Department of Justice Canada
Ministère de la Justice Canada

Modernizing Canada's *Privacy Act*: What We Heard Report

Justice Canada's Preliminary Technical Engagement on *Privacy Act* Modernization

Summer and Fall 2019

Canada

Cat. No. J2-494/2020E-PDF
ISBN 978-0-660-34470-6

Contents

INTRODUCTION

About the *Privacy Act* Modernization Initiative

Our world has changed dramatically since the *Privacy Act* came into force in 1983. After more than 35 years of technological advances and social change, Canadians' expectations of how federal institutions collect, use, share and store their personal information have evolved. Given these societal and technological shifts, Justice Canada is currently undertaking a review of the *Privacy Act*, the federal public sector privacy legislation focused on the protection of personal information held by federal government institutions.

As part of its commitment to modernizing the *Privacy Act*, Justice Canada launched a preliminary targeted technical engagement with experts – a preliminary step to an eventual broader public consultation process. In June 2019, Justice Canada engaged privacy, data and digital, and government stakeholders in an initial discussion on a number of technical and legal considerations to modernizing the *Privacy Act*.

The preliminary engagement had three main objectives, with a view to informing the review of the *Privacy Act* where appropriate:

1. To confirm with privacy, digital and data experts key legal policy considerations the Government should be taking into account in modernizing the *Privacy Act;*
2. To seek the views of a range of Government of Canada departments and agencies*;* and
3. To seek views from experts on legal and policy considerations touching on the *Privacy Act* that have a particular impact on Indigenous Peoples.

Format of the Preliminary Technical Engagement

Given the preliminary and targeted nature of this engagement, Justice Canada sought to generate a focussed discussion on the modernization of the *Privacy Act* with stakeholders with a specialized expertise in privacy, technology and digital issues. Justice Canada prepared five discussion papers as a launch pad for the engagement (See Appendix A). The discussion papers set out commentary and questions about the underlying challenges and opportunities that arise out of modernizing the *Privacy Act,* and were posted on Justice Canada's *Privacy Act* modernization webpage (available at https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/index.html).

The discussion papers were also provided to academics, Indigenous groups, legal experts, industry experts and international data protection experts, based on their demonstrable interest and expertise in privacy and digital issues. Some recipients had appeared before the

ETHI Committee during its 2016 study on *Privacy Act* review and its 2019 study on Privacy and Digital Government Services. Stakeholders were encouraged to share the discussion papers with other experts within their respective networks, to reach the broadest network of relevant experts as possible. Stakeholders were asked to provide written comments in response to the issues raised in the discussions papers by the fall of 2019.

HIGHLIGHTS

Justice Canada received submissions from a number of stakeholders, including from the Office of the Privacy Commissioner of Canada (OPC), the Office of the Information Commissioner of Canada (OIC), the Canadian Bar Association (CBA), various Government of Canada departments and agencies, Indigenous organizations with expertise in data governance and claims research, and international experts. Given the breadth of stakeholders and their unique perspectives, the comments received were wide ranging. However, a few themes and common points emerged throughout – these are highlighted below.

Embracing a Principles-Based Approach

There was broad support for adding privacy principles to the *Privacy Act.* Principles were seen as a way to provide greater flexibility in light of evolving technology and the fact that the mandates of Government of Canada departments and agencies sometimes change. Many respondents, including government institutions, generally agreed that the inclusion of principles in the Act could encourage more innovative uses of personal information for public good, while ensuring the responsible management and treatment of personal information. One key observation was that the Act should focus on baseline principles relating to the treatment of personal information, including the collection, use and disclosure of personal information, as opposed to articulating mechanisms specifying how institutions could achieve a certain outcome. In particular, the OPC noted that consideration should be given to incorporating principles without creating interpretation challenges, such as those encountered under Canada's federal sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The OIC did not comment on the general utility of adopting privacy principles, but suggested that introducing two specific balancing tests could be more beneficial than over-arching privacy principles – an unjustified invasion of privacy test to guide the disclosure of personal information that may not always warrant protection from disclosure and a compassionate disclosure test to guide the disclosure of personal information about a deceased person to a spouse or close relative where a broader public interest in disclosure cannot be identified.

