Department of Justice Canada
Ministère de la Justice Canada

PRIVACY ACT MODERNIZATION: A DISCUSSION PAPER

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

A technical engagement with experts on the future of the *Privacy Act*, Canada's federal public sector privacy law.

This discussion paper is being sent to expert stakeholders for their views and feedback on technical and legal considerations to consider in modernizing the *Privacy Act*. This targeted technical engagement will help the Government of Canada refine potential proposals for changes to the *Privacy Act*.

Canada

Earning trust through transparency and accountability

Digital transformation has resulted in increasingly rapid, effortless, opaque and technologically complex information flows. The current reality is overwhelming and difficult to comprehend for most individuals. At the same time, Canadians legitimately expect to see, understand, recognize value, and ultimately have trust in how government institutions collect, use, share and protect their personal information in a digital age. Effective transparency and accountability measures will be critical to meeting these legitimate expectations.

Accountability requires, but is much more than, transparency. While transparency is unquestionably fundamental, transparency alone cannot ensure accountability. The Privacy Commissioner of Canada has defined accountability in relation to privacy practices as "the acceptance of responsibility for personal information protection".[1] Viewed in this light, it is easy to see why accountability is gaining traction internationally as a concept that can effectively further proactive, systematic, holistic, and dynamic approaches to privacy governance. To accept responsibility for personal information protection, institutions must embrace their privacy responsibilities, invest in the internal capacity, tools, and processes