THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Privacy Act Modernization

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW AND ABORIGINAL LAW SECTIONS

October 2019

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

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

This submission was prepared by the CBA Privacy and Access Law Section, with comments from the CBA Aboriginal Law Section on *Modernizing the Privacy Act's relationship with Canada's Indigenous People*, and with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law and Aboriginal Law Sections.

TABLE OF CONTENTS

Privacy Act Modernization

Privacy Act Modernization

I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law Section (CBA Section) is pleased to comment on several issues raised in the discussion papers issued by Justice Canada in June 2019 on the modernization of the *Privacy Act*. We acknowledge and appreciate the CBA Aboriginal Law Section's work on the fifth discussion paper, *Modernizing the Privacy Act's Relationship with Canada's Indigenous People*. Given the breadth of material in the discussion papers, we have limited our responses to the questions most pertinent to our expertise.

The CBA has long advocated for reform and modernization of the *Privacy Act.*[1] The legislation, enacted in 1982, has not kept pace with societal and technological developments, or with parallel legislation for the private sector, most notably the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In this current consideration of modernizing the *Privacy Act*, we incorporate by reference several past CBA submissions and resolutions:[2]

- *Privacy Act* amendments, submission of the CBA Privacy and Access Law Section to the Privacy Commissioner of Canada (September 2016)
- *Privacy Act* Reform, submission of the CBA to the Standing Committee on Access to Information, Privacy and Ethics (June 2008)
- Letter to the Minister of Justice on *Privacy Act* amendments (June 2012)
- Resolution 12-01-M, *Privacy Act* amendment (February 2012)
- Resolution 08-06-A, Comprehensive Revision of the *Privacy Act* (August 2008)
- Resolution 06-03-A, *Privacy Act* Review (August 2006)
- Resolution 04-06-A, Limiting State Access to Private Information (August 2004)
- Resolution 04-05-A, Privacy Rights in Canada (August 2004)

We also rely on past CBA submissions on the *Access to Information Act* (ATIA) and PIPEDA[3] concerning the need for a five-year statutory review, the ability to decline to investigate complaints or complete investigations, breach notification and other issues.

---

1 See for e.g., Resolution 06-03-A, *Privacy Act* Review (August 2006).

2 Submissions and resolutions are available on https://www.cba.org/Our-Work.

3 Examples include, PIPEDA: Draft Guidelines for Obtaining Meaningful Consent (December 2017); Bill C-58, *Access to Information Act* amendments (October 2017); PIPEDA Data Breach Notification and Reporting Regulations (May 2016); *Personal Information Protection and Electronic Documents Act (*PIPEDA) (March 2017); *Modernization of Access to Information Act* (January 2013).

Any departures from our past positions are simply intended to address other legislative changes and current realities.

II. PRIVACY PRINCIPLES AND MODERNIZED RULES FOR A DIGITAL AGE

Q. 1(a) Could a reasonableness and proportionality principle achieve the same purpose (reasonable data minimization) as a "necessity" standard, but in a way that is more sensitive to contextual considerations?

In its June 2008 submission, the CBA Section recommended that the *Privacy Act* be amended to require government institutions to identify the specific purpose for collecting personal information and ensure that the information is reasonably necessary for the articulated purpose or is authorized by law. The inadequacy of the existing, "directly relevant" provision in the *Privacy Act* is apparent when compared with the comprehensive principles in PIPEDA.

The "data minimization" principle under the *General Data Protection Regulation* (GDPR)[4] does not exclude or replace the concept of necessity in the collection of personal information. The "data minimization" principle seems somewhat different than the broad-based "privacy impact minimization" principle contemplated in the discussion paper. Put another way, "data minimization" is only one element of "privacy impact minimization". An unreasonable or disproportionate impact on an individual's privacy brought about by collecting particularly sensitive personal information for a particular purpose may give a government institution cause to seriously consider whether the information should be collected. However, a determination that a particular collection, use, retention or disclosure of personal information would have a proportionate impact on individual privacy should not excuse the initial collection of personal information beyond what is necessary to satisfy a legitimate purpose of the government institution.

4 (EU) 2016/679.

Q. 1(b) Could a reasonableness and proportionality principle effectively support government institutions to advance "Data and Digital for Good" through the ethical use of data in the public interest?

Q. 1(c) Is a reasonableness and proportionality principle a useful and effective way of explicitly bringing into the Privacy Act a legal framework similar to that which guides the balancing of individuals' fundamental rights and interests against important public interests in the Canadian human rights law context (e.g. section 1 of the Canadian Charter of Rights and Freedoms) and reflects underlying administrative law obligations (e.g. reasonable exercises of discretion)?

A "reasonableness and proportionality" principle might guide government institutions to narrowly define circumstances in which the *Privacy Act* may offer them limited discretion. There may be benefits to requiring the exercise of discretion in a manner harmonious with concepts developed in *Charter* jurisprudence and administrative law. However, a "reasonableness and proportionality" principle should not become the standard for lawful collection, use or disclosure of personal information in the public sector. An explicit "necessity" test should be adopted, as recommended by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee) in its 2016 *Privacy Act* review, and supported by most witnesses appearing before that Committee.

The *Privacy Act* should embody what Parliament considers to be reasonable and proportional limitations on the collection, use and disclosure of personal information by the public sector consistent with a free and democratic society. Given the asymmetrical power and resources between the state and individuals and the importance of privacy, Canadians reasonably expect that Parliament's delegation to governmental officials to determine what constitutes any reasonable and proportional invasion of the privacy of individuals should be limited to prescribed circumstances.

The *Privacy Act* applies to many government institutions of varying sizes and resources. We are concerned about sufficient capacity in these institutions to make determinations about what is reasonable and proportional, and to do so consistently across all government institutions. If "reasonableness and proportionality" became a generalized threshold for the collection, use and disclosure of information, capacity building in these government institutions would be needed, matched with strong oversight by the Office of the Privacy Commissioner of Canada (OPC). The OPC's resources are already stretched and capacity to monitor and investigate government institutions with broad authority to determine what is "reasonable" and "proportional" might be lacking. The inevitable result would be inconsistent approaches across

government institutions, with the potential for a general erosion of privacy rights for Canadians.

> **Q. 1(d) Could introducing a requirement for a "privacy by design" approach effectively advance privacy protection? If yes, would such a requirement function best as an overarching principle, and specific and/or supporting rule elsewhere in the Act, or as a matter of policy guidance?**
>
> **Q. 1(e) Would it make sense that compliance with a privacy by design principle also be subject to a reasonableness and proportionality standard? In other words, a design that is maximally protective of privacy would not be absolutely required if another reasonable and proportionate alternative were adopted in light of broader or competing considerations?**

While the CBA Section supports including a requirement for government institutions to consider privacy by design principles in developing, implementing and maintaining operational activities, adherence to these principles could be part of Treasury Board requirements. It would not be necessary to embody those principles in the *Privacy Act*, although it may be beneficial to do so. In either case, the suggestion that privacy by design would need to be qualified by a reasonableness or proportionality standard is the type of "zero sum" approach that privacy by design actually aims to avoid.

