Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Information and Privacy Commissioner Ontario, Canada

March 4, 2015

Daryl Kramp
Chair, Standing Committee on
Public Safety and National Security and Members of the Committee
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6
Canada

Dear Chair Kramp:

Re: Bill C-51 – The *Anti-terrorism Act, 2015*

We are writing to you in our capacity as independent provincial and territorial privacy commissioners to express our deep concern about the far reaching implications of Bill C-51 (the *Anti-terrorism Act, 2015*) for the fundamental rights of Canadians.

Last fall, Information and Privacy Commissioners from across Canada shared the grief of all Canadians over the murders of Warrant Officer Patrice Vincent and Corporal Nathan Cirillo. Like all Canadians, we believe that effective measures are necessary to deal with threats to our national security. As all Canadian Commissioners said then, those measures must be evidence-based, proportionate, and subject to effective oversight and review.[1] They must protect Canadians' constitutionally-enshrined privacy rights and freedoms. Bill C-51 fails to do these things.

Bill C-51 challenges fundamental rights and freedoms on several fronts, but the focus of our concern is on its mandate for overbroad, unregulated and intrusive sharing of the personal information of ordinary Canadians. If enacted, the portion of Bill C-51 comprising the *Security of Canada Information Sharing Act* (SCISA) would significantly expand the power of the state to surveil and profile ordinary, law-abiding Canadians.

Canadians rightly expect their governments will take reasonable measures to prevent acts of terrorism, but the potential to interpret SCISA as equating dissent

[1] Links to October 29, 2014 FPT statement. English: https://www.priv.gc.ca/media/nr-c/2014/nr-c_141029_e.asp; French: https://www.priv.gc.ca/media/nr-c/2014/nr-c_141029_f.asp.

with violence, sabotage and subversion would facilitate a substantial shift towards routine surveillance of large portions of the populace. It could be used to authorize, in effect, surveillance across governments in Canada, and abroad, for virtually unlimited purposes. Such a state of affairs would be inconsistent with the rule of law in our democratic state and contrary to the expectations of Canadians.

Given the sweeping implications of SCISA, Canadians should expect there to be clear and persuasive evidence that these proposals are truly necessary, limited and proportionate. The government has yet to produce any evidence on these foundational points. It has not explained why the existing statutory provisions allowing for the disclosure of personal information for law enforcement and national security-related purposes are not sufficient to meet current security requirements.

In light of the above, and for the reasons stated below, we urge government to withdraw SCISA.

If the government declines to do this, substantial amendments to SCISA are, as we explain below, necessary in order to ensure that any new information-sharing powers are limited, proportionate, and protect Canadians' constitutional rights and freedoms.

THE CONCEPT OF WHAT "UNDERMINES THE SECURITY OF CANADA" IS EXCESSIVELY BROAD

Section 2 of SCISA would define an "activity that undermines the security of Canada" very broadly, more so than any comparable concepts in the *Canadian Security Intelligence Service Act* or the *Anti-terrorism Act, 2001*.[2] The definition would capture activities such as those directed at planning and preparing to carry out a terrorist attack or an act of foreign-directed sabotage. However, SCISA would also open the door to virtually limitless information sharing. It would set no boundaries for the broad and open-ended terms "undermine" and "security".

Many of the s. 2 examples of security-undermining activities are overly broad; notably the classes of activities listed in ss. 2(a), (b), (f), and (i). These extend well beyond what generally would be accepted as representing genuine security threats. Moreover, it is not clear that evidence of any link to unlawfulness (including criminality or violence) is a pre-condition to information sharing under s. 5. This would expose Canadians innocent of any illegality to the risk of virtually limitless information sharing, including with respect to their civic activities.

---

[2] See the definition of "threats to the security of Canada" in s. 2 of the *Canadian Security Intelligence Service Act*, and the definition of "terrorist activity" in s. 83.01 of the *Criminal Code*.

