THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Modernizing Canada's Privacy Act

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION

February 2021

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 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 Section.

TABLE OF CONTENTS

Modernizing Canada's Privacy Act

Modernizing Canada's Privacy Act

I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law Section (CBA Section) is pleased to comment the discussion papers issued by Justice Canada in November 2020 on the modernization of the Privacy Act. The Section represents specialists in privacy law and access to information issues from across Canada. In October 2019, the CBA Section responded to Justice Canada's call to modernize the *Privacy Act* and related subjects[1] (October 2019 submissions). The CBA Section would like to expand on those submissions for several points raised in the November 2020 Discussion Paper:

- Title and Purpose of the *Privacy Act*
- Definition of Personal Information
- Definition of Federal Public Body
- Limiting Collection of Personal Information
- Publicly Available Information
- De-identified Personal Information
- Security Safeguards and Breaches of Safeguards
- Automated Decision-Making
- Access by Non-Residents
- Sharing and Disclosure of Personal Information Among Public Bodies and Service Providers
- Enforcement
- In addition to the October 2019 Submissions, we incorporate by reference several past CBA submissions and resolutions:
- Letter to Minister of Justice on *Privacy Act* amendments (June 2012)[2]
- Privacy Act amendments, CBA Privacy and Access Law Section submission to Privacy Commissioner of Canada (September 2016)[3]

---

1 Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA, online, *Privacy Act Modernization*, online and Transfers of Information for Processing, online.

2 www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR8434213/br-external/CanadianBarAssociation-e.pdf

3 www.cba.org/CMSPages/GetFile.aspx?guid=872b4258-e501-41cf-8676-fe08dea34deb

- *Privacy Act* Reform, CBA submission to House of Commons Committee on Access to Information, Privacy and Ethics (June 2008 submission)[4]
- CBA Resolution 12-01-M, *Privacy Act* amendment (February 2012)[5]
- CBA Resolution 08-06-A, Comprehensive Revision of the *Privacy Act* (August 2008)[6]
- CBA Resolution 06-03-A, *Privacy Act* Review (August 2006)[7]
- CBA Resolution 04-06-A, Limiting State Access to Private Information (August 2004)[8]
- CBA Resolution 04-05-A, Privacy Rights in Canada (August 2004)[9]

II. TITLE AND PURPOSE OF PRIVACY ACT

The CBA Section supports amending the title of the *Privacy Act* to accurately reflect the specific context in which it regulates the collection, use, retention and disclosure of personal information in the broader set of laws that embody the fundamental value of privacy, such as the *Criminal Code*, common law and civil law obligations, human rights laws, and other federal, provincial and territorial legislation. We believe the purpose clause should be modernized to reflect the balance of privacy interests against the legitimate needs of government institutions to collect, use, and, in limited cases, disclose personal information to develop public policy, to support innovation in public services, to manage the economy prudently, and to effectively and efficiently deliver services to individuals. We would also add an overarching principle that pseudonymized or anonymized data should be used where possible in research and in the development and management of government programs and services.

III. DEFINITION OF PERSONAL INFORMATION

Justice Canada suggests updating the definition of "personal information" to include unrecorded personal information. In our October 2019 submissions, we agreed that reference to "recorded" information should be removed from the definition. While the *Privacy Act* is organized around the concept of a "record," including all forms of personal information is consistent with fostering the dignity, autonomy and self-determination of individuals and

4 www.cba.org/CMSPages/GetFile.aspx?guid=602bcb8f-8195-48d9-b156-506f18995c20

5 www.cba.org/getattachment/Our-Work/Resolutions/Resolutions/2012/Privacy-Act-Amendment/12-01-M-ct.pdf

6 www.cba.org/CMSPages/GetFile.aspx?guid=e57b3073-09bd-44a3-91d5-c664b44309f2

7 www.cba.org/CMSPages/GetFile.aspx?guid=e57b3073-09bd-44a3-91d5-c664b44309f2

8 www.cba.org/CMSPages/GetFile.aspx?guid=e57b3073-09bd-44a3-91d5-c664b44309f2

9 www.cba.org/CMSPages/GetFile.aspx?guid=e57b3073-09bd-44a3-91d5-c664b44309f2

public trust and confidence in government. A comprehensive Act is important to achieve those purposes. In practice, the *Privacy Act* could include the express duty to record personal information used to make a decision about an individual. The Act could also include an express duty of confidentiality for unrecorded personal information.

