



BC FREEDOM OF INFORMATION
AND PRIVACY ASSOCIATION

20210214 PRIVACY ACT LAW REFORM SUBMISSION

Submitted By:

BC Freedom of Information and Privacy Association

fipa@fipa.bc.ca

Prepared By:

Matthew A. J. Levine, Barrister & Solicitor

February 14, 2021

File No. 21-2-06

David Lametti
Minister of Justice and Attorney General of Canada
Department of Justice Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8

By electronic submission

Re: A Public Consultation About the Future of the Privacy Act -- Privacy Obligations, Enforcement Mechanisms, and Transparency

I am writing on behalf of the BC Freedom of Information and Privacy Association ("BC FIPA") in response to your office's "A Public Consultation about the Future of the *Privacy Act*."¹

BC FIPA is a non-partisan, non-profit society that was established in 1991 for the purpose of advancing freedom of information, transparency, and privacy in British Columbia and Canada. We seek to empower all Canadians by increasing their access to information and their control over their own personal information.

As noted in "Respect, Accountability, Adaptability: A discussion paper on the modernization of the *Privacy Act*" ("Discussion Paper" or "*Respect, Accountability, Adaptability*"), reform of the *Privacy Act* is necessary to balance a range of policy

¹ Government of Canada, Department of Justice, "Modernizing Canada's Privacy Act – Online Public Consultation" <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.html>>.

objectives.² The importance of skillfully balancing these objectives and the underlying, quasi-constitutional rights to privacy over personal information entrenched in the *Privacy Act* comes in to especially clear focus vis-à-vis the increasing use of digital technologies by public bodies.³

FIPA has, in this regard, drawn attention to concerns about the use of private, cloud-based information technologies in public school classrooms.⁴ In light of disruptions caused by Covid-19 and related public health measures, privacy concerns associated with digital technologies are top of mind for not only an increasing number of students, parents, and educators but frankly almost all Canadians.⁵

2 Government of Canada, Department of Justice, "Respect, Accountability, Adaptability: A discussion paper on the modernization of the *Privacy Act*" ["Discussion Paper"] at 7 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

3 As stated in the Discussion Paper, the policy objectives are: protecting individuals' human dignity, personal autonomy, and self-determination; enhancing public trust and confidence in government; promoting the responsible use and sharing of data to advance government objectives in the public interest; promoting effective and accountable public governance; advancing reconciliation with Indigenous peoples in Canada by promoting improved data sharing with Indigenous governments and communities; and, supporting sound, ethical and evidence-based public sector decision making. See, Discussion Paper at 7 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>. We note that individual autonomy, dignity, and privacy are, in the words of the Supreme Court of Canada, "fundamental values that lie at the heart of a democracy." See, *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19. We return to this point in the conclusion.

4 Troubling Clouds: Gaps affecting privacy protection in British Columbia's K-12 education system. <https://fipa.bc.ca/wordpress/wp-content/uploads/2020/09/2020_troubling_clouds_LMS_report.pdf>.

5 The above statement is based on anecdotal evidence. However, in 2020 BC FIPA, after reviewing previous surveys, analyzing key legislation, and discussing with stakeholders, BC FIPA commissioned an IPSOS poll on BC citizens' opinion regarding BC's private sector privacy laws. The results indicated that 92% of respondents were at least somewhat concerned with the protection of their privacy. BC Freedom of Information and Privacy Association, "British Columbians want action on privacy protection: Polling results.", (June 3, 2020), <https://fipa.bc.ca/category/libraries/publications/publication-types/surveys-and-polling/> ("BC FIPA 2020 Survey")

The Discussion Paper provides an excellent basis for public consultation

We have reviewed the Discussion Paper with interest. It provides an excellent basis for meaningful public consultation.⁶ We address three of the specific proposals raised by the Discussion Paper:

- Proposal 5 regarding existing obligations;⁷
- Proposal 8 regarding accountability mechanisms;⁸ and
- Proposal 9 regarding transparency mechanisms.⁹

Our submission seeks to illustrate the mutual compatibility between these three proposals. It does so by considering the relevance of each proposal to a single risk reduction tool, i.e., privacy impact assessments (“PIAs” or “Privacy Impact Assessments”).