The formulation of privacy by design by former Information and Privacy Commissioner Ann Cavoukian involves seven foundational principles:

1. Proactive not reactive: preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality: positive-sum, not zero-sum
5. End-to-end security: full lifecycle protection
6. Visibility and transparency: keep it open
7. Respect for user privacy: keep it user-centric

The concept of "data protection by design and by default" is embodied in the GDPR, Article 25. The principle of data protection "by design" is a general statement that an organization should implement measures that integrate safeguards into processing to implement data-protection principles. The concept of data protection "by default" is that only personal data necessary for each specific purpose of the processing are processed. However, in the GDPR, the EU has explicitly recognized in Article 25 that operational requirements will be subject to "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing

as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing."

Neither the classic formulation by former Commissioner Cavoukian nor the GDPR require design that is maximally protective of privacy rights. Rather, the concepts of "privacy by design" and "data protection by design and by default" are principles that guide operational design to ensure that privacy is embedded into design and that institutions and organizations do not approach privacy as though it must be traded against operational results.

The CBA Section cautions against layering a reasonable or proportionate standard onto privacy by design principles. This confuses the purpose of the principles, which is to challenge government institutions and organizations to design solutions that do not create false trade-offs between privacy and other "broader or competing considerations". The very function of privacy by design is to challenge designers to embed privacy into operational systems to meet operational needs while respecting privacy, rather than trade privacy for operational needs. Qualifying privacy by design with a reasonableness and proportionate standard would confuse and dilute the purpose of privacy by design.

Q. 1(f) What data security obligations can best ensure Canadians can rely on the integrity, authenticity and security of the government services they use, and know that their personal information is secure?

In our June 2008 and September 2016 submissions, the CBA Section recommended that the *Privacy Act* impose a general duty on government institutions to protect the personal information they hold with safeguards appropriate to the sensitivity of the information being protected. This is a feature common to many other Canadian and international privacy laws that regulate both the public sector and the private sector and accords with the recommendation on safeguards in the ETHI report.[5]

By adopting a principled approach to security obligations, the *Privacy Act* would create a technology neutral but legally enforceable obligation for government institutions to meet. Technological neutrality would assist the legislation to stand the test of time in many contexts, while being readily adaptable to future, now unforeseen, digital transformation. If further specificity in current standards for security safeguards (e.g. required standard and level of encryption) is necessary to guide the activities of government institutions, these specific

5 Blaine Calkins, Chair, Report 4: Protecting the Privacy of Canadians: Review of the *Privacy Act* (Ottawa: House of Commons, December 2016).

standards can be in Treasury Board policy, which can be updated or replaced as needed without legislative amendment.

Q. 1(g) Should the Privacy Act mirror the Safeguards principle in PIPEDA in the way proposed to facilitate improved interoperability in contracting situations? Are there other models to consider?

See response to Q.1(f).

Q. 1(h) Are any supporting legal rules required or should individual institutional responses be favoured?

See response to Q.1(f).

Q. 1(j) Would a principles-based approach effectively further openness and transparency? Would any supporting legal rules be required to give effect to these objectives?

Q. 1(k) What are the relevant factors for institutions in determining how to communicate about personal information practices?

Q. 1(l) Would a principles-based approach effectively further accountability? Would any supporting legal rules be required to supplement an accountability principle?

Q. 1(m) What does governmental accountability for practices with personal information look like in the federal public sector context? Are concepts and requirements that have developed with the private sector in mind relevant? Adequate? Sufficient?

The CBA Section supports amending the Act to strengthen requirements for accountability, openness and transparency in the personal information protection practices of government institutions. However, accountability, openness and transparency of government institutions should not be left to principles-based statements in the Act. For example, government institutions should be required to consider principles of openness and transparency when designing operational programs. There should also be minimum baseline requirements consistent with the role of the government in an open and democratic society.

The CBA Section recommends that openness and transparency requirements should be buttressed by minimum legislative requirements. For example, the CBA Section stated in our September 2016 submission that meaningful accountability for the collection, use and disclosure of personal information requires written information-sharing arrangements between multiple organizations. Further, we recommended that information-sharing be codified and accessible to data subjects to buttress openness and transparency.

Consideration should be given to a legislative requirement for government institutions to provide layered and accessible disclosures about their information-sharing practices to empower citizen engagement and the accountability of institutions. This should include simplified, plain language summaries of, for example, information-sharing arrangements and disclosure of the details of those arrangements. Plain language summaries meet the needs of a broad cross-section of individuals. However, there should also be proactive disclosure of details to support deeper citizen engagement. The Act can be drafted so the specific design and means of disclosure are technologically neutral while still mandating requirements for the minimum information to be disclosed, which could be supplemented by regulation.

The CBA Section also recommends that the federal government consider whether the siloed approach to notices under the *Privacy Act* is appropriate given increased sharing across government institutions. The consultation documents start from the premise that retaining personal information in silos is an antiquated approach to protecting personal information. However, they do not fully address the challenges for citizen engagement and literacy with the siloed approach to providing notice to individuals about information collection and use. Currently, the practice is to give statutory notice at the point of collection. There is no cross-government approach, such as a central repository or explanation to Canadians on how or why their information is shared across government institutions. Canadians expect that if personal information will be shared across government institutions and disclosed, they should have an easy and comprehensive way to find how their information is used, shared and disclosed, as well as details on specific types of collection, use and disclosure.

To improve accountability, transparency and openness of government institutions, the CBA Section recommends that the federal government consider, among other things, specific legislative provisions to require:

- information-sharing agreements, including the minimum contents of those agreements, which may be supplemented by regulation.
- government institutions to notify individuals about the purpose of the collection of information and also why that collection is necessary, the primary and secondary purposes for collection, the broad retention periods for information, any information-sharing arrangements, how the information may be used by recipients of shared information, and individuals' rights with respect to the collection, use and disclosure of the information in a simplified, plain language summary supported by more detailed information.

- a whole of government approach to disclosures to individuals of how government institutions may collect, use and disclosure information across institutions.
- government institutions to conduct internal audits and reviews against standards to be enacted by regulation and to publish the results of those audits along with the steps for remediation of deficiencies.