Identifying Specific Principles

Many comments centered on what specific principles might be enshrined in a modern *Privacy Act.* The OPC was of the view that the Act should generally balance the privacy rights of

individuals with the government's requirements for collecting, using and disclosing personal information. Specifically, the OPC favoured an approach that would ensure that the processing of personal information by government institutions is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals. Other respondents, including some government institutions, agreed with including a principle that would allow government institutions to carry out activities involving personal information "for the public good". The OIC noted that any proactive disclosure obligations in support of a new principle oriented around openness and transparency must not be at the expense of Canadians' right of access under the *Access to Information Act*.

Supporting Flexible Practices and Innovation

Government institutions also generally noted that more flexibility in the manner they can respect the rules under the Act would better allow the government to unlock the potential of the data it holds. Government institutions noted the growing public importance of delivering improved and modern services to Canadians, including policy analysis, research and evaluation. They noted that these uses should be specifically recognized and enabled in a modernized *Privacy Act,* along with appropriate checks and balances, and greater individual greater control over their personal information.

Many government institutions also supported including a "reasonableness and proportionality" principle that would govern all collections, uses and disclosures of personal information. Some recognized that that a "reasonableness and proportionality" principle might not meet the more internationally recognized privacy standard of "necessity and proportionality", and could also raise the risk of overreach in certain program areas. For this reason, mandatory transparency mechanisms would be needed to empower the public to know how their information is being used and by whom.

The main general takeaway from responses was that further thought would have to be given to exactly what principles are identified in the Act, and how such principles would interact with other provisions in the Act.

Future-Proofing the Act

Another recurrent theme was the importance of future-proofing the Act, in light of the speed at which technology evolves. Many underscored how the Act should remain technologically neutral, and avoid including overly prescriptive mentions of specific types of technology. In particular, the OPC was of the view that the Act should include high-level, technology neutral principles that provide flexibility to institutions in responding to emerging privacy issues. According to the OPC, such principles would have to be accompanied by a foundation of

privacy rights for individuals, enhanced rules for government institutions, and stronger enforcement mechanisms for the Privacy Commissioner.

Privacy Protections that Respect Canadians' Service Expectations

Many government institutions, as well as the CBA, noted the growing need for federal institutions to adapt to meet Canadians' evolving expectations to receive government services in a more efficient and user-friendly manner. Some government institutions referenced an increasing frustration among Canadians about the need to disclose the same information to several departments or agencies, whether at the federal, provincial or territorial level, and shared the view that a modernized Act should take into account not only the privacy expectations of Canadians, but also their expectations as to how they would like to receive government services.

Enshrining Updated and New Rules

Another key theme was adding specific obligations in the *Privacy Act* to better align it with other personal data protection legislation in Canada and elsewhere. There was an overall consensus that the *Privacy Act* should impose a number of updated requirements on federal institutions, including: (i) requiring institutions to identify the purposes for which personal information is collected; (ii) setting out a necessity standard for the collection of personal information; (iii) adding a technology neutral obligation to safeguard personal information; (iv) adding a requirement to include privacy-related considerations when designing government programs and activities; and (v) adding a requirement to notify individuals and the OPC of data breaches in certain cases.

Updating the Threshold for Collecting Personal Information

Some stakeholders remarked that the collection threshold under the Act should be linked to the underlying mandate and functions of a government institution, as opposed to programs and activities. The OPC was of the view that the collection of personal information by government institutions should be governed by a necessity and proportionality standard. Although some government institutions recognized that there appeared to be an emerging international consensus that collections of personal information should be demonstrably necessary, many were of the view that Canada should be careful not to create new barriers for institutions to use of data effectively. Others noted that aligning the collection threshold with more internationally recognized standard of necessity might be overly restrictive and could cause unintended effects on government operations.

Privacy Breaches

Government institutions generally agreed that while they should be transparent and accountable for privacy breaches, the applicable threshold for reporting breaches would have to be properly defined, and federal institutions would have to be supported through policy and directives in understanding the types of privacy breaches and how to respond.