The Discussion Paper suggests clarifying when an individual is "identifiable". In the absence of statutory guidance, the Federal Court adopted two statements explaining the meaning of identifiable. Recently, in *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness),*[10] Justice McHaffie summarized and attempted to reconcile the appropriate test:

> [53] At the same time, however, the "serious possibility" of Gordon and the "reasonable to expect" of NavCanada both appear to convey effectively the same standard: a possibility that is greater than speculation or a "mere possibility," but does not need to reach the level of "more likely than not" (i.e., need not be "probable" on a balance of probabilities). Applying such a standard recognizes the importance of access to information by not exempting information from disclosure on the basis of mere speculative possibilities, while respecting the importance of privacy rights and the inherently prospective nature of the analysis by not requiring an unduly high degree of proof that personal information will be released.
>
> [54] Beyond this, it seems unnecessary, and may even be impossible, to try to further subdivide or parse the requisite degree of likelihood that an individual could be identified.

This decision highlights two identification challenges: (i) articulating what is greater than speculation or mere possibility; and (ii) understanding how to evaluate that threshold given other "available information". Importantly, what constitutes "speculation" or a "mere possibility" is not a common-sense matter. The assessment depends on the person's data science skill and knowledge of otherwise available information – whether to the public or to a class of individuals or organizations (see paras. 63 to 68).

Given the challenges in recognizing identifiable information, the CBA Section considered whether statutory guidance would assist government institutions. Ultimately, we continue to support our October 2019 submissions that state it is not possible to create an exhaustive list of factors to determine what constitutes "identifiable" information. This would likely result in a mere crystallization of the current state of the law or a minor variation of it which may have unintended negative consequences. Occasional judicial consideration of this concept in the context of an actual fact pattern has the benefit of revealing nuances or criteria that are difficult to anticipate.

---

10 2019 FC 1279, at paras. 53-54.

IV. DEFINITION OF FEDERAL PUBLIC BODY

The CBA Section supports replacing the term "government institution" with "federal public body". To ensure full accountability to the public, the definition of "federal public body" should include institutions like the Prime Minister's Office, Minister's offices, Senators, Members of Parliament and administrative institutions that support Parliament. Exceptions should include personal, political or constituent records, similar to provincial privacy legislation which excludes constituency records of members of elected office.

V. LIMITING COLLECTION OF PERSONAL INFORMATION

The Discussion Paper suggests that the personal information requirement to "relate directly to an operating program or activity" of the government institution be removed as a limiting principle. Instead, the test would be whether the information was "reasonably required." The CBA Section recognizes the inadequacy of the existing "directly relevant" test. However, we continue to be concerned that the "reasonably required" test is inappropriate in the public sector context. We question why the public sector would have a lower threshold for lawful collection than is imposed on the private sector under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the proposed *Consumer Privacy Protection Act*.

The CBA Section asserts its longstanding position that government institutions identify the specific purpose for collecting personal information and ensure the information is reasonably necessary for its articulated purpose or authorized by law. As outlined in 2019, 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[11] and supported by most witnesses appearing before that Committee.

Reasons supporting our October 2019 submissions include:

- Parliament's delegation to government officials to determine what constitutes a reasonable and proportional invasion of privacy should be limited given the quasi-constitutional nature of privacy.
- Government institutions have various sizes and internal capacity to make these decisions.
- Without proactive review of government institutions' decisions by the Office of the Privacy Commissioner, it is likely that inconsistent practices will develop across institutions.