The Treasury Board Secretariat of Canada’s Interim Directive on Privacy Impact Assessment states that:

The Government of Canada is committed to ensuring that privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information.¹⁰

When used correctly, PIAs facilitate a process whereby government institutions can adaptatively learn to make risk identification and reduction a core consideration in the initial framing of their programs and activities.

6 FIPA does not necessarily agree with all of the proposals in the Discussion Paper. This Submission’s silence on any particular topic or issue raised in either the Discussion Paper or the Privacy Act should in no way be considered as an endorsement.

7 Discussion Paper at 10 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

8 Discussion Paper at 16 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

9 Discussion Paper at 17 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

10 Treasury Board Secretariat of Canada, Interim Directive on Privacy Impact Assessment at 3.1 <<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>>.

The responsibility for government institutions to pro-actively identify and reduce privacy risks flows naturally and directly from the individual, quasi-constitutional rights over personal information that are entrenched in the *Privacy Act*.¹¹

Reform of the *Privacy Act* offers an important opportunity for your office to guide and enable federal public bodies to effectively and efficiently utilize PIAs specifically and risk reduction tools generally. We are hopeful that the following will provide a useful basis for you and your office in formulating specific legislative reforms.

Discussion Paper 5: Obligations for federal public bodies should be updated and new ones introduced

In addition to quasi-constitutional rights to privacy over personal information, the *Privacy Act* articulates a range of privacy-related obligations for federal public bodies. The Discussion Paper notes several such obligations (collectively, “Existing Obligations”).¹² The Existing Obligations demonstrate that federal public bodies can be subjected to legal obligations pertaining to personal information. There is, however, a persistent concern that the Existing Obligations do not fully ensure the protection of privacy rights. In light of, *inter alia*, widespread use of digital technologies and the vastly greater amounts of personal information now held by government institutions, obligations under the *Act* should be updated and new obligations should be added.

The Discussion Paper in Proposal 5 does note certain new obligations, which are:

- A specific principle to protect personal information with appropriate technical, administrative and physical security safeguards

¹¹ On the quasi-constitutional status of privacy rights, see *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

¹² Discussion Paper at 10 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

- An obligation to contain personal information breaches and to subsequently notify the Privacy Commissioner and affected individuals in certain cases
- An obligation to retain information about any personal information breach (collectively, the “Mooted Obligations”)¹³

The Mooted Obligations are certainly welcome. In fact, the Mooted Obligations are in some ways more expansive than an obligation to conduct a Privacy Impact Assessment. However, the Mooted Obligations are not sufficient to meet the challenges created by the widespread use of digital technologies.

In this respect, it is interesting that *Respect, Accountability, Adaptability* in Proposal 8 states that:

The *Privacy Act* should require each federal public body to undertake an analysis to identify and mitigate privacy risks, commonly known as a privacy impact assessment (PIA).¹⁴

We agree.

Respect, Accountability, Adaptability at Proposal 8 furthermore states that

[t]his obligation would apply to new programs or activities or substantially modified existing programs that involve the collection, use or disclosure of personal information.¹⁵

¹³ Discussion Paper at 12 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

¹⁴ Discussion Paper at 17 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

¹⁵ Discussion Paper at 17 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

The Discussion Paper, therefore, explicitly proposes an “obligation” for public bodies to perform a Privacy Impact Assessment or PIA in appropriate circumstances. Again, we agree.

In fact, the Treasury Board Secretariat’s (TBS) interim Directive on Privacy Impact Assessment requires, as a matter of policy, that federal public bodies both conduct and submit a PIA in certain circumstances.¹⁶ It is laudable that this obligation has been recognized by the TBS; however, now is the time for this obligation to be entrenched in the *Privacy Act*.

In this respect, the OPC has recommended to Parliament that federal public bodies should be legally obligated to conduct PIAs for new or significantly amended programs involving personal information, i.e., in appropriate circumstances.¹⁷

In short, there is an effective consensus that Canada’s government institutions should be routinely conducting Privacy Impact Assessments. (We note that because a Privacy Impact Assessment is a process and the first phase in this process is risk identification, routine conduct of PIAs does not mean that the entire process will always be necessary.)

¹⁶ Treasury Board Secretariat of Canada, Interim Directive on Privacy Impact Assessment at 1.1 <<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>>.