We are deeply concerned that SCISA would permit the sharing of personal information of individuals who have participated in lawful, peaceful demonstrations like the large-scale protests against investment in apartheid-era South Africa and the incarceration of Nelson Mandela. The historic peaceful protests in support of nuclear disarmament would also almost certainly have been caught as well. This is because SCISA would define, as an activity that undermines the security of Canada, anything that amounted to "interference with the capability of the Government of Canada in relation to … defence, … public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada". It would also include "unduly influencing a government in Canada by … unlawful means", noting—as only one example—that sometimes peaceful marches are held without complying with all municipal bylaws. Moreover, in contrast to the approach under the *Anti-terrorism Act, 2001*, SCISA risks surveillance of anyone *associated* with any group whose protests, demonstrations or pickets breach any law in Canada, however trivial.

THE SCOPE FOR INFORMATION SHARING IS ALSO EXCESSIVELY BROAD

Section 5(1) of SCISA would expressly authorize a "Government of Canada institution*"* to disclose any information it decides is "relevant" to the mandate of a recipient institution with respect to "activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption". Section 8(2)(b) of the *Privacy Act* authorizes government institutions to disclose personal information for any purpose in accordance with an Act that authorizes its disclosure. Section 5 of SCISA would appear to give that authority. In combination, these provisions would allow institutions to share personal information, on their own initiative or on request, for overbroad purposes.

SCISA would, in other words, open the door to systematic disclosure of a broad range of information about ordinary Canadians. It would funnel that information from, and to, disparate institutions, the list of which can be expanded by Cabinet at any time, without open debate.

Another serious concern is that s. 6 of SCISA would permit an institution to disclose personal information to "any person" and for "any purpose". This would enable ungoverned sharing of personal information of Canadians with other Canadian governments and public institutions, private sector organizations and foreign governments or their agencies. SCISA would also enable this unprecedented information sharing without any parallel increase in the already overstretched resources and limited authorities of existing independent review officials. The torture and unlawful imprisonment suffered by Maher Arar as a result of the unconstrained sharing of inaccurate personal information with foreign agencies illustrates the grave dangers of this opening of the information floodgates.

SIGNIFICANT AMENDMENTS ARE NEEDED TO PROTECT CANADIANS

In light of the above, the following amendments are critical to remedy the defects in SCISA and protect Canadians' privacy, associational and expressive rights:

> ***Recommendation 1:*** Drawing on the definition of "terrorist activity" in s. 83.01 of the *Criminal Code,* the Committee should narrow the s. 2 definition of an "activity that undermines the security of Canada" to ensure that SCISA information-sharing programs do not target innocent Canadians, including those that fund, support or participate in peaceful protests or other non-violent activities.
>
> ***Recommendation 2:*** The Committee should amend s. 5 of SCISA to limit information sharing to that which is strictly necessary to accomplish a specific security purpose associated with preventing "terrorist activity" or "threats to the security of Canada" (as those terms are defined in s. 83.01 of the *Criminal Code* and s. 2 of the *Canadian Security Intelligence Service Act*, respectively).
>
> ***Recommendation 3:*** The Committee should amend s. 4 of SCISA to require all disclosing and recipient institutions to implement responsible information-sharing practices and ensure that information sharing is conducted in a proportionate, transparent and accountable manner. Specific information-sharing requirements should be set out in binding regulations under s. 10 of SCISA. Those requirements should include a duty to establish appropriately limited retention periods (*e.g.*, two years), to securely destroy records at the end of the retention period (unless the further retention of a specific record can clearly be justified), and to keep records reflecting what information was shared with whom, when, why, and subject to what controls.
>
> ***Recommendation 4:*** Section 6 of SCISA, which would lead to recipient institutions using and further disclosing personal information to "any person" and for "any purpose" should be repealed.
>
> ***Recommendation 5:*** Section 10 of SCISA should be amended to restrict Cabinet's power to list recipient institutions under Schedule 3 of SCISA to those federal agencies that have primary responsibility for law enforcement or national security.
>
> ***Recommendation 6:*** SCISA should be subject to a sunset clause that requires the completion of a Parliamentary review within five years of its coming into force. That review should be mandated to determine whether any derogations in and under SCISA from the right to privacy are necessary, rational and proportionate.