11 Report 4: Protecting the Privacy of Canadians: Review of the Privacy Act (2016)

The CBA Section has not seen evidence that the "necessity test" unduly hampers government institutions' ability to carry out their mandates effectively. If they are so hampered, it indicates that the information collection is necessary. A requirement that the information be "reasonably necessary" must not be confused with "strict necessity". The Act could clarify that "reasonable necessity" is met if there is a demonstrable evidentiary need that the information assists in achieving the collection purpose, and the loss of privacy is proportional to the collection given other ways of achieving the objective.

If government institutions require broader information to conduct research and develop public policy, a less strict test for the collection and use of anonymized or pseudonymized information may be appropriate. However, as discussed below with respect to sharing information, the CBA Section believes that additional safeguards would be required during a privacy impact assessment process.Finally, the CBA Section believes there should be a right to appeal to the Office of the Privacy Commissioner (OPC) and, thereafter, to the Data Protection Tribunal. Individuals or organizations could challenge whether the reasonable necessity test has been met and/or whether a government institution is correctly interpreting its statutory right to collect, use or disclose personal information. We will comment on the organization and implementation of the Data Protection Tribunal in the context of submissions relating to Bill C-11, which we will share separately with Justice Canada.

VI. PUBLICLY AVAILABLE INFORMATION

The Discussion Paper states that the *Privacy Act* applies to "publicly available personal information" so the rules relating to collection and retention of personal information apply to publicly available personal information. However, the *Privacy Act* does not restrict government institutions from the subsequent use or disclosure of publicly available information.

The *Privacy Act* does not define "publicly available" personal information. The CBA Section supports the proposal to define that term, noting it is similar to the express definition of "publicly available information" in the *Communications Security Establishment Act* (CSE Act). The CSE Act defines "publicly available information" in section 2:

> Publicly available information means information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. It does not include information in respect of which a Canadian or a person in Canada has a reasonable expectation of privacy.

The *Canadian Security Intelligence Service Act* (CSIS Act) also includes the concept of a "publicly available dataset". In contrast to the CSE Act, the CSIS Act does not define "publicly available". However, the CSIS Act has a governing regime for use and retention of publicly available datasets. The CBA Section supports defining what constitutes "publicly available" information and endorses ensuring that the definition excludes information for which a person has a reasonable expectation of privacy. However, unlike in the CSE Act (with its consideration of national security), the CBA Section does not believe that the *Privacy Act* definition should distinguish between the interests of Canadian citizens and persons in Canada from non-Canadians and persons outside of Canada. Where appropriate, exceptions can be made on a case-by-case basis in statutes where a distinction is required for the context of that legislation.

The CBA Section supports specialized rules for using or sharing publicly available information "to align public sector use and disclosure of publicly available personal information with individual's reasonable expectations of privacy" as stated in the Discussion Paper. In our October 2019 submissions, we stated that "[t]hought 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." In our comments on Bill C-59*, National Security Act*, 2017,[12] we said even though the expectation of privacy may be lower or non-existent in publicly available information, "inferences not obvious in the data themselves could still be obtained by processing the information through modern analysis methods, particularly when combined with other datasets." Therefore, consideration should be given to:

- Criteria for determining what constitutes "publicly available" and requiring a mechanism to ensure accountability for that determination.
- Ensuring privacy impact assessments are conducted for the use or disclosure of publicly available information.
- Criteria for determining appropriate retention periods, including the likely relevance and accuracy of the information.
- Requirements to disclose the types of information and the uses and disclosures of publicly available information.
- Notification of adverse decisions based on publicly available information and mechanisms to challenge decision-making about an individual based on publicly available information.

12 Bill C-59 – *National Security Act*, 2017, online.

Finally, as said in the October 2019 submissions, the CBA Section remains of the view that collection of publicly available information must be *necessary* to achieve the government institution's mandate.