Q. 1(n) What are the most important roles for principles to play if they were introduced into the Privacy Act?

The CBA Section urges caution in transitioning to a principles-based *Privacy Act*. The relationship of individuals with the state is not analogous to commercial activities in the private sector. If principles are adopted, the CBA Section believes they would most effectively protect privacy interests by forming part of a purpose statement in the *Privacy Act*. In a purpose statement, they would be useful in interpreting specific provisions of the Act. In addition, they could be legislatively required to be considered in exercising any limited discretion given to the institution under the Act and in the institution's operations. The principles could form some of the criteria against which the government institution would be required to conduct internal audits and reviews. They could also serve as the lens through which the OPC would be required to assess the government institutions' practices.

Q. 1(p) Could an ongoing five-year review provision support the Privacy Act to stay current in the face of change?

The CBA Section supports a five-year period for statutory review of the *Privacy Act*. Further, and in keeping with the CBA position on Bill C-58[6] on amendment of the *Access to Information Act,* we believe that this should be a full Parliamentary review, rather than a Ministerial review.

The quasi-constitutional nature of privacy rights necessitates a rigorous review process. Ministerial reviews can be criticized for being too narrow and lacking the appropriate rigour given the importance of privacy rights. We recommend that a Parliamentary committee conduct the mandatory statutory review beginning with broad-based public consultations.

Q.1(q): Where are the meaningful opportunities for individuals to make informed decisions and provide valid consent in the public sector context?

The CBA Section believes that the current in-depth review of the law under the *Privacy Act* is necessary to provide meaningful opportunities for individuals to make informed decisions and

6 Bill C-58, Access to Information Act and Privacy Act amendments (May 2018).

give valid consent in the public sector context. Distinctions need to be made between instances where the personal information is required for the program or services to be available, and situations where the personal information may relate to and be demonstrably necessary, but not be required. This approach does not exist now in the *Privacy Act*. For instance, the current requirement that "information relate directly to an operating program or activity of the institution" offers little protection from indiscriminate collection of personal information.

Further, a considerable loophole is in the government policy that "[limits] the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities". This requirement can be met by merely recognizing the government program through budgetary approval. If there is a lack of scrutiny and detail in Parliament's budget approval process, some government institutions may collect personal information based on loose authority, and elected representatives may not be aware that approving the budget increased the government's ability to collect personal information in accordance with the *Privacy Act*.

The definition of consent in other jurisdictions could be useful to further delineate consent in the *Privacy Act*. For instance, Article 4(11) of the GDPR defines consent as follows:

> Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Considering consent in the Canadian healthcare context could also be useful to improve the definition and framework for consent in the Canadian federal public sector. Consider the concept of "implicit consent", where an individual is deemed to have implicitly consented to the collection, use and disclosure of information within that individual's circle of care.

The word "meaningful" should also be defined. For instance, in Ontario law, "meaningful consent" requires that consent must be knowledgeable, related to the information at issue and not obtained through deception or coercion. "Knowledgeable" consent requires the individual to fully understand the purpose for which the information was collected, used or disclosed. In the public sector, meaningful opportunities for individuals to consent to the disclosure of personal information given what is relevant to the mandate of the government institution could include broad scenarios as examples in questionnaires and offered to individuals when the government institution collects information.

Q. 1(r) How can individuals be supported to exercise control and consent in relation to their personal information under the Privacy Act's lawful authority/legal authorization governance model?

The federal public sector should look to the banking and finance sector and the healthcare sector for how individuals can be supported to exercise control and consent. However, the sensitivity of the information should be considered in determining the strength and necessity of any controls.

Individuals should be given options in the same questionnaires to not answer those questions they believe infringe on their privacy rights.

Q.1(s) How can the Privacy Act's approach to collection be designed to be sufficiently principled flexible and clear to offer robust privacy protection without compromising individuals' and the public's other expectations of government?

The CBA Section appreciates that the approach to collection should be specifically designed for different contexts and different governmental institutions. Each may handle personal information at various levels of sensitivity, and the public may have different expectations for the quick delivery of their services. There may also be reasons, such as national security, for the government to avoid obtaining consent to collection, use or disclosure. In addition to defining the threshold to collection, for instance, as reasonable or demonstrably necessary, the *Privacy Act*'s approach must be sufficiently principled, flexible and clear to offer robust privacy protection without compromising other governmental responsibilities. The *Privacy Act*'s approach to collection must be more general and ensure that the collection of personal information is more closely regulated for each government institution.

Q.1(t) Are different approaches for different contexts necessary? For example, are specific rules required to guide the collection of personal information that is publicly available on the internet and through social media?

The CBA Section believes a range of approaches to collection are necessary for different contexts, including the collection of information through internet and social media, as opposed to non-electronic or direct collection. Thought should be given to the appropriateness of government institutions collecting personal information from public sources, in what circumstances that collection makes sense considering their mandate and programs, and what form of transparency is required.

Q. 1(u) What should the collection threshold be linked to? That is, should the collection threshold be tied to the purposes of a specific program or activity; a legitimate or authorized public purpose; the mandate and functions of a department? Something else?

Government institutions have legitimate reasons to collect, use and disclose personal information where it is required for limited, legitimate public objectives. As articulated by the CBA in 2004, the collection, use and disclosure of personal information by government institutions should be balanced and well-considered to minimize the infringement of personal privacy and civil rights in a free and democratic society.[7] Further, in 2008, the CBA called for governments to limit the personal information they collect to that demonstrably necessary for clear and articulate state goals.[8]

Q. 1(v) If there is a principle of reasonableness and proportionality that applies to collection, is a necessity threshold still useful.

See response to question Q.1(a).

Q. 1(y) Would a proportionality test, as was proposed before the ETHI Committee, represent a viable means of transitioning to a more flexible, principles-based approach for retention?

Q. 1(z) Are there particular criteria that should inform retention decisions?

The ETHI Committee did not recommend that the principle of proportionality alone guide the retention of personal information. Rather, the necessity test should apply to the retention of personal information. The CBA Section supports the ETHI Committee recommendation that section 6 of the *Privacy Act* be amended to require that personal information be retained as necessary to achieve the purposes for collection. The necessity test should also include consideration of the retention period required for transparency and openness to those about whom the information was collected, and for them to be able to challenge decisions made about them based on that information.

The CBA Section does not believe the proportionality principle is relevant to retaining personal information by a government institution. Under a necessity test, personal information might be retained for a long time if collected for a *bona fide* longitudinal study. This may accommodate future uses consistent with the longitudinal study. However, the fact that personal information

7 Resolution 04-06-A, Limiting State Access to Private Information (August 2004).

8 Resolution 08-06-A, Comprehensive Revision of the Privacy Act (August 2008).

might be relevant to a hypothetical future use is an insufficient legal basis for the state to retain it, even if a proportionality test suggests that the impact on privacy is low.