PROPER OVERSIGHT AND REVIEW MEASURES ARE NECESSARY

It is useful to separately address the reasons for our last recommendation, set out below. Given the dramatic expansion of state power that SCISA represents, one would expect provision for robust, proportionate, independent oversight and review. Bill C-51 fails to do this.

Aspects of SCISA speak vaguely to information sharing principles and some form of self-regulated compliance with such principles. This is far from adequate. The reference in s. 4 of SCISA to responsible information sharing, such as the use of "information-sharing arrangements …when Government of Canada institutions share information regularly", offers no protection. For one thing, there is no indication that any such "principles" would be binding. Nor would they establish legally-enforceable rights for affected individuals.[3]

We therefore strongly endorse the concerns raised by Daniel Therrien, the Privacy Commissioner of Canada, that the government's proposal to establish a new information-sharing regime will exacerbate longstanding gaps in the independent oversight and review of law enforcement and intelligence agencies. The secrecy that accompanies this form of surveillance drastically reduces the opportunity for affected individuals to learn of and challenge the state's use and disclosure of their information. Independent oversight and review is thus critical. It also helps to improve both agency performance and the general public's confidence in the integrity and propriety of the agency's actions.

Accordingly, significant enhancements are needed for independent oversight and review of all agencies involved in national security and intelligence. The recommendations of the Arar Inquiry provide a good starting point for the development of many of the necessary reforms, including outside the context of Bill C-51 as a whole.

> ***Recommendation 7:*** The Committee should call on the government to introduce legislation to ensure that all national security and intelligence agencies are subject to meaningful, independent oversight and review.

CONCLUSION

We are committed to the development of effective, transparent, and privacy-protective approaches to achieving public safety and national security. As Commissioners charged with advising legislators with respect to complex privacy issues, we understand that developing a rational and proportionate response to

[3] In addition, s. 9 makes it clear that any person who discloses information under SCISA in good faith will enjoy immunity under any civil proceedings.

terrorism can be extremely challenging. We are confident that it is possible to both improve our capacity to pre-empt future terrorist attacks and enhance the privacy, accountability and transparency safeguards necessary to preserve our free and open democracy.

In the interests of transparency, we will be making this letter a matter of public record.

Respectfully submitted by,

Brian Beamish
Information and Privacy Commissioner, Ontario

Elizabeth Denham
Information and Privacy Commissioner, British Colombia

Jean Chartier
Chair, Commission à l'information du Québec

Jill Clayton
Information and Privacy Commissioner, Alberta

Mel Holley
Acting Ombudsman, Manitoba

Elaine Keenan Bengts
Information and Privacy Commissioner, Nunavut and Northwest Territories

Ronald J. Kruzeniski
Information and Privacy Commissioner, Saskatchewan

Maria C. MacDonald
Information and Privacy Commissioner, Prince Edward Island

Diane McLeod-McKay
Yukon Ombudsman and Information and Privacy Commissioner

Ed Ring
Information and Privacy Commissioner, Newfoundland and Labrador

Catherine E. Tully
Freedom of Information and Protection of Privacy Review Officer, Nova Scotia

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Commissaire à l'information et à la protection de la vie privée, Ontario, Canada

4 mars 2015

Daryl Kramp
Président, Comité permanent de la
sécurité publique et nationale et membres du Comité
Sixième étage, 131, rue Queen
Chambre des communes
Ottawa ON K1A 0A6 Canada

Président Kramp:

Objet : Projet de loi C-51 – *Loi antiterroriste de 2015*

Nous vous écrivons dans notre capacité de commissaires indépendants à la protection de la vie privée, provinciaux et territoriaux, afin d'exprimer nos profondes inquiétudes concernant les répercussions de grande envergure du projet de loi C-51 (*Loi antiterroriste de 2015*) sur les droits fondamentaux des Canadiens et Canadiennes.