VII. DE-IDENTIFIED PERSONAL INFORMATION

Justice Canada proposes to define "de-identified" personal information and to regulate its use. The CBA Section has previously stated that de-identified information is not "personal information" (see above for Federal Court's test for what constitutes "identifiable"). We suggest that proposals to regulate de-identified information require further study. "De-identified personal information" is defined in the Discussion Paper as "personal information that has been modified so that it can no longer be attributed to a specific individual without the use of additional information". We believe what is being described is "pseudonymized data," the term used in the European Union's General Data Protection Regulation[13] (GDPR) and more broadly in the privacy profession. Article 4 of the GDPR defines "pseudonymization":

> Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

We agree that pseudonymized information can meet the definition of "personal information" if the "additional information" is otherwise available and there is a serious possibility that it can be combined with the pseudonymized data.

The recently tabled Bill C-11 takes a different approach to the meaning of de-identified information. It defines "de-identify" in a manner that would arguably not be "personal information" under the current threshold established by the Federal Court:

> Personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.

Pseudonymizing personal information is a privacy protection technique and the CBA Section endorses its use. However, in our view, pseudonymization would not allow for the types of uses and disclosures the Discussion Paper suggests unless they were permitted for the

13 (EU) 2016/679

information in its identifiable form. By contrast, if the information is de-identified to the extent that it could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual, then we question whether this information is personal information at all under the Federal Court's test.

In conclusion, we think there is a significant risk of introducing terminological and analytic confusion by introducing a concept of "de-identified" personal information and we recommend that Justice Canada subject this to further study and consultation.

VIII. SECURITY SAFEGUARDS AND BREACHES OF SAFEGUARDS

The CBA Section has long called for government institutions having a general statutory obligation to protect the personal information they hold with appropriate safeguards to the sensitivity of the information being protected: see June 2008, September 2016, and October 2019 submissions.

The CBA Section agrees with the Discussion Paper that the *Privacy Act* set out the statutory obligation in general terms, to be supplemented with regulations and operational guidance from the Minister. We encourage developing and refreshing minimum published standards. Probable salutary effects for doing so include: (1) Canadian businesses that wish to do business with the Government of Canada could design their products and services to meet these evolving standards; and (2) these standards could be instructive more generally for the public and private sectors as well as being educative for the general public.

Consistent with our September 2016 and October 2019 submissions, the CBA Section advocates for a breach notification and reporting obligation that is as stringent as the private sector's obligation under PIPEDA. The triggering threshold should be a "real risk of significant harm". There is no principled basis for imposing an additional "materiality" threshold resulting in different treatment of information depending on whether the information is in the control of a public body or a private sector organization. Indeed, a less onerous standard for public bodies is likely to erode government trust and is antithetical to the principle of accountability. Adding a "materiality" threshold for reporting breaches to the OPC can be considered, however, as originally contemplated for the private sector, though it is important that government institutions keep records of all breaches. The different standard for reporting to the OPC could be justified when paired with the power of the Commissioner to conduct compliance audits (and resources to do so).

IX. AUTOMATED DECISION-MAKING

The CBA Section agrees that automated decision-making is important for government institution activities and their transparent use should be encouraged. While much academic or policy work deals with privacy and automated decision-making, there has been less direct *practical* experience on to how automated decision-making will fit in established principles of administrative law – including substantive and procedural fairness.

Some CBA Section members endorse greater transparency and accountability requirements to notify individuals of automated decision-making systems, the types and sources of personal information they use and general information on how they function. Other members believe that this emphasis is misplaced. They do not support notification obligations that imply automated decision-making is inherently dangerous to the dignity and privacy of individuals. These members think government institutions should focus on notifying individuals when an adverse decision has been made about them by applying automated decision-making and on a redress mechanism that meets the principles of procedural and substantive fairness. Given the potential complexity and opacity of automated decision-making, these CBA Section members emphasize the need for individuals to have a practical ability to meaningfully challenge adverse decisions.