While the CBA Section does not have specific recommendations about retention periods, we do not support a trade-off between access rights and prudent disposal. In the case of information not used to make a decision that affects the rights, privileges or entitlements of an individual, what may be relevant is not so much the underlying information that was collected but the fact that information was collected and the type of that information. In these cases, it might be appropriate to dispose of the underlying information while retaining records of the fact of collection for longer to assist with transparency and openness about the government institution's practices.[9] In contrast, where a government institution has made a decision about an individual, personal information relating to that decision should generally be retained for a minimum period to enable the individual to access it. This is reflected in the regulations under the *Privacy Act* that set the default retention standard at a minimum of two years. The CBA Section supports the need for government institutions to document their retention period, without advocating for specific maximum retention periods given the practical inability to determine a period that meets the needs of each institution subject to the *Privacy Act*. However, in both cases – where the information relates to a decision and where it does not – the necessity test offers appropriate guidance.

The CBA Section also recommends that the *Privacy Act* require institutions to be transparent and open about their retention periods, the rationale for that period, and any changes to the retention periods over time.

Q. 1(cc) Do the purposes for use and disclosure still align with the purposes for which an individual should reasonably expect government institutions to be using and disclosing personal information?

We believe that the use and disclosure sections on consistent use and public interest require amendment. The relevant parts of section 8(2) of the *Privacy Act* are:

> Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed.

9 This should not include training data that may have been used for a decision support system. It would be inappropriate to dispose of the training dataset used to develop the algorithmic tool later used for making individual decisions. Without the possibility of auditing the training dataset, it would be harder to ensure true accountability in the use of the algorithmic tool. Training biases flowing from biased data is a problem. That said, measures must also be taken to limit the risks of re-identification of anonymized data provided for auditing purposes.

a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose,

m) for any purpose where, in the opinion of the head of the institution,

i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

Consistent use is problematic as personal information can be collected if it is "directly related to and demonstrably necessary for the government institution's programs or activities". As discussed at Q.1(q), this can lead to problematic and expansive collection of personal information if interpreted too broadly.

The consistent use provision can also be problematic for the definition of administrative purpose. According to the *Privacy Act*, personal information concerning an individual that has been used by a government institution for an administrative purpose shall be retained by the institution for at least two years following the last time the personal information was used for the administrative purpose. "Administrative purpose" is defined as the use of information in a decision-making process that directly affects the individual. Keeping in mind the increase of collection of personal information and increased administrative decisions by government institutions since the Act was originally written, this definition should be updated. For instance, at present, the information of a federal employee using a key card to enter a government building could be considered as subject to an administrative decision. Thus, the concepts of consistent use and administrative purpose are problematic.

Additionally, the public interest provision could further be expanded. Provincial and territorial public sector statutes often allow non-consensual disclosure of personal information if release of the information would not result in an unreasonable invasion of privacy. For example, Nova Scotia's *Freedom of Information and Protection of Privacy Act* discusses the term "unreasonable invasion of [personal] privacy" and discusses factors and describes examples of situations. Provincial and territorial legislation should be considered when expanding the public interest provision.

Q. 1(dd) What use and disclosure provisions require additional safeguards, transparency and accountability mechanisms? Many stakeholders have highlighted information-sharing agreements as one example. Are there others?

The CBA Section agrees that information-sharing agreements would be useful to safeguard privacy. It would also help to give the OPC targeted, expanded powers to hold institutions to account, particularly after audits.

Q. 1(ee) With respect to information-sharing agreements, should domestic and international information-sharing be treated differently? Should government institutions be required to be transparent about the existence of information-sharing agreements and publish their contents? If yes, in what circumstances would exceptions to such a requirement be appropriate?

As highlighted in the CBA Section's 2016 submission, meaningful accountability for the collection, use and disclosure of personal information requires written information-sharing arrangements between government institutions (domestic or foreign), as well as with private sector organizations that receive personal information from government institutions. Wherever possible, these information-sharing arrangements should be transparent to the individuals who may be affected by them. We understand the need for confidentiality in some circumstances, such as where national security interests are engaged. While these considerations may militate against complete transparency of all details in information-sharing arrangements, they require a contextual case-by-case analysis. The general rule should be that these arrangements must be transparent and limits on transparency should apply only to the extent that transparency is reasonably likely to undermine the legally authorized and articulated purpose of the information-sharing.

We continue to support the requirement proposed by the Privacy Commissioner in 2006 that disclosure of personal information-sharing to a foreign government must be subject to a formal written agreement or arrangement and contain the following elements:

- a description of the personal information to be shared
- the purposes for which the information is being shared and will be used
- a statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially in regards to its use and disclosure
- a statement specifying whether information received by the federal government would be subject to the provisions of the *Privacy Act*
- a statement specifying whether information disclosed by the federal government would be subject to the provisions of the *Privacy Act*, and
- the names, titles and signatures of appropriate officials in both the supplying and receiving institutions and the date of the agreement.

Q.1(ff) In general, what criteria would be useful to guide the recognition of any new use and disclosure authorities?

For any new use and disclosure authorities identified, it is imperative that the mechanism used should be secure and transmit only necessary information. The federal public sector could use

the public health sector as a model, similar to how different health organizations and doctors have access to patients' personal information.

Q.1(gg) Where might there be gaps in the existing use and disclosure authorities? Is there a need to better support Canadians through particular life stages or events like the death of a loved one? Could all benefits programs share information to assist individuals and improve efficiency in their delivery?

Existing gaps were discussed at Q.1(cc). The CBA Section agrees that there is a need to better support Canadians through difficult life stages and events, such as the death of a loved one.

In this context, sharing examples of relevant privacy situations for applicable benefit programs will assist the public and improve awareness, understanding and efficiency of delivery.

Q.1(ii) In light of this complex legal environment, do any of the general use and disclosure provisions in the Privacy Act require modernization to ensure appropriate interoperability with these regimes?

The CBA Section believes that the *Privacy Act* requires modernization to ensure appropriate interoperability with specialized legal regimes dealing with national security, intelligence and law enforcement. However, individuals' privacy must not be unfairly compromised in the interest of these specialized legal regimes and only relevant information should be disclosed as part of these regimes. It is extremely important, particularly when one is dealing with aims of national security, intelligence and law enforcement, that privacy is not infringed unfairly, given the imbalance of power between the individual and the state.

We recommend that measures to modernize the *Privacy Act* for appropriate interoperability with specialized regimes dealing with national security, intelligence and law enforcement be made by amendments to the Act or by regulation. We have previously raised concerns about amendments to *Security of Canada Information-sharing Act* (SCISA) and the manner in which thresholds and safeguards to protect privacy in disclosing information in the interest of national security to other federal government institutions is not established by legislation (in SCISA or its regulation) but through national security mandates and Ministerial directives.[10] Important privacy requirements and obligations of government institutions should be articulated in express statutory provisions and not Ministerial directives that can be easily amended without notice or discussion.