¹⁷ Expectations: OPC’s Guide to the Privacy Impact Assessment Process” <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>. As mentioned in the same document, the OPC has also recommended that federal public bodies be obligated to submit their PIA reports to the OPC before implementing a covered program or activity. We return to this requirement regarding review by and submission to the OPC in the next section.

There is also growing recognition that the *Privacy Act* should contain an affirmative, legal obligation for public bodies, in appropriate circumstances, to conduct a Privacy Impact Assessment.

In our submission, the Privacy Act should also clearly and unambiguously require that this obligation to perform a PIA must also be fulfilled when the relevant program or activity is performed by a public body's service provider.

Discussion Paper 8: Specific accountability mechanisms should be added in the Act to help federal public bodies demonstrate how they are accountable for their personal information practices

The case study of PIAs also demonstrates that existing accountability mechanisms should be strengthened, and new accountability mechanisms should be added.

It is helpful to start with a general observation. As noted in the Discussion Paper, a truly 'modernized' *Privacy Act* will help federal public bodies to demonstrate accountability for their personal information practices and incentivize the development of organizational cultures that:

- enhance public trust and confidence in government;
- promote effective and accountable public governance; and,
- promote the responsible use and sharing of data to advance government objectives in the public interest.

In turn, increased use of Privacy Impact Assessments, especially when done at the appropriate time and in a transparent manner, will be complimentary to the development of the abovementioned organizational cultures and therefore the associated policy

objectives. In sum, there is a real opportunity to spark positive feedback effects, but in order to achieve those positive feedback effects there is a clear and present need for improved and additional accountability mechanisms.

The remainder of this section reviews the need for reform.

It is now widely accepted that public bodies should be performing Privacy Impact Assessments¹⁸; however, existing enforcement mechanisms are not fit for purpose. The current enforcement mechanisms are unfortunately confusing and weaker than desirable.

Existing enforcement mechanisms for the use of PIAs are confusing because they are based on policy, which is inherently subject to change. Indeed, as of March 13, 2020 the Treasury Board Secretariat of Canada's ("TBS") issued an Interim Directive on Privacy Impact Assessments ("TBS Interim Directive").¹⁹ The TBS Interim Directive replaced the TBS's Directive on Privacy Impact Assessment dated April 1, 2010.²⁰ It is effective from March 13, 2020 to March 31, 2021.²¹

The OPC has acknowledged that reliance on the TBS is less than ideal and has, therefore, issued a document addressed to federal public bodies titled "Expectations: OPC's Guide to the Privacy Impact Assessment Process" ("*Expectations*").²² *Expectations* reviews not

¹⁸ As reviewed in the proceeding section of this Submission.

¹⁹ Treasury Board Secretariat of Canada, Interim Directive on Privacy Impact Assessment at 1.1 <<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>>.

²⁰ Treasury Board Secretariat of Canada, Interim Directive on Privacy Impact Assessment at 1.2 <<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>>.

²¹ Treasury Board Secretariat of Canada, Interim Directive on Privacy Impact Assessment at 1.1 <<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>>.

²² *Expectations: OPC's Guide to the Privacy Impact Assessment Process* <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.

only when a Privacy Impact Assessment is required or recommended but also the correct use thereof. It is a source of concern that the correct use of Privacy Impact Assessments apparently remains unclear to federal public bodies.

Furthermore, the existing enforcement mechanisms for PIAs are also weaker than desirable because they are based on policy rather than law. This conclusion applies both in circumstances where the program or activity is covered by the TBS's Interim Directive as well as circumstances where the program or activity is not covered by the TBS's Interim Directive. Of particular concern, where a program or activity is not covered by the TBS, the strongest existing enforcement mechanism is the discretionary decision by the head of a federal public body to submit a PIA for review by the OPC and the subsequent review by the OPC. A discretionary review process cannot be classified as anything other than a weak enforcement mechanism.

There is therefore a need for reform in terms of both the improvement of existing enforcement mechanisms and legislation of additional, specific enforcement mechanisms. Indeed, the OPC has recommended to Parliament that the *Privacy Act* be amended to: require federal public bodies to submit PIA reports to the OPC; and, require that submission be made prior to implementing a covered program or activity.²³

The OPC has developed important expertise in reviewing PIAs, which is leveraged through its review and commentary on those PIAs that are submitted. This enforcement mechanism should be continued and strengthened. Furthermore, as the OPC has already recommended to Parliament, its review should be made mandatory.