X. ACCESS BY NON-RESIDENTS

The Discussion Paper proposes a pilot to expand access rights to include foreign nationals not present in Canada (with adequate procedures to verify the identity of the person). We suggest a pilot is an appropriate method to test the impact of this on public resources and the system as a whole.

The CBA Section does not believe there is a principled basis on which to distinguish access rights between Canadians and foreign nationals not present in Canada. As noted in the Discussion Paper, a universal right of access would "bring Canadian law in line with other jurisdictions' practices of providing universal access to personal information and enhance interoperability with the European Union in particular." Further, in current practice, foreign nationals use third parties present in Canada to request personal information on their behalf under the *Access to Information Act* (ATIA).

The CBA Section asks Justice Canada to consider whether individual identity verification procedures will act as a natural limiting condition on the volume of requests.

XI. SHARING AND DISCLOSING PERSONAL INFORMATION

The Discussion Paper proposes that the *Privacy Act* "clarify which federal public body, or bodies, would be responsible for personal information where two or more federal public bodies have access to the same datasets, such as where a shared database is accessed by a number of federal public bodies".

The CBA Section generally supports this proposal but recommends taking it further. The *Privacy Act* should contain a framework clarifying how it applies when information is: (i) shared with or disclosed to provincial and territorial government institutions or public bodies; (ii) shared with or disclosed to foreign government institutions; (iii) shared with service providers of federal government institutions; (iv) collected from private sector entities; and (v) disclosed to private sector entities for their own use. In addition, we recommend that federal public bodies consult with affected provincial and territorial government institutions or public bodies and affected private sector entities when preparing privacy impact assessments (PIAs)on the collection from or disclosure to those other institutions or private sector entities so privacy impacts (and alternative measures) are examined in their total context.

Meaningful accountability for 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. The CBA Section envisions limited exceptions to this general principle. For example, a written information-sharing arrangement would be required for sharing information to further an investigation or other cases of disclosure permitted under the Privacy Act that were not part of a systematic program of information sharing.

Subject to situations where confidentiality is required for national security reasons or to protect other compelling national interests, sharing arrangements should be transparent to the individuals who may be affected by them. Further, there should be adequate mechanisms to seek redress for the misuse of personal information by the government institution (domestic or foreign) or the private sector organization. In particular, the CBA Section continues to support the requirement proposed by the OPC in 2006 that disclosure of personal information-

sharing to a foreign government must be subject to a formal written agreement or arrangement with 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 for 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.

The CBA Section also believes that the *Privacy Act* would benefit from controller provisions addressing processor obligations when government institutions use third-party service providers to process personal information or to perform duties on behalf of the government institution, as well as when a government institution acts as a service provider to another federal, provincial or territorial government institution. In the CBA Section's March 2020 submission to Innovation, Science and Economic Development Canada (ISED),[14] we described the uncertainty created under *PIPEDA* by the OPC's Report of Findings #2019-001 on the Equifax data breach and the OPC and the Information and Privacy Commissioner for British Columbia's joint investigation report into AggregateIQ Data Services (AIQ) (Report of Findings #2019-004). A particularly disturbing feature of the AIQ Report of Findings is the suggestion that *PIPEDA* requires the service provider to second-guess the government institution's legal basis for processing (and, indeed, require the individual's consent even if not a feature of the applicable government institution law) when a private sector organization processes personal information on behalf of a government institution. Many of our concerns will be addressed if Bill C-11[15] is enacted as currently drafted. However, the roles and responsibilities of private sector organizations processing personal information could be addressed directly to avoid uncertainty or inconsistent provisions in government contracts. In particular, the following issues could be addressed:

- Confidentiality of personal information.
- Duty to comply with the public body's instructions.

---

14 Proposed amendments to PIPEDA to address controller/processor obligations, letter online.

15 Bill C-11, *Digital Charter Implementation Act, 2020* (November 2020)

- Access requests.
- Breach notification and reporting.