10 See, CBA Section submission, Security of Canada Information Sharing Act (January 2017).

III. TRANSPARENCY AND ACCOUNTABILITY: DEMONSTRATING THE COMMITMENT AND RESPECT NECESSARY TO FACILITATE TRUST

Q. 2(k) What should the standard be before reporting a privacy breach? For example, how should a "material" breach be defined in the federal public sector?

As outlined in our 2016 submission, the CBA Section believes that while there should be a balanced approach to breach notification under the *Privacy Act*, the obligation imposed on government institutions should be at least as stringent as the breach notification regime imposed on private sector organizations under PIPEDA. In other words, the triggering threshold for notifying affected individuals and reporting to the Privacy Commissioner should be a "real risk of significant harm". This is essentially the same threshold as in the private sector privacy law in Alberta and the public sector law in Newfoundland and Labrador. The same test has been recommended by a special all–party legislative committee for inclusion in the BC *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*. Adding a "materiality" threshold for reporting breaches to the OPC might also be considered, as originally contemplated for the private sector, though it would be important that government institutions be required to keep records of all breaches.

Q. 2(l) In what circumstances should individuals be notified of breaches?

See response to Q.2(k).

Q. 2(m) How should the question of timelines for breach notification be managed? Is a prescriptive or context-sensitive approach better?

The CBA Section supports prompt notification to individuals and reporting to the Privacy Commissioner where a government institution has identified a "real risk of significant harm". Instead of a specific timeframe, the timing of notification and reporting should be flexible to accommodate considerations and circumstances of each breach. For example, it may be necessary to delay notification for law enforcement and other investigations. This approach was adopted in PIPEDA, which requires notification to be given "as soon as feasible".

The CBA Section recognizes the need to allow the government institution time to complete its response to the breach and collect as many facts as possible to report. Additionally, as is current practice in the private sector, government institutions should be permitted to update breach reports with new information as required.

Q. 2(n) Does the Privacy Commissioner require any new tools or powers to effectively oversee a privacy breach notification regime?

To the extent that the approach to breach notification under the *Privacy Act* is standardized with the approach under PIPEDA, the Privacy Commissioner should be granted the same powers as under PIPEDA. This would include, for example, the ability to require a government institution to provide access to or produce a record of a breach to the OPC.

IV. GREATER CERTAINTY FOR CANADIANS AND GOVERNMENT: DELINEATING THE CONTOURS OF THE *PRIVACY ACT* AND DEFINING IMPORTANT CONCEPTS

Q.3(a) Should the definition of personal information be grounded in the concept of identifiability, and if so, should this concept be defined?

The definition of personal information should be grounded in the concept of identifiability and the reference to recorded information removed from the definition. Removing reference to recorded information would modernize the *Privacy Act* and better recognize the importance of individuals' expectations for privacy and the government's collection, use and disclosure of their personal information.

The CBA Section, however, does not believe that identifiability should be defined. While we realize the possible challenges without a specific definition, we believe that determining whether specific information constitutes personal information should be done on a case-by-case basis given all the circumstances. It is practically impossible to create an exhaustive list of the kinds of information to be considered, just as the GDPR definition of "an identifiable natural person" does not aim for a comprehensive and exhaustive list of factors and information to be considered in making that determination. The burden of determining if the information is personal information is always on the entity subject to the legislation. That burden should be discharged considering all available information about the individual and the context surrounding the government institution.

Q.3(b) Does metadata require a separate definition altogether, or can the privacy issues relating to such information be addressed by an updated definition of personal information (including by adding an example)?

The CBA Section does not believe that metadata requires a separate definition. We agree that it would be appropriate to update the list of non-exhaustive examples of personal information to clarify new forms such as metadata and biometric data. However, we have two concerns about a separate definition for metadata. First, a separate definition might imply that metadata is something different from personal information. Second, a separate definition (and potentially different obligations and rights when it comes to metadata) may be counterintuitive to the principled approach of a technologically neutral *Privacy Act*. From our perspective, an updated list of non-exhaustive examples of personal information that includes metadata would be the better approach and one likely better to achieve the objectives of a principles-based approach to *Privacy Act* amendments.

Q.3(c) What role could de-identified, pseudonymized, or encrypted personal information play in a modern Privacy Act, and how should such terms be defined?

The legislation applies to personal information. Anonymized, de-identified or pseudonymized information is not personal information, so the legislation would not apply. Given this, the CBA Section does not object to defining anonymized, de-identified or pseudonymized information to provide that the legislation would not apply, provided that the legislation is clear that those kinds of information can possibly be reversed back to personal information such that the legislation would apply. Additionally, with respect to anonymized, de-identified or pseudonymized information, the legislation should clarify that the burden remains on the responsible government institution to ensure that the information is not personal information. It is important that once again context is considered, as rarely can black and white definitions apply.

We understand that encrypted information can remain individually identifying. Accordingly, the legislation should continue to apply to encrypted personal information from a broad application of the law perspective. However, the legislation may provide affirmative compliance incentives or liability exclusion based on reasonable investigation or due diligence for encrypted personal information. The burden should remain on the responsible entity to establish that this method was reasonably and diligently employed to safeguard the personal information given all the circumstances, including when a breach of security safeguards has occurred.

Q.3(d) What do you foresee to be the public's expectations concerning publicly available personal information?

Q.3(e) How could "public available personal information" be defined under a modern Privacy Act?

As the Supreme Court of Canada held in *R v Jarvis,*[11] "'privacy,' as ordinarily understood, is not an all-or-nothing concept … being in a public or semi-public space does not automatically negate all expectations of privacy." In our view, there is an expectation of privacy in personal information that may exist in the public domain when it comes to the collection and use by government institutions, unless proved otherwise given all the circumstances. The burden of proof should rest on the responsible government institution. In all cases, the collection of personal information, including personal information in the public domain, must be necessary for the government institution's mandate.

The CBA Section recommends that these concepts not be defined or carved out from the scope of the legislation's application. Including these definitions and concepts would give rise to confusion and uncertainty, as legally defining and determining publicly available personal information would be practically impossible. These issues require a case-by-case assessment of each circumstance, as to;

a) what constitutes the public domain,
b) which of the variety of public domains should be considered to determine if personal information is publicly available,
c) who is responsible to determine if certain personal information is publicly available, and
d) who is responsible for ensuring that the publicly available personal information is accurate and complete.

Q.3(f) Should consent be defined under a modern Privacy Act, and if so, what elements would it include?

The individual's control over disclosure and use of their personal information is the cornerstone of privacy as currently understood. Accordingly, the individual's consent is the single most important factor that determines expectations, rights and responsibilities. Consent should be defined and remain a key element in a modernized *Privacy Act*.

11 2019 SCC 10 at para. 41.