23 Expectations: OPC's Guide to the Privacy Impact Assessment Process" <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.

Additional enforcement mechanisms should also be entrenched in the *Privacy Act* so as to encourage federal public bodies to make correct use of PIAs and demonstrate that they are accountable for their personal information practices. (In the following section, we review a transparency-based mechanism.)

It is helpful to consider certain legislative reforms introduced in the Government of Canada's proposed consumer privacy legislation for the private sector, i.e., Bill C-11.

We note that Bill C-11, if passed, would require private sector organizations to not only designate an accountable person but also create and maintain a Privacy Management Program ("PMP"). A PMP may be understood, per the Discussion Paper, as:

an organizational plan for protecting personal information that a government public body can use to identify, organize, review and improve its practices relating to personal information. It would serve as an individualized guide for compliance with the Act. 24

The Discussion Paper states that the *Privacy Act* could identify the minimal requirements for public bodies PMPs. We agree.

One of the minimal requirements in public bodies' PMPs should, *inter alia*, be the obligation to perform Privacy Impact Assessments. This enforcement mechanism could be supplemented by supporting regulations or policy.

At the current point in time, we have yet to see any reason why PMPs should be mandatory for the private sector but not for the public sector. Rather, this enforcement

24 Discussion Paper at 17 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>>.

mechanism and its associated requirements regarding PIAs would be complimentary to the policy objectives of developing organizational culture within federal public bodies that:

- enhance public trust and confidence in government;
- promote effective and accountable public governance; and,
- promote the responsible use and sharing of data to advance government objectives in the public interest.

In sum, the case study of PIAs demonstrates how existing accountability mechanisms should be strengthened and new accountability mechanisms should be added to the *Privacy Act*.

Discussion Paper 9: Specific transparency mechanisms should be added to the Act for federal public bodies to provide readily available explanations of their personal information protection practices

A truly 'modernized' *Privacy Act* should include specific transparency mechanisms so that federal public bodies can provide readily available explanations of their personal information protection practices. This principle is, in fact, also, complimentary to the correct use of Privacy Impact Assessments.

The following paragraphs review the relationship between specific transparency mechanisms, i.e., publication and summarization, and Privacy Impact Assessments.

It is appropriate that the *Privacy Act* require each federal public body to publish its PIAs. In order to ensure that published PIAs are accessible to the public, federal public bodies should seek to include summaries. This specific transparency mechanism may be subject

to exceptions in specific, limited circumstances as deemed necessary either in the Act or by regulation.

In January of this year, the federal Information Commissioner published *Observations and Recommendations from the Information Commissioner on the Government of Canada's Review of the Access to Information Regime* ("Information Commissioner's Report" or "Report").²⁵ The Information Commissioner's Report highlights a number of serious concerns.²⁶ In particular, the Report identifies inappropriate reliance on S. 69 of the *Access to Information Act*²⁷ to unreasonably exclude and prejudicially restrict public access to documents involving consideration of operational issues, such as Privacy Impact Assessments. Through our own work in British Columbia, we have observed a similar increase in ill-founded attempts to prevent Privacy Impact Assessments from being made public.

It is certainly possible that that either the *Access to Information Act* will be reformed or the inappropriate reliance on S. 69 thereof will be addressed through some other means. In the case of Privacy Impact Assessments, a more direct solution is available. Simply put, federal public bodies should be required to publish their PIAs.²⁸

25 Office of the Information Commissioner of Canada, *Observations and Recommendations from the Information Commissioner on the Government of Canada's Review of the Access to Information Regime* <https://www.oic-ci.gc.ca/sites/default/files/2021-01/Review_of_the_Government_of_Canada's_Access_to_Information_Regime_Observations_and_Recommendations_from_the_Information_Commissioner-ENG.pdf>.

26 A useful review of these concerns is contained in Vincent Gogolek, "Close the Loophole Shielding Cabinet Documents from Access to Information Requests" (Feb 04, 2021) Policy Options <<https://policyoptions.irpp.org/magazines/february-2021/close-the-loophole-shielding-cabinet-documents-from-access-to-information-requests>>.