Another situation to be addressed, possibly by regulation-making powers, is when a government institution is involved in an activity with multiple levels of government. There was much confusion as to how federal and provincial privacy laws would apply in Waterfront Toronto's proposed partnership with Google affiliate Sidewalk Labs. Waterfront Toronto was not itself subject to the *Privacy Act* or the Ontario *Freedom of Information and Protection of Privacy Act*[16]. Many early proposals involved processing information that might have involved multiple levels of government as well as private sector organizations.

More concretely, the CBA Section is aware of the difficulties that Saskatchewan has had in implementing *The Interpersonal Violence Disclosure (Clare's Law) Act*[17] , or its equivalent in other provinces, when the Royal Canadian Mounted Police (RCMP) acts as a local police service – essentially as a service provider to a province or municipality. The RCMP, while supporting the development of Clare's Law, has stated that the federal *Privacy Act* precludes it as a "government institution" from making the required disclosures. The CBA Section agrees with this interpretation of its *Privacy Act* obligations but finds it at odds with reasonable expectations that the RCMP, acting as a contracted provincial or municipal police force, will comply with provincial laws governing access and disclosure of records under provincial freedom of information and privacy laws or legislation such as Clare's Law.

The uneven application of provincial law also concerns broad police accountability. For example, in Halifax, the RCMP and Halifax Regional Police jointly deliver services. If an individual seeks information related to an incident, access to information and application of the law depends on which police agency responded to the incident. A Nova Scotian appears to have different rights depending on who was the first officer on the scene. The same situation can exist in other provinces where the RCMP acts as the provincial police force.

Confusion relating to local law enforcement accountability was also highlighted in the aftermath of the mass shooting in Nova Scotia in April 2020. The shootings took place in an

16 R.S.O. 1990, C. F.31

17 SS 2019, c I-10.4. The CBA Section does not take a view at this time on the merits of Clare's Law though it does endorse the CBA submission on non-conviction records and the privacy of alleged offenders. We note CBA Resolution 19-03-A urging federal, provincial and territorial governments to adopt or amend legislation and policies limiting disclosure of non-conviction information in law enforcement databases, and providing a mechanism for individuals to review and address errors or immaterial information in those databases.

area policed by the RCMP acting under contract as the Nova Scotia provincial police. The provincial government held that shooting inquiries fell under the federal *Inquiries Act* since the provincial statute would not confer jurisdiction over the actions of the RCMP, though they were clearly acting as a police force under the provincial *Police Act.*[18]

In these circumstances, the RCMP acts as a contractor for the province, fulfilling the provincial constitutional mandate for local law enforcement. A citizen's rights should not depend on the government official's uniform. Residents of provinces whose public sector privacy laws restrict outsourcing personal information would not benefit from those laws if the province contracts policing services to an organization whose provincial privacy laws have no similar restriction.

Finally, the CBA Section recommends federal government institutions consult with other affected governmental institutions or private sector entities when conducting PIAs) involving arrangements in which information is collected from, shared or disclosed to those governmental institutions and private sector entities. We believe this consultation is necessary to give the federal government institution the full context of the potential privacy impacts of the collection, use and disclosure. It would also assist the federal government institution in exploring ways to mitigate the impacts of the collection, use or sharing. In the private sector, service providers and business partners are routinely consulted during the PIA process. Internationally, a cooperation clause for data privacy impact assessments is a standard feature of data protection agreements under the GDPR, given the benefits to this type of consultation.[19]

XII. ENFORCEMENT

On the Discussion Paper proposals to enhance and modernize enforcement provisions in the *Privacy Act* and to grant the Privacy Commissioner additional powers, the CBA Section refers to its October 2019 submissions in support. We make the following additional comments.

