,
Commissioner

Encl.

[21] This includes the *Youth Criminal Justice Act* (which prevents publication of the names of youth offenders, and limits access to youth records) and newer laws aimed at the online environment such as California's *Privacy Rights for California Minors in the Digital World*, which allows youth to remove or obtain removal of any information provided to a website, app or online service.

ANNEX A: List of Recommendations

RECOMMENDATION 1: That Part 5 be amended to stipulate that the *Privacy Act* continues to apply to all personal information disclosed pursuant to the *Security of Canada Information Disclosure Act*.

RECOMMENDATION 2: That Part 1 be amended to clarify any ambiguity regarding the role of the Privacy Commissioner and add a provision to the following effect: "Nothing in this Act or any other Act of Parliament should be construed as limiting the powers of the Privacy Commissioner to conduct an investigation to ensure compliance with sections 4 to 8 of the *Privacy Act*."

RECOMMENDATION 3: That the OPC should be among the review bodies having the legal authority and flexibility to share confidential information obtained in the course of their work and to determine when and how to cooperate to avoid duplication, increase efficiency and produce more comprehensive reports. Sections 22 and 23 of the *National Security Committee of Parliamentarians Act* could be used as a model to provide all review bodies with similar authority to share information "related to the fulfillment of the mandate" of the other review bodies. These provisions could be transposed in the form of parallel amendments to:

i. the *Privacy Act*;
ii. Part 1 of C-59, which creates and empowers the NSIRA, and;
iii. the *National Security Committee of Parliamentarians Act*.

RECOMMENDATION 4: That Bill C-59 be amended to require the necessity and proportionality threshold to apply to receiving institutions, either by way of an amendment to SCIDA or by way of a consequential amendment to section 4 of the *Privacy Act*. In this way, a dual threshold would apply to national security information sharing: the new s.5 of SCIDA would apply to disclosing institutions and receiving institutions would be governed by a necessity and proportionality threshold.

RECOMMENDATION 5: That Bill C-59 be amended to impose on recipient institutions retention and destruction rules in respect of personal information that does not meet or no longer meets the recipient's threshold for collecting the information. More specifically, we recommend an explicit provision for record disposal by receiving institutions in these three instances:

i. any personal information that does not meet the collection threshold;
ii. any personal information that the recipient institution does not believe "will contribute to the exercise of its jurisdiction or the carrying out of its responsibilities"; and,
iii. any personal information which, after analysis, leads to the opinion that the individual concerned is not a threat to national security.

RECOMMENDATION 6: That SCIDA be amended so that the record keeping obligations found in subsection 9(1) apply not only to disclosing institutions but also to recipient institutions.

RECOMMENDATION 7: That a new subsection be added to section 9 of SCIDA: "For greater certainty, the Government of Canada institution must also, on request by the Privacy Commissioner under s.34 of the *Privacy Act*, provide the Commissioner with a copy of any record requested that it prepared under subsection (1)."

RECOMMENDATION 8: That information-sharing agreements and privacy impact assessments be made into legal requirements either by way of amendment to Bill C-59 in the national security context, or more generally, by way of amendments to the *Privacy Act*.

RECOMMENDATION 9: That the rules and standards under SCIDA, amended as proposed above, should be extended to all domestic intra-governmental national security information sharing.

RECOMMENDATION 10: That section 24 be amended to add a limit to the activities listed in 24(1) namely: the measures shall be reasonable and proportional in the circumstances, having regard to the reasonable foreseeable effects on Canadians and people in Canada including on their right to privacy.

RECOMMENDATION 11: That the definition of "publicly available information" in section 2 be amended to specify that information is published or broadcast lawfully, and that information obtained through purchase or subscription was legally obtained or created by the vendor.