The underlying elements of proper consent have long been recognized in Canada's privacy laws:

a) proper disclosure of the purpose of the collection and use of personal information

b) voluntary provision of personal information for use within the disclosed purpose

c) ability to withdraw consent, subject to legal or contractual restrictions and reasonable notice

We agree in principle with the GDPR definition of consent but recommend that the definition be gender neutral and consent not be limited to "the processing of personal data." We propose the following: "any freely given, specific, informed and unambiguous indication of the data subject's desire, expressed by a statement or by an affirmative action, for the collection and use of personal information for their stated purpose."

Q.3(g) Should a modern Privacy Act still make distinction between administrative and non-administrative uses, and if so, how should an "administrative use" be defined?

All personal information collected, used and disclosed by a government institution should have the same principled approach whether its purpose is an administrative or non-administrative use. The distinction between administrative and non-administrative uses should be eliminated from the *Privacy Act*. In an effort to recognize the importance of privacy and to satisfy the expectations of individuals, government institutions should have the responsibility of viewing and approaching the collection, use and disclosure of personal information with the same principled approach regardless of its ultimate purpose.

Q.3(h) Should the concept of a "consistent use" be defined under the Privacy Act? If so, how?

Q.3(i) Could the criteria-based approach to "compatible uses under the GDPR assist to clarify the proper scope of a "consistent use" under the Privacy Act? If so, what factors should institutions consider?

A modernized *Privacy Act* should require government institutions to identify a specific purpose for collecting personal information and ensure the information is necessary for the articulated purpose or is authorized by law. An extension of this is ensuring that government institutions only use and disclose personal information for the specific purpose for which it has been collected.

PIPEDA contains an explicit consistent purpose provision for information "produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced." Some provincial and territorial public sector privacy laws grant a government institution the ability to use or disclose personal information for a purpose consistent with the purpose for which it was originally collected. For example, Alberta's *Freedom of Information and Protection of Privacy Act* states that personal information may be used or disclosed for the purpose for which the information was collected or compiled, or "for a use that is consistent with that purpose".[12] The Act further defines consistent use in section 41: "a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure (a) has reasonable and direct connection to that purpose, and (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information."

The CBA Section finds the GDPR approach to "compatible use" similar in nature to the approach under provincial and territorial public sector privacy legislation and believes it would add clarity and accountability for a government institution that could potentially rely on a consistent use. A defined consistent use would place the burden on the government institution to assess and determine if the use or disclosure of personal information is a consistent use, which should support a principled approach to respecting the privacy rights of individuals. The CBA Section supports a defined approach and believes that the obligation should be on government institutions if a consistent use is statutorily permitted.

V. A MODERN AND EFFECTIVE COMPLIANCE FRAMEWORK WITH ENHANCED ENFORCEMENT MECHANISMS

Q. 4(a) Should the Privacy Commissioner have an explicit mandate for education and outreach in relation to the public sector and if so, what should it include?

In its June 2008 and September 2016 submissions, the CBA Section supported former Privacy Commissioner Stoddart's recommendation to amend the *Privacy Act* to give the Privacy Commissioner a clear public education mandate. Many public sector privacy statutes authorize commissioners to engage in public education and section 24 of PIPEDA gives this mandate to the Privacy Commissioner in terms of private sector privacy. In the interest of standardization,

12 Section 39(1)(a) and section 40(1)(c)).

and since one federal regulator oversees privacy compliance in the public and private sectors, we recommend that the *Privacy Act* be amended to include similar language to that in section 24 of PIPEDA, with appropriate modifications for the public sector context.

> **Q. 4(b) Should a requirement to conduct a PIA be added to the Privacy Act? If so, is the current, policy-based "test" for when a PIA is required the most appropriate approach or are there other circumstances in which an institution should be legally required to undertake a PIA?**

In our June 2008 and September 2016 submissions, the CBA Section recommended that the *Privacy Act* be amended to require government institutions to conduct Privacy Impact Assessments (PIA) prior to developing any new, or substantially modifying existing programs or activities that involve the collection, use or disclosure of personal information. This would bring the Act in line with other public sector privacy statutes including the *Freedom of Information and Protection of Privacy Act* in BC[13], the *Health Information Act* in Alberta, and the *Access to Information and Protection of Privacy Act* in Newfoundland and Labrador.

The obligation to conduct a PIA in the provincial legislation mentioned is broader than the current policy-based test established by the Treasury Board for government institutions. As noted in the discussion paper, the Treasury Board Secretariat Directive only requires completion of a PIA where a new or substantially modified program or activity proposes to use personal information as part of a decision-making process that directly affects the individual, or where substantial modifications are made to a program or activity that is contracted out or transferred to another level of government or the private sector.

By contrast, BC's FIPPA and Newfoundland and Labrador's AIPPA each have a mandatory PIA requirement so a PIA must be completed by the provincial ministry in accordance with directions from the minister responsible for each Act. In BC, the minister's directions are that all ministries must complete a PIA when developing or changing an enactment, system, project, program or activity even if determined that no personal information is being collected, used or disclosed. Where no personal information is involved, however, a ministry is only required to complete Part 1 of the approved PIA template, which amounts to a preliminary assessment. In practical terms Newfoundland and Labrador takes a similar approach, however the availability of the preliminary assessment is expressly in section 72(1)(b) and (2) of AIPPA. In both provinces, completed PIAs (or preliminary assessments) must be submitted to the minister

13 See section 69(5)-(5.5).

responsible for the Act for review and comment. In some circumstances, like where a PIA concerns a common or integrated program, service or activity, the PIA must also be submitted to the commissioner for review and comment.

The broader scope of the mandatory PIA requirement in the provincial legislation mentioned is preferable to the narrower, policy-based approach in the Treasury Board Secretariat Directive. Particularly if the *Privacy Act* is amended to include a guiding principle of reasonableness and proportionality, privacy impacts should be minimized even where personal information is not used or disclosed to make a decision that directly affects the individual but is still collected for some legitimate purpose. In this respect, privacy impact minimization encompasses considerations about what and how much information is collected, how it is collected (directly or indirectly), how long it is retained and the security safeguards to which it is subject.

Conducting a PIA can be a significant undertaking. We commend the Newfoundland and Labrador approach that enshrines the availability of the preliminary assessment in legislation. If no significant personal information is implicated in a new or substantially modified program, service or activity, so there is little to no value in completing a PIA, then no PIA should be required.

Q. 4(d) Could the PIA process be improved by setting out the role of the Privacy Commissioner in response to a PIA, including what must be included by the OPC in any response to a PIA it reviews?