The Discussion Paper proposes that federal government institutions can, with the Privacy Commissioner's approval, refuse requests for access to personal information under the *Privacy Act* if the request is vexatious, made in bad faith, or otherwise an abuse of the right to make such requests. The CBA Section does not have a uniform position on this proposal. Some CBA

---

18 CHAPTER 31 OF THE ACTS OF 2004 amended 2007, c. 10, s. 5; 2010, c. 12, s. 2; 2010, c. 68; 2011, c. 69; 2014, cc. 25, 55, 56

19 See OPC's report on its investigation into Statistics Canada: Invasive data initiatives should be redesigned with privacy in mind (December 9, 2019). Broader consultation may have assisted Statistics Canada in the development of its PIA.

Section members think an approach similar to the *ATIA Ac*t is appropriate and that the Privacy Commissioner's approval should be required. Other members note that, unlike requests under the *ATIA*, *Privacy Act* requests ordinarily pertain to the individual's own personal information. If individuals have appropriate rights to challenge a vexatious requester designation, these members believe that notifying the Privacy Commissioner is sufficient to address systemic issues with the application of the government institution's right.

As noted in the CBA Section's October 2019 submissions, while we cannot comment on the anticipated effectiveness of amending the *Privacy Act* to make compliance agreements available as a remedial and enforcement mechanism, we generally support this tool. Its effectiveness will depend on whether the Privacy Commissioner has other available enforcement tools to incentivize a government institution to enter into a compliance agreement to avoid an order or further investigation.

However, some CBA Section members caution there are a wide variety of government institutions with different roles in the development and implementation of government policy. Some government institutions, such as Crown Corporations, perform similar functions to those in the private sector and for which compliance agreements may be appropriate. Others, such as Employment and Social Development Canada have a policy development mandate. Compliance agreements reflect a particular Privacy Commissioner's interpretation of the law at a particular juncture (often untested by the courts) and may go beyond the black letter of the law. While the Department must follow the law, the incumbent Minister should not be fettered by compliance agreements binding a predecessor that may have been entered into it for a mix of reasons, including political convenience to avoid an ongoing public investigation.

The CBA Section supports enhancing the Privacy Commissioner's powers to include the ability to issue binding orders on matters governed by both the *Privacy Act* and *PIPEDA.* As stated in our September 2016 submission, we support having the same oversight and enforcement model apply to both the Privacy Commissioner and the Information Commissioner, given their related roles. With the passage of C-58,[20] the Information Commissioner has enhanced enforcement powers, including issuing binding orders to government institutions to take effect after 30 business days. A government institution that is subject to an order, and has serious concerns about it, can seek a review by the Federal Court within 30 days of receipt. We believe the Privacy Commissioner should have similar order making powers under the *Privacy Act* and

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

that similar consideration is taken with respect to the enforcement of *PIPEDA.* It is the view of some members of the CBA Section that enhancing the role of the Privacy Commissioner and his enforcement powers will contribute towards the Government's goals of ensuring respect for individual's rights and increasing accountability that is both meaningful and transparent.

However, the CBA Section is concerned about the organizational structure of the OPC. We are currently analyzing this issue to respond to Bill C-11 and when completed, will be able to share our comments. More particularly, we urge a formal separation of investigative and audit functions on the one hand and adjudicative functions on the other. Given the potential deference the Data Protection Tribunal will afford the OPC, the CBA Section believes that there must be strong procedural safeguards to ensure a fair hearing at the OPC. The CBA Section encourages the government to mandate a separation of investigative and adjudicative functions to avoid an apprehension of bias against organizations which may become more acute as the OPC's powers increase. Bifurcation would ensure the continuing confidence of all stakeholders in the results of investigations and adjudication.

XIII. CONCLUSION

In closing, the CBA Section commends Justice Canada in conducting a thoughtful review of the *Privacy Act* to develop a comprehensive and cogent Discussion Paper. We look forward to ongoing dialogue. If there is anything in our current or prior submissions on which you would like us to expand or clarify, we would be pleased to do so.