27 *Access to Information Act* (R.S.C., 1985, c. A-1).

28 Here we use the term PIA inclusively to include the PIA report. We understand that there may be legitimate reasons for certain PIA-adjacent deliberations not to be published, but the PIA itself is fundamentally an operational document.

In addition to the above and in light of concerns amongst Canadians about the proliferation of digital technologies, it is important to consider albeit briefly the relationship between PIAs and certain digital technologies. In this respect, one particular type of digital technology is especially relevant, i.e. so-called “Artificial Intelligence” or “AI”. A core input in to AI is predictive analytics with predictive analytics understood to be the use of data, statistical algorithms and machine learning to identify the likelihood of future outcomes based on massive volumes of data.²⁹ Predictive analytics can be used in advertising but it is also being used in many other domains. An AI-empowered system may, at times, also be referred to as an automated decision-making system. In this respect, Canadian privacy commissioners have found on several occasions that there are serious questions about whether the current framework for privacy laws is adequate for addressing the challenges posed by AI. For instance, in 2017 the Information and Privacy Commissioner of Ontario observed that: “To allow for big data-type practices in general, a new or modified legislative framework is needed.”³⁰ In 2020, the federal Privacy Commissioner stated that:

Based on our own assessment, AI (artificial intelligence) presents fundamental challenges to all foundational privacy principles as formulated in PIPEDA (*Personal Information Protection and Electronic Documents Act*). For instance, the data protection principle of limiting collection may be incompatible with the basic functionality of AI (artificial intelligence) systems.³¹

²⁹ Ajay Agrawal, Joshua Gans, & Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence*, (Harvard Business Press, 2018). It entails a system that is closely related to but distinguishable from data mining, as data mining merely generates inferences from retrospective pattern analysis. Predictive analytics provides an assessment of what will happen in the future based on data about past activities that is both sufficiently accurate and inexpensive with the result that can efficiently replace human prediction.

³⁰ Office of the Information and Privacy Commissioner of Ontario, *Big Data Guidelines* May 2017, <<https://www.ipc.on.ca/wp-content/uploads/2017/05/bigdata-guidelines.pdf>>.

³¹ Office of the Privacy Commissioner of Canada, Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence, January 2020

The above statements may be collectively referred to as the “Commissioner Statements on AI”. We do not disagree with the Commissioner Statements on AI.

The basic principle articulated in the Commissioner Statements on AI is that AI is a major challenge that may require re-thinking the fundamental structures of Canadian privacy law. A fundamental re-structuring of privacy laws applicable to federal public bodies may ultimately be necessary. In the meantime, however, there is a need to take prompt action to identify and reduce risk, which has been the guiding spirit behind our Submission. The following paragraph touches on two references to AI in the Discussion Paper that illustrate how use of AI-empowered systems by public bodies may intersect with an increased use of PIAs.

The Discussion Paper states that:

Certain rights relating to enhanced public awareness of interactions with automated decision-making systems (such as artificial intelligence tools): Aligning *Privacy Act* transparency and accountability requirements with leading federal public sector policy instruments guiding the use of automated decision-making systems could help ensure that individuals know when they are interacting with *automated decision-making systems*, what types and sources of personal information these systems use, and general information on how these systems function.³² (Italics added.)

The Discussion Paper also states that

The Act could be amended to broaden the scope of administrative purpose to capture any practice involving personal information that could directly affect the individual, whether or not a decision-making process was involved. This would ensure that the full suite of protections in the Act applied to the design

<https://priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/?wbdisable=true>.

³² Discussion Paper at 12 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>.

and development of *artificial intelligence systems*, for example.³³ (Italics added.)

The above passages may be referred to as the “First Passage on AI”, the “Second Passage on AI”, and collectively the “Discussion Paper Passages on AI”

For current purposes, our comments are as follows. First, the Discussion Paper Passages on AI appear to use the terms “automated decision-making systems” and “artificial intelligence systems” interchangeably. This is understandable and reflects the changing vocabulary of our everyday language. However, as noted by the Privacy Commissioner’s 2020 consultation on artificial intelligence there may be a need for legal definition of these terms.³⁴ You and your office are well positioned in terms of both expertise and resources to address this concern.