In jurisdictions where completion of a PIA is mandatory in the public sector, it is typically the role of the commissioner, as expressed in the applicable legislation, to review and comment on the draft. As the Privacy Commissioner has indicated, a PIA is essentially a risk management exercise and government institutions should retain full accountability for decisions that reflect their risk tolerance. This is particularly true when compliance is assessed against a set of principles as opposed to prescriptive rules with a bright line between right and wrong.

If the *Privacy Act* includes a mandatory PIA requirement and a requirement that certain types of PIAs be submitted to the Privacy Commissioner, the Privacy Commissioner would be reasonably expected to identify potential compliance issues. It should not, however, fall to the Privacy Commissioner to give a government institution specific instructions on how to achieve compliance. This would be overly burdensome for both the government institution and the Privacy Commissioner and could stifle innovation.

Q. 4(e) Is there a role for advance rulings or advisory opinions to supplement more general guidance from the OPC?

In some circumstances, advance rulings or advisory opinions could be useful to supplement general guidance from the OPC. The OPC must be cautious, however, in giving advance rulings or advisory opinions where it is difficult to determine all material facts, there is a question about proper jurisdiction, the request requires an interpretation of the legislation rather than the application of specific facts to the legislation and other circumstances.

The Alberta OIPC issued a *Practice Note* with guidelines for making an advance ruling and outlines circumstances where a request for one can be refused. Among other things, it states that a request for an advance ruling will be refused if it involves a new legal issue. New legal issues, issues that arise from advancements in technology as an example, might be suitable for advance rulings or advisory opinions in certain circumstances.

If the OPC had authority to make advance rulings or issue advisory opinions and it followed similar guidelines as in the Alberta *Practice Note*, we do not expect the OPC would receive a large volume of requests. Reported data from 2007 to 2018 shows the Alberta OIPC received only two requests for advance rulings. One request was refused in a reported decision, and the response to the other was not reported.

Q. 4(f) In what circumstances would the issuance of an advance ruling or advisory opinion be appropriate? Could it be integrated into the PIA process in some circumstances?

See response to Q.4(e).

Q. 4(g) Should the Privacy Commissioner have the discretion to decline to investigate a complaint? Under what circumstances?

In 2012, the CBA urged the federal government to amend the *Privacy Act* to give the Privacy Commissioner discretion to decline complaints or discontinue investigations based on certain criteria, including those that are trivial, frivolous, vexatious, made in bad faith, supported by insufficient evidence, dealt with already by the Privacy Commissioner or better resolved in a different forum. This amendment would be consistent with provincial and territorial laws as well as federal laws applicable to the private sector. It would also allow the resources of the Privacy Commissioner to be used more efficiently and effectively, such as to allocate greater investigative resources to systemic issues that affect all Canadians.

At a minimum, we support amending the *Privacy Act* to authorize the Privacy Commissioner to refuse to investigate or cease to investigate a complaint that the Privacy Commissioner believes to be trivial, vexatious or made in bad faith. Otherwise, the complaint investigation backlog will only be increased. This would parallel the approach in BC and Quebec, and mirror the Privacy Commissioner's powers under sections 12 and 12.1 of PIPEDA. The CBA Section recommends that, similar to PIPEDA, the *Privacy Act* require that parties to the complaint be given written reasons for the decision, which could then be subject to judicial review.

To the extent that compliance agreements may become a feature of the *Privacy Act*, the Privacy Commissioner should have discretion to discontinue a complaint investigation where the government institution has entered into a related compliance agreement.

Q. 4(h) Should the Privacy Commissioner have the discretion to discontinue a complaint investigation or decline to prepare a comprehensive investigation report? If so, in what circumstances?

See response to Q.4(g).

Q. 4(i) Should the Privacy Act be amended to require a complainant to first address their complaint to the government institution involved?

There are arguments both for and against imposing a mandatory requirement on individuals to first address privacy complaints to the government institution involved. While this requirement may reduce workload by diverting complaints from the Privacy Commissioner's investigative process, individual access to justice may also be impaired by the lack of a timely response by the government institution.

Individuals should be encouraged to first address their complaints to the government institution directly. In the provincial and territorial context, it is our experience that most public bodies actively encourage individuals to do that, particularly for access to information requests. We also know that many complaints are not resolved this way. To enhance access to justice, any obligation added to the *Privacy Act* to initially address complaints to government institutions should be coupled with an obligation on the government institution to respond to the complaint in a legislated timeframe. On receiving the government institution's response, or on receiving no response in the legislated timeframe, the individual should then be permitted to file a complaint with the Privacy Commissioner without delay.

If the Privacy Commissioner is granted the power to decline to investigate or to discontinue an investigation, which we support, it could still be open to the Privacy Commissioner to cease an

investigation where a government institution does eventually provide what the Privacy Commissioner considers to be a fair and reasonable response to the individual.

Q. 4(j) How can the Privacy Commissioner's mediation role best be reconciled with the potential introduction of order-making powers?

If order-making powers for the Privacy Commissioner are added to the *Privacy Act*, the current ombudsperson model office must be reorganized to accommodate an administrative tribunal model. Given the need for additional formality and process considerations, a clear delineation between staff responding to complaints and staff acting as adjudicators is necessary to ensure administrative fairness for all parties in the context of a formal inquiry.

Many commissioners with order-making powers (e.g. BC, Alberta, Ontario) publish annual reports on the number of requests for review received, the number that settle in mediation and the number that proceed to inquiry. Most requests for review settle in mediation.[14]

Q. 4(k) Would introducing compliance agreements be an effective way of promoting a negotiated but binding resolution of complex privacy issues in the public-sector context?

While the CBA Section cannot comment on the anticipated effectiveness of amending the *Privacy Act* to make compliance agreements available as a remedial and enforcement mechanism, we support this tool for the Privacy Commissioner. With an element of choice by the government institution, the effectiveness of compliance agreements can only be assessed once the willingness of government institutions to enter into agreements is known.

The effectiveness of compliance agreements will also be affected by the alternative enforcement mechanisms that may be available to the Privacy Commissioner. Under the current Act, there is little incentive for a government institution to enter into a compliance agreement to avoid completion of an investigation by the Privacy Commissioner. This is because there is no effective remedy or enforcement mechanism if the government institution does not voluntarily comply with a recommendation resulting from the findings of that investigation. Possible embarrassment to a government institution of being named by the Privacy Commissioner in a public report is insufficient. This is in contrast to the potential impact of public reporting of investigations in the private sector context, where private organizations stand to lose goodwill, market share and price, at least to the extent that

14 See for example, the 2017/18 *Annual Report* of the Information and Privacy Commissioner of BC indicating that 431/556 requests for review closed that year were mediated/resolved (at 27).

individuals have the option to deal with a different organization offering similar products or services. Individuals do not have the same choice about making their personal information available to government.

Q. 4(m) How could an order-making model under the Privacy Act retain the elements of the existing regime that support access to justice for complainants?

See response to Q.4(j) about maintaining the mediation role of the Commissioner.

Q. 4(n) Would expanding the Federal Court's judicial review jurisdiction to ensure comprehensive legal remedies were available for the full range of rights under the Privacy Act be a viable alternative to order-making powers as the impact of other significant changes was becoming known?

Shortcomings in the current ombudsperson model have been identified throughout the history of the *Privacy Act*. Under section 41, the Federal Court may only review a refusal by a government institution to grant access to personal information under section 12 of the Act. While the Act contains other legal restrictions on what personal information a government institution can collect, how that information can be used and when it can be disclosed, there is no clear remedy in the Act for individuals who believe a government institution has not met its duties.

We have previously recommended that the *Privacy Act* be amended to give the Federal Court oversight and a remedy for individuals with grievances under the Act. The *Access to Information Act* was recently amended to grant the Information Commissioner limited order-making powers. The *Privacy Act* and the *Access to Information Act* have historically been treated as a package – a seamless code in the form of two complementary statutes – so it may be desirable to grant the Privacy Commissioner the same or similar order-making powers as the Information Commissioner, given their related roles. Access to Information and Privacy (ATIP) Coordinators in federal departments routinely deal with both statutes.

However, that in and of itself should neither be the sole reason nor a determining factor. Consideration should also be given to the current powers of the Privacy Commissioner under PIPEDA for the private sector. Access to justice considerations should also be part of any decision to expand the Federal Court's judicial review jurisdiction without a corresponding amendment of the enforcement model for the Privacy Commissioner. The practical viability of accessing the Federal Court would be questionable for many applicants, given the time and

expense, though the experience on the private sector side is that individuals can and do seek recourse to the Federal Court.

VI. MODERNIZING THE PRIVACY ACT'S RELATIONSHIP WITH CANADA'S INDIGENOUS PEOPLES

The First Nations Principles of OCAP (ownership, control, access and possession) means that First Nations control data collection processes in their communities."[15] The principles are standards published by the First Nations Information Governance Centre.[16] We are aware of the principles and the importance of the associated concept of community privacy rights. The principles establish how First Nations data should be collected, protected, used or shared, and guide how research relating to First Nations communities should be approached. The premise is that First Nations have control over data collection processes in their communities and that they (referring to the collective community) own and control how that information can and should be used.

We suggest that Justice Canada consult with First Nations, other Indigenous groups (OCAP does not apply to Indigenous groups beyond First Nations) and non-Indigenous stakeholders to craft specific principles or directions for collection, use, disclosure, storage and handling of personal information of Indigenous peoples. Consideration should be given to whether all or some of the OCAP principles can or should have any application to groups, including other Indigenous groups, beyond First Nations.

It is questionable whether a specific approach to government institutions' handling and sharing of the personal information of Indigenous persons – assuming a tailored approach will be developed – would be best incorporated in the *Privacy Act*, or in stand-alone legislation that the *Privacy Act* references. We note that some non-Indigenous groups may also argue that the concept of community privacy rights should be extended to their groups.

15 https://www.afn.ca/uploads/files/nihbforum/info_and_privacy_doc-ocap.pdf.

16 The Centre is an incorporated non-profit with a mandate from the Assembly of First Nations Chiefs in Assembly: see, https://fnigc.ca/.

Q.5(a) What changes to the Act could be implemented to assist Indigenous peoples in accessing personal information held by the federal government that is relevant to their communities or claims? How should this be managed?

Section 8(2)(k) of the Act says that personal information under the control of a government institution may be disclosed to "any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada." This could be interpreted to allow any of the Indigenous empowered persons listed first, across Canada, to request disclosure of personal information for the "purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada", which might include personal information of members of distinct Indigenous peoples (First Nation, Inuit, Métis) and sub-groups (bands, councils, etc.) by any other Indigenous empowered persons. This may diminish the sovereignty of distinct Indigenous peoples in Canada and be considered pan-Indigenous.

We are concerned that this clause may be interpreted very broadly. Disclosure of personal information without consent to an Indigenous government, association of Indigenous people, band, etc. might be justified where the recipient is the entity to which the subject individuals belong (e.g. disclosure of personal information without consent to a band where the subject individuals are members of that same band). Consideration should be given, however, to the extent to which personal information should be disclosed without consent to an entity with which the subject individual is not associated in any way. For example, in keeping with the OCAP principles, would a First Nation have a right under the *Privacy Act* (or elsewhere) to exercise control over further distribution of the personal information of its members to other Indigenous entities? These requirements would have to be balanced against the advantages of freer disclosure of personal information for research, validation of claims, disputes and grievances. However, this clause could also be open to abuse where one Indigenous entity authorizes a third-party with an economic interest in collecting personal information for the validation of claims, who then requests personal information of individuals who are members of a separate Indigenous community (e.g. a lawyer pursuing a class action may receive authorization from an Indigenous entity and then request disclosure of personal information on individuals across Canada who belong to other Indigenous communities).

Currently, disclosures under section 8(2)(k) are not subject to other requirements, including that the recipient is able to protect the personal information on receipt. We suggest consideration be given to whether the recipient should be subject to the same provisions for the protection of personal information, on receipt of the information, as other organizations under the Act. In the alternative, receipt of personal information under section 8(2)(k) could be subject to the Act or an agreement among Canada and the recipient on protection of the information. Another option would be for receipt of personal information under section 8(2)(k) to be subject to the Act or an agreement with Canada, unless the recipient has enacted its own laws on protection of personal information that are consistent with the Act. Again, these changes would need to be balanced against the chilling effect that further requirements imposed on recipients may have.

Q.5(b) How should the existing provisions organized around Indigenous groups, governments or other collectivities be updated?

The definitions of "Indian Band" and "aboriginal government" should be updated to remain current with recent and future treaties. It may be advisable to change the "Indian band" definition to include a catch all phrase like "first nation recognized as a "band" pursuant to any act of Parliament" (for example), and similarly for "aboriginal government" to include communities that have entered into self-government agreements or treaties with Canada.

Additionally, there does not seem to be a definition of "association of aboriginal people" in section 8 which may be necessary to avoid disclosure of personal information to associations claiming to be Indigenous but not recognized by the federal government or the Indigenous peoples of Canada.

Though it may not be necessary, it may be advisable to include a definition of Indigenous peoples in the interpretation section of the Act or in section 8.

Q.5(c) Are there other issues respecting Indigenous peoples and personal information that should be addressed in the modernization of the Privacy Act?

In the wake of the Truth and Reconciliation Commission, the Act may need to address the ability of survivors to have personal information exempt from disclosure. Consideration should be given to the Act offering a mechanism specifically for survivors of the residential school system in Canada to opt out of having personal information about their experiences and trauma disclosed without their consent.