À l'automne dernier, les commissaires à l'information et à la protection de la vie privée de partout au Canada ont partagé le deuil de tous les Canadiens et Canadiennes, quant aux meurtres de l'Adjudant Patrice Vincent et du Caporal Nathan Cirillo. Comme tous les Canadiens et Canadiennes, nous croyons que des mesures efficaces sont nécessaires pour faire face aux menaces à notre sécurité nationale. Comme tous les commissaires canadiens l'avaient alors mentionné, ces mesures doivent être fondées sur des preuves, proportionnées, et assujetties à une surveillance et un examen efficaces.[1] Elles doivent protéger les droits et libertés inscrits dans la loi, quant au respect de la vie privée des Canadiens et Canadiennes. Le projet de loi C-51 échoue à tous ces niveaux.

Le projet de loi C-51 s'oppose, à plusieurs égards, à des droits et libertés fondamentaux, mais notre préoccupation se centre autour de son mandat qui permet le partage trop général, non régulé et intrusif de renseignements personnels des Canadiens et Canadiennes ordinaires. La partie du projet de loi C-51 comprenant la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), si adoptée, élargirait substantiellement le pouvoir de l'État pour surveiller et profiler des Canadiens et Canadiennes ordinaires et respectueux de la loi.

[1] Liens vers la déclaration FPT du 29 octobre 2014. Anglais : https://www.priv.gc.ca/media/nr-c/2014/nr-c_141029_e.asp; français : https://www.priv.gc.ca/media/nr-c/2014/nr-c_141029_f.asp.

Les Canadiens et Canadiennes s'attendent, avec raison, à ce que leurs gouvernements prennent des mesures raisonnables pour prévenir des actes terroristes. Cependant, le potentiel d'interpréter la dissidence comme étant équivalente à la violence, le sabotage et la subversion dans la LCISC, faciliterait un déplacement important vers une surveillance de routine de larges parties de la population. Celle-ci pourrait, en effet, être utilisée pour autoriser la surveillance dans l'ensemble des gouvernements au Canada, et à l'étranger, à des fins pratiquement illimitées. Une telle situation serait incompatible avec la primauté du droit comprise dans notre démocratie, et serait contraire aux attentes des Canadiens et Canadiennes.

Étant donné l'ampleur de la portée de la LCISC, les Canadiens et Canadiennes devraient s'attendre à ce qu'il y ait des preuves claires et convaincantes pour justifier que ces propositions sont vraiment nécessaires, limitées et relatives. Le gouvernement n'a toujours pas fourni de preuves quant à ces points de fondement. Il n'a pas expliqué pourquoi les dispositions législatives en place permettant la divulgation de l'information personnelle à des fins d'application de la loi ou en lien avec la sécurité nationale ne sont pas suffisantes pour satisfaire aux exigences actuelles en matière de sécurité.

Compte tenu de l'information ci-dessus, ainsi que pour les raisons énumérées ci-dessous, nous exhortons le gouvernement de retirer la LCISC.

Si le gouvernement refuse de le faire, des amendements importants à la LCISC sont nécessaires, tel qu'expliqué ci-dessous, afin d'assurer que tous nouveaux pouvoirs de partage d'information soient limités, relatifs, et qu'ils protègent les droits et libertés constitutionnels des Canadiens et Canadiennes.

LE CONCEPT DE CE QUI "PORTE ATTEINTE À LA SÉCURITÉ DU CANADA" EST EXCESSIVEMENT VASTE

L'article 2 de la LCISC donne une définition très vaste d'une *"activité portant atteinte à la sécurité du Canada",* plus encore que tout autre concept comparable dans la *Loi sur le Service canadien du renseignement de sécurité* ou dans la *Loi antiterroriste de 2001*.[2] La définition engloberait les activités telles que celles liées à la planification et la préparation d'une attaque terroriste ou d'un acte de sabotage dirigé par l'étranger. Cependant, la LCISC ouvrirait la porte à un partage d'information pratiquement illimité. Elle ne fixerait pas de limites pour les termes "portant atteinte" et "sécurité", qui sont vastes et ouverts.

Dans l'article 2, plusieurs des exemples d'activités portant atteinte à la sécurité sont trop vastes; particulièrement les catégories d'activités énumérées aux

[2] Voir la définition de "menaces envers la sécurité du Canada" dans l'article 2 de la *Loi sur le Service canadien du renseignement de sécurité*, et la définition d' "activité terroriste" dans l'article 83.01 du *Code Criminel*.

paragraphes 2(a), (b), (f), et (i). Celles-ci s'étendent bien au-delà de ce qui serait accepté d'une façon générale comme représentant une authentique menace à la sécurité. De plus, il n'est pas précisé qu'une preuve d'illégalité (y compris les activités criminelles et la violence) serait une précondition au partage de l'information selon l'article 5. Ceci exposerait les Canadiens et Canadiennes innocents de toute illégalité au risque d'un partage pratiquement illimité de leur information, y compris à l'égard de leurs activités civiques.

Nous sommes profondément préoccupés par le fait que la LCISC permettrait le partage des informations personnelles d'individus ayant participé à des manifestations pacifiques légitimes, telles que les manifestations de grande envergure contre l'investissement dans l'apartheid en Afrique du Sud et l'incarcération de Nelson Mandela. Les manifestations pacifiques historiques en faveur du désarmement nucléaire auraient également, presque certainement, été touchées. C'est le cas puisque la LCISC définirait, comme activité portant atteinte à la sécurité, tout ce qui pourrait équivaloir à "entraver la capacité du gouvernement fédéral — ou de son administration — en matière de … défense … de sécurité publique, d'administration de la justice, de relations diplomatiques ou consulaires ou de stabilité économique ou financière du Canada." La définition comprendrait aussi le fait d' "influer indûment sur un tel gouvernement par l'emploi … de moyens illégaux", notant — comme un seul exemple — que parfois certaines marches non violentes ont lieu sans se conformer à tous les règlements municipaux. De plus, à l'opposé de l'approche dans la *Loi antiterroriste de 2001*, la LCISC risque la surveillance de quiconque *associé* à un groupe dont les protestations, manifestations ou piquets de grève violent quelconque loi au Canada, peu importe sa futilité.

LE CHAMP D'APPLICATION DU PARTAGE DE L'INFORMATION EST AUSSI EXCESSIVEMENT VASTE

L'article 5(1) de la LCISC donnerait expressément la permission à toute "organisation du Gouvernement du Canada" de divulguer des informations qu'elle juge "pertinentes" au mandat de l'organisation destinataire quant aux "activités portant atteinte à la sécurité du Canada, notamment en ce qui touche la détection, l'identification, l'analyse, la prévention ou la perturbation de ces activités ou une enquête sur celles-ci." L'article 8(2)(b) de la *Loi sur la protection des renseignements personnels* permet aux institutions gouvernementales de divulguer des informations personnelles à n'importe quelles fins, conformément à une Loi qui permet sa divulgation. L'article 5 de la LCISC semblerait confier cette autorisation. Ensemble, ces dispositions permettraient aux organisations de partager des informations personnelles, par leur propre initiative ou sur demande, pour des fins à l'étranger.

Autrement dit, la LCISC ouvrirait les portes à la divulgation systémique d'un large éventail d'information concernant des Canadiens et Canadiennes ordinaires. Ceci permettrait le passage de l'information en provenance, et en direction, des organisations diverses, la liste desquelles pourrait être élargie à tout moment, sans faire l'objet de débat public.