Second, although we have indicated above that PIAs should be a primary obligation – rather than, for example, a ‘transparency requirement’ or ‘accountability requirement’, in the language of the First Passage on AI – we are in agreement with the First Passage on AI that: the public should be made aware when AI is being used in the provision of government services; there should be alignment between obligations, enforcement mechanisms, and government transparency; and, where a recently-enacted policy instrument has specifically identified a risk or risks associated with the use of “artificial intelligence systems” that risk should be considered during the PIA process. For the avoidance of doubt, the formulation of a relatively more permissive approach to a risk associated with artificial intelligence systems should not be used to ‘water down’ the PIA process.

³³ Discussion Paper at 10 <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf>.

³⁴ Office of the Privacy Commissioner of Canada, Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence, January 2020 <https://priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/?wbdisable=true>.

Third, the Second Passage on AI suggests amending the scope of the term administrative purpose so as to capture any practice involving personal information that could directly affect the individual, whether or not a decision-making process was involved. We are in agreement.

Cost of Compliance with Obligation to Prepare Privacy Impact Assessments

Our submission calls for increased use of Privacy Impact Assessments as a risk reduction tool. If the *Privacy Act* is amended to realize the reforms described above, federal public bodies will likely need to invest more resources in the preparation of PIAs and compliance with the Act.

In addition to simply undertaking PIAs, such an investment may include hiring and/or training staff, acquiring privacy-protective technologies, and developing privacy-compliant operational practices. While these initiatives may seem quite burdensome, the costs associated with non-compliance are far more onerous.

Costs associated with non-compliance include: operational disruption, productivity loss, loss of public trust and confidence, diminution of effective and accountable public governance; and, reduced capacity to promote the use and sharing of data to advance government objectives in the public interest. For example, a study done in the United States by Ponemon Institute indicates that the total costs of non-compliance with privacy legislation are nearly three times higher than the costs of compliance.³⁵ Therefore, while

35 Ponemon Institute LLC, "Whitepaper: The True Cost of Compliance with Data Protection Regulations", (December 2017), <<http://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf>>.

risk reduction and compliance require an initial investment of resources, organizations who make this upfront investment are better positioned over the medium and long term.

Conclusion

For the reasons mentioned above, the *Privacy Act* must create an obligation for federal public bodies to conduct Privacy Impact Assessments. Moreover, existing accountability mechanisms relating to PIAs must be strengthened and new accountability mechanisms must be added. Finally, a truly 'modernized' *Privacy Act* must include specific transparency mechanisms relating to PIAs.

When used correctly, PIAs provide an effective and efficient tool that federal public bodies should use to

- enhance public trust and confidence in government;
- promote effective and accountable public governance; and,
- promote the responsible use and sharing of data to advance government objectives in the public interest.

It may be trite to say that government institutions collect and use much more personal information today than when the *Privacy Act* became law in 1983. However, it underscores the key point that it is no longer tenable for risk reduction tools to be used only after a problem comes to light. Instead, these tools, such as PIAs must be used proactively.

It is instructive to note the words of the Office of the Privacy Commissioner of Canada ("OPC") who wrote in 2020 that:

PIAs are an early warning system, allowing institutions to identify and mitigate risks as early and as completely as possible. They are a key tool for decision-makers, enabling them to deal with issues internally and proactively rather than waiting for complaints, external intervention or bad press.

An effective PIA can help build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices.

A PIA report documents the PIA process. The real value comes from the analysis that occurs as part of the process of working through the PIA questions.³⁶

We concur.

In turn, the Supreme Court of Canada has affirmed that:

... individual autonomy, dignity and privacy [...] are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society.³⁷

As a direct result, reform of the *Privacy Act* so as to fully safeguard the underlying privacy rights of individuals over their personal information is much more than a desirable policy objective, it is a necessity.

36 Office of the Privacy Commissioner of Canada, *Expectations: OPC's Guide to the Privacy Impact Assessment Process* (2020), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.

37 *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19.

Accordingly, this public consultation offers an important opportunity to begin the law reform process within government and, in due course, introduce legislative reforms

We hope that these comments will form a useful part of your public consultation as well as that reform process.