Updating the Rules around the Retention of Personal Information

With respect to the retention of personal information, the OPC recommended that the Act require personal information to be retained only so long as it remains directly related to and demonstrably necessary to fulfill the purpose for which it was collected, while also allowing an individual a reasonable amount of time to access that information in order to understand, and possibly challenge, the basis for a decision. However, one government consideration raised was that the rules relating to the retention of personal information should be modified to allow for the immediate destruction of information that could potentially be harmful to national security where no longer required.

Other Concepts

Finally, some government institutions noted that certain privacy protection concepts may be more appropriate for the private-sector, such as the notion of consent or rights such as the "right to be forgotten". Others noted that there should also be support and guidance for institutions regarding data analytics and the use of artificial intelligence mechanisms that implicate the collection, use or disclosure of personal information.

Clarifying Concepts

Defining "Personal Information"

Some, including the OPC and the CBA, were of the view that the definition of "personal information" should be changed to include personal information that is not "recorded", such as live video footage. Additionally, the OPC and the OIC agreed that the Act should include a definition of "identifiability" as delineated by the Federal Court in *Gordon v. Canada (Health),*[1] with the OIC indicating that the test set out in *Gordon v. Canada (Health)* (i.e. information will be about an identifiable individual where there is a serious possibility that the information, alone or in combination with other available information, can identify an individual) is not workable in all contexts and scenarios. However, some government institutions noted that a broader definition of personal information could have profound effects on national security and law enforcement activities.

[1] *Gordon v. Canada (Health),* 2008 FC 258.

Defining Metadata

While some suggested defining metadata in the Act, others raised concerns about including a broad definition of metadata in the Act, since a large proportion of metadata relates largely to the technical operational of telecommunications, which was not necessarily seen by these stakeholders as being personal information. The OPC and the CBA were of the view that the Act should not include a specific statutory definition of metadata, and that any privacy issues related to metadata could instead be addressed through an updated definition of personal information.

Consent in the Public Sector Context

Many respondents provided submissions on the role and meaning of consent under the *Privacy Act.* While some saw a need to strengthen consent as a basis for whether federal institutions can use or share personal information, others, including international experts, saw consent as typically being an inadequate or inappropriate foundation for processing personal information in the public sector context. Some government institutions and the CBA suggested that consent should be defined as it is in other jurisdictions. For example, the European Union's *General Data Protection Regulation* ("GDPR"), a regulation on data protection and privacy in the European Union that came into force in May 2019, defines "consent" to mean "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".

The OPC acknowledged that consent presents challenges and impracticalities in the federal government context. The OPC also expressed the view that a necessity and proportionality obligation in the Act, and other changes to strengthen the Act (e.g. enhancing transparency, clearer presentation of choices where available, strengthened enforcement and reporting powers for the OPC), would address the absence of consent for most citizens receiving government services.

Some stakeholders familiar with the experiences of Indigenous Peoples also raised the view that consent should be "free, prior and informed", such that any consent provided for uses or disclosures of information for secondary or unknown purposes may not be meaningful.

Publicly Available Personal Information

A number of stakeholders provided comments on whether "publicly available personal information" should be defined in the *Privacy Act.* The OPC was of the view that the Act should include a definition of "publicly available personal information" which considers context, the reasonable expectation of privacy, accessibility of information, including with new technologies, and the collecting organizations' obligations for accuracy, currency and

completeness. The OIC and a number of government institutions were of the view that a definition of "publicly available" should balance the protection of privacy with the right to access government records. Some government institutions and the CBA identified a number of relevant considerations that should inform a modern framework under the Act touching on publically available personal information. These include whether it is appropriate for a particular institution to collect publicly available personal information in light of their mandate, how the information at issue was made public, and the appropriate transparency mechanisms needed where an institution collects, uses or discloses publicly available personal information.

Other government institutions made the comment that recent amendments to the *Canadian Security Intelligence Service Act* and the *Communications Security Establishment Act* that deal with publicly available information could be useful comparators, and that some institutions require the use of open source data for investigative purposes. Some stakeholders were of the view that disclosures of personal information should be allowed in the public interest where it is public and where there is no "reasonable expectation of privacy" in the information.