Une autre sérieuse préoccupation est que l'article 6 de la LCISC permettrait à une organisation de divulguer de l'information personnelle à "toute personne" et ce, "à toute fin". Ceci permettrait le partage non-réglementé de l'information personnelle des Canadiens et Canadiennes avec d'autres gouvernements et organisations publiques au Canada, organismes du secteur privé et gouvernements étrangers ou leurs agences. La LCISC permettrait également ce partage d'information sans précédent sans pour autant accroître les ressources, déjà surexploitées, et les pouvoirs limités des agents d'examen indépendants actuels. La torture et l'emprisonnement illicite dont a souffert Maher Arar à la suite d'un partage sans contraintes d'informations personnelles inexactes avec des agences étrangères, illustrent les graves dangers de cette ouverture des vannes de l'information.

DES MODIFICATIONS IMPORTANTES SONT NÉCESSAIRES POUR PROTÉGER LES CANADIENS ET CANADIENNES

À la lumière de ce qui précède, les modifications suivantes sont essentielles pour remédier aux défaillances dans la LCISC et protéger la vie privée des Canadiens et Canadiennes ainsi que leurs droits d'association et d'expression :

> ***Recommandation 1 :*** En s'appuyant sur la définition d ' "activité terroriste" à l'article 83.01 du *Code criminel*, le Comité devrait réduire la portée de la définition d'une "activité portant atteinte à la sécurité du Canada" afin d'assurer que les programmes de partage d'information de la LCISC ne ciblent pas des Canadiens et Canadiennes innocents, y compris ceux qui financent, soutiennent ou participent à des manifestations pacifiques ou d'autres activités non-violentes.
>
> ***Recommandation 2 :*** Le Comité devrait modifier l'article 5 de la LCISC afin de s'assurer que le partage d'information est employé seulement lorsque strictement nécessaire pour permettre d'accomplir des buts spécifiques reliés à la sécurité, en lien avec la prévention d' "activités terroristes" ou de "menaces envers la sécurité du Canada" (tel que ces termes sont définis dans l'article 83.01 du *Code criminel* et l'article 2 de la Loi sur le Service canadien du renseignement de sécurité, respectivement).

Recommandation 3 : Le Comité devrait modifier l'article 4 de la LCISC pour obliger toutes les organisations divulgatrices et récipiendaires à mettre en œuvre des pratiques responsables quant au partage d'information et s'assurer que le partage d'information est mené de manière proportionnée, transparente et responsable. Des exigences particulières quant au partage d'information devraient être fixées dans les règlements contraignants sous l'article 10 de la LCISC. Ces exigences devraient comprendre une obligation d'établir des délais de conservation limités et appropriés (p. ex., deux ans), de détruire de façon sécuritaire les documents à la fin du délai de conservation (à moins qu'une conservation plus longue ne soit clairement justifiée), et de garder les documents témoignant du contexte dans lequel cette information a été partagée (avec qui, quand, pourquoi et sous réserve de quel contrôle).

Recommandation 4 : L'article 6 de la LCISC devrait être abrogé puisqu'il mènerait à une utilisation et une divulgation élargies, de la part des organisations récipiendaires, des informations personnelles à "toute personne" et ce "à toute fin".

Recommandation 5 : L'article 10 de la LCISC devrait être modifié pour restreindre les pouvoirs du Cabinet à nommer les institutions destinataires dans l'Annexe 3 de la LCISC, aux organismes fédéraux ayant comme responsabilité principale l'application de la loi ou la sécurité nationale.

Recommandation 6 : La LCISC devrait faire l'objet d'une disposition de réexamen qui exige la complétion d'un examen parlementaire dans un délai de cinq ans suivant son entrée en vigueur. Cet examen devrait être autorisé afin de déterminer si les dérogations au droit àla vie privée, découlant de l'application de laLCISC, sont nécesssairess, justifiées et relatives.

DES DISPOSITIONS APPROPRIEES EN MATIERE DE SURVEILLANCE ET DE REVISION SONT NECESSAIRES

Il est utile de traiter séparément des raisons pour notre dernière recommandation, retrouvée ci-dessous. Étant donné l'expansion drastique du pouvoir de l'état que représente la LCISC, on pourrait s'attendre à ce qu'il y ait une disposition robuste, relative et indépendante en matière de surveillance et de révision. Le projet de loi C-51 omet cela.

Certains aspects de la LCISC se rapportent vaguement à des principes de partage d'information et à une forme ou une autre de conformité auto-réglée

avec de tels principes. Ceci est loin d'être vrai. La référence dans l'article 4 de la LCISC qui traite du partage d'information, tel que le recours à une "conclusion d'ententes de communication d'information … aux institutions fédérales qui communiquent régulièrement entre elles de l'information", n'offre aucune protection. Premièrement, il n'y a aucune indication que ces principes seraient obligatoires. Deuxièmement, aucuns droits en vertu de la loi n'ont été institués pour les personnes concernées.[3]

Ainsi, nous soutenons fortement les préoccupations soulevées par Daniel Therrien, commissaire à la protection de la vie privée du Canada, que la proposition du gouvernement pour instituer un nouveau régime de partage d'information risque d'exacerber les lacunes de longue date dans la surveillance et la révision indépendantes des organismes d'application de la loi et des organismes de renseignements.

Le secret qui accompagne cette forme de surveillance réduit grandement la possibilité que les individus concernés puissent être informés de l'utilisation et la divulgation de leurs renseignements par l'État, et qu'ils puissent contester celle-ci.

Une surveillance et une révision indépendantes sont donc essentielles. Elles aideraient aussi à améliorer la performance des organisations ainsi que la confiance du public par rapport à l'intégrité et le bien-fondé des mesures prises par les organisations.

Par conséquent, d'importantes améliorations sont nécessaires en matière de surveillance et de révision indépendantes de tous les organismes de sécurité nationale et de renseignements. Les recommandations de l'enquête Arar fournissent un bon point de départ pour le développement de plusieurs réformes nécessaires, y compris à l'extérieur du contexte du projet de loi C-51 dans son ensemble.

> ***Recommandation 7 :*** Le Comité devrait demander au gouvernement d'adopter une loi pour garantir que tous les organismes de sécurité nationale et de renseignements soient soumis à une surveillance et une révision, significatives et indépendantes.

[3] De plus, l'article 9 précise que toute personne qui divulgue, de bonne foi, des informations selon la LCISC, profitera d'une immunité lors des procès civils.

CONCLUSION

Nous nous engageons à l'élaboration d'approches efficaces, transparentes et protectrices du droit à la vie privée afin d'assurer la sécurité du public et la sécurité nationale. En tant que commissaires chargés de conseiller les législateurs sur les questions complexes relatives à la protection de la vie privée, nous comprenons que l'élaboration d'une réponse rationnelle et relative au terrorisme peut être extrêmement difficile. Nous somme confiants qu'il est possible d'améliorer à la fois notre capacité à préempter des attaques terroristes futures et les mesures de protection quant à la protection des renseignements personnels, la reddition des comptes et la transparence, qui sont nécessaires afin de conserver notre démocratie ouverte et libre.

Dans l'intérêt de la transparence, nous mettrons cette lettre à la disposition du public.

Respectueusement,

Brian Beamish,
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Elizabeth Denham,
Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique

Jean Chartier,
président, Commission à l'information du Québec

Jill Clayton,
commissaire à l'information et à la protection de la vie privée, Alberta

Mel Holley,
Ombudsman par intérim, Manitoba

Elaine Keenan Bengts,
commissaire à l'information et à la protection de la vie privée, Nunavut et Territoires-du-Nord-Ouest

Ronald J. Kruzeniski,
commissaire à l'information et à la protection de la vie privée, Saskatchewan

Maria C. MacDonald,
commissaire à l'information et à la protection de la vie privée, Île-du-Prince-Édouard

Diane McLeod-McKay,
Ombudsman et commissaire à l'information et à la protection de la vie privée, Yukon

Ed Ring,
commissaire à l'information et à la protection de la vie privée, Terre-Neuve-et-Labrador

Catherine E. Tully,
agent d’examen à l'information et à la protection de la vie privée, Nouvelle-Écosse