Clarifying "Consistent Uses"

Some government institutions, Indigenous stakeholders and the CBA suggested clarifying what a "consistent use" entails. The OPC was of the view that the Act should be amended to include a definition of "consistent use" which requires a reasonable and direct connection between the original purpose of collection and the proposed use, and that takes into account reasonable expectations. Some government institutions made the point, however, that consistent uses would be better defined in policy as opposed to in the Act.

Distinguishing Between Administrative and Non-Administrative Purposes

The OPC and the CBA were of the view that the Act should no longer distinguish between administrative and non-administrative uses of personal information, given increasing risks to privacy posed by non-administrative uses in the digital age. For example, the OPC identified non-administrative uses like research, statistical, audit and evaluation purposes as increasingly posing risks to privacy in a digital age, highlighting the use of personal information in profiling and targeting activities that can lead to discrimination, exclusion, and marginalization as of particular concern. Some government institutions and Indigenous stakeholders also suggested eliminating the concept of administrative purpose from the Act, agreeing that a specific decision impacting a particular individual may no longer be the best measure of when the full suite of legal protections under the Act should apply in light of new technologies that can pose risks to individuals but may fall outside the current definition.

Strengthening Accountability and Transparency

One of the main themes raised in the submissions received was the need to strengthen the Act's accountability and transparency mechanisms. While there was general support for incorporating strong accountability and transparency mechanisms in the Act, the CBA observed that accountability and transparency should not be left to general principles alone, and that there should be baseline requirements set out in the Act.

Privacy Management Programs and Privacy Impact Assessments

The OPC, as well as many government institutions and data protection experts, were of the view that privacy management programs (PMPs) should be formally required of government institutions. However, many agreed that the details of what should be included in a PMP should be left to policy and guidance. This would allow the institution to choose from a possible suite of recommended tools that best suited the context, the institution's mandate and structure, and its operating environment.

Many respondents also agreed that institutions should be formally mandated to conduct Privacy Impact Assessments (PIAs) for new or substantially modified programs or activities that involve personal information. The OPC added that PIAs should focus on the impact a program has on privacy rights, and that the Act should (i) specify when PIAs should be conducted and the timelines for doing so; (ii) require that PIAs be submitted to the OPC; (iii) require institutions to inform the OPC of measures to mitigate identified risks; and (iv) allow the OPC to publish a list of all PIAs it receives.

Some saw a greater role for the OPC with respect to PIAs, commenting that the OPC should review and comment on draft PIAs, but only to provide views on potential compliance issues and not specific instructions on how to achieve compliance with the Act. These submissions tended to emphasize government institutions' need to maintain discretion around how to achieve privacy compliance in a way that was sensitive to broader operational complexities and policy considerations. Government institutions suggested that, to fully realize the potential of the PIA process, the scope of a PIA should be expanded from a limited "program or activity" assessment perspective to one that considers the lifecycle of institutional engagement with and administration of personal information and the effects on privacy rights.

However, some government institutions noted that it could be time consuming and burdensome for institutions to be subject to a mandatory requirement to undertake PIAs, with some suggesting that a mandatory PIA legal requirement could be disproportionate for less sensitive personal information or less privacy-intrusive activities. Accordingly, the threshold for triggering the requirement to undertake a PIA should be unambiguous and

targeted to situations where a comprehensive review of personal information management practices is warranted.

Information-Sharing Agreements

For many government institutions, transparency could be promoted by including rules in the Act requiring information sharing agreements (ISAs) amongst partners, internal and external to the institution, and requiring privacy statements describing an institution's intended uses of personal information at the point of collection. The OPC specifically recommended amending the Act to require: (i) that regular sharing of personal information as a "consistent use" be subject to ISAs; (ii) that the sharing of personal information with other domestic or foreign governments be done pursuant to a written ISA; (iii) institutions to develop written ISAs and notify the OPC of new or amended ISAs; and (iv) the publication of ISAs. The OPC also recommended strengthening the reporting requirements on privacy issues and specific transparency requirements for lawful access requests made by agencies involved in law enforcement.

Some government institutions suggested that domestic and international ISAs should be treated differently because some may be impacted by other international legal considerations, such as treaties or trade agreements; the negotiation of international ISAs can be complex; international ISAs may regulate particularly sensitive information exchanges; and the nature of the legal authority conferred under an ISA may vary, depending on the jurisdictions involved. Most government institutions agreed that transparency of ISAs needs to be carefully considered and that a standardized approach to the full range of ISAs across government may not be feasible.

Proactive Disclosure of Certain Information

Certain stakeholders advocated for incorporating a requirement to provide proactive and accessible disclosures about information-sharing practices to individuals, to conduct internal reviews and audits, and to publish the results. Others commented that federal institutions should clearly communicate how individuals can exercise their privacy rights in a timely and accessible manner.

The Right to Access One's Own Personal Information

Under the *Privacy Act*, individuals who are not Canadian citizens or permanent residents, or who are not physically present in Canada, are not able to access their personal information that is under the control of a federal government institution. Some respondents addressed whether the right to access one's personal information should be broadened to these individuals. The OPC recommended that the Act be amended to include enforceable rights for

any individual whose personal information is under the control of a Canadian federal government institution to request and receive access to it, and to correct the information.

Many government institutions provided views on expanding the right of access under the Act. Some noted the potential operational impact that may result from expanding the right of access, while also recognizing that certain administrative changes could be considered to address impacts, including potential delays. Some noted that certain information about how and why information is treated and protected could also be proactively offered to an individual requesting access to their personal information in order to provide greater context to a response.

The need for a "decline to act" provision in the *Privacy Act* was also noted, such that institutions could seek the Privacy Commissioner's approval to decline to process access requests that are made in bad faith or vexatious, similar to the power recently granted to the Information Commissioner of Canada.

A Focus on Proactive Compliance...

The OPC is seen as a center of expertise on matters relating to privacy and personal information management. Some felt that proactive advice or advance rulings would be more effective in achieving the objectives of the Act, as opposed to waiting for notices of non-compliance from the OPC. Others were of the view that the OPC's expertise would be useful during the design phase of a new program or activity, when a PIA would be prepared, where the OPC could provide valuable advice on privacy implications before a program is launched, particularly when new technologies or more sensitive personal information is at issue.

Many government institutions, the CBA, and international experts supported providing the OPC with additional tools to guide the public, and federal institutions, on privacy issues relating to the federal public sector. The OPC recommended amending the Act to grant it a clear mandate to conduct research, education and outreach, including funding external research. A number of respondents were also of this view.

The OPC made other recommendations aimed at promoting compliance with the Act, and was open to exploring new avenues for proactively engaging with government institutions. For example, the OPC recommended explicitly enshrining the OPC's mediation role in the Act, as doing so would serve as an incentive for federal institutions to resolve complaints more quickly. The OPC was also open to having the power to issue advance rulings, as long as the OPC had the discretion to decide which circumstances required such rulings as a way to ensure the strategic use of resources and that the accountability for decisions relating to personal information rested with government institutions.

... But Stronger Enforcement Powers Where Required

The OPC recommended a number of changes to the Act to provide the Privacy Commissioner with greater enforcement tools. The OPC recommended moving away from the current model where the Privacy Commissioner provides recommendations to a model that would include the ability for the Privacy Commissioner to issue binding orders with respect to all obligations under the Act, and provide judicial recourse for individuals to challenge non-compliance with the Act. The OPC also recommended amending the Act to give it the power to enter into compliance agreements with institutions when there are reasonable grounds to suspect a contravention of the Act, with such agreements being enforceable in Federal Court. Many government institutions were open to giving the OPC the power to issue certain specified types of orders after an investigation, with some arguing that the complaint mechanism under the *Privacy Act* is currently ineffective and can lead to delays.

Government institutions also indicated that procedural fairness would require a clear separation between the different sections of the OPC charged with administering order-making powers, and providing guidance and proactive advice to institutions. Others, including the CBA, noted that if the OPC were granted order-making powers, the current model would need to be turned into an adjudicative model, requiring additional formality and procedural rights for parties, and that all orders should be subject to further independent scrutiny and evaluation through a review or appeals process.

Addressing the Needs of Indigenous Groups

Some respondents provided focussed insights relating to the interests of Indigenous Peoples, and how they could be impacted by the modernization of the Act. They noted concerns with the definition of "aboriginal government" under the Act, as it excludes many Indigenous collectivities. They argued that this violates the United Nations Declaration on the Rights of Indigenous Peoples. The OIC also noted that the current definition of "aboriginal government" excludes Indigenous Nations operating under other forms of traditional governance. The CBA agreed and noted a similar need to update the definition of "Indian band" to introduce new flexibilities that would allow the Act to remain current with recent and future treaties. As well, paragraph 8(2)(k) of the Act is not seen as reflective of current needs, as First Nations occasionally need to access their own information held by Canada for reasons other than to research or validate claims.

One theme that surfaced was that under the current access to information and privacy regime, Indigenous Peoples regularly face significant barriers in obtaining complete and timely access to records, and that given the importance of section 8(2)(k) in the resolution of historical grievances against the Crown, there should not be any amendments to the Act which might undermine or restrict the effectiveness of this provision. Other comments include that First Nations communities have an interest in personal information regardless of

whether it is in aggregate or de-identified form, and that First Nations recognize community privacy as a concept (whereas the *Privacy Act* focusses on the protection of individual privacy).

KEY OPPORTUNITIES AND CHALLENGES GOING FORWARD

Allowing Innovative, but Responsible, Uses of Personal Information for Public Good

According to many stakeholders, a modern *Privacy Act* will need to incorporate principles and requirements that protect individual privacy, while also allowing for reasonable and responsible uses of personal information for public benefit. One issue the Government will need to further consider is the appropriate accountability, transparency and oversight framework for such greater flexibility in the use and sharing of personal information.

Interoperability With Other Regimes

The Act cannot be modernized in a vacuum. In a world of increasingly important and valuable data flows, modern data protection laws should aim to ensure a certain measure of interoperability with other regimes, whether domestically or internationally. Some were of the view that the *Privacy Act* should be interoperable with not only PIPEDA, but with other Canadian provincial privacy regimes and other international examples such as the GDPR. As the *Privacy Act* modernization initiative progresses, the Government will need to consider how to reflect internationally recognized data protection principles in the Act, and look to approaches in other countries, provinces and territories, and other specific pieces of legislation like PIPEDA and the GDPR.

What Should be Legislated, and What Should be Left to Policy

While the *Privacy Act* is a fundamental source of legal obligations for federal institutions, other legal and policy instruments can help provide a measure of flexibility in the methods institutions choose to meet their privacy obligations. Given their more flexible nature, there may be a role for regulations, or Government-wide policy and directives, to address specific mechanisms or standards institutions should be considering in order to meet their privacy obligations.

Addressing Fears of Hacking, Privacy Breaches and Misuse of Personal Information

Many respondents were supportive of including requirements to safeguard personal information and to report privacy breaches in certain contexts. Others, such as the OPC, mentioned adding offences to the Act to address deliberate misuse of personal information, or attempts at re-identifying personal information without due cause.

Ensuring the Perspectives of Indigenous Peoples are Taken into Account

This targeted engagement was a starting point in understanding the perspectives of Indigenous Peoples that will need to be considered in modernizing the *Privacy Act.* As many changes to the Act may have a unique impact on Indigenous Peoples, the Government will be seeking further engagement opportunities with Indigenous groups.

CONCLUSION

This preliminary targeted engagement provided officials with a number of important perspectives and comments from experts, Indigenous groups and Government of Canada institutions. The views gathered during this preliminary engagement will help the Department of Justice better orient its work in developing options for reform for the *Privacy Act*. This preliminary engagement is an important first phase of a broader external engagement strategy meant to continue the conversation on the modernization of the *Privacy Act*. Eventually, the Government of Canada plans to engage the broader Canadian public, as it works to develop specific proposals for amendments to the Act.

Appendix A – Discussion Papers

1. Privacy principles and modernized rules for a digital age.

2. Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust.

3. Greater certainty for Canadians and government – delineating the contours of the *Privacy Act* and defining important concepts.

4. A modern and effective compliance framework with enhanced enforcement mechanisms.

5. Modernizing the *Privacy Act*'s relationship with Canada's Indigenous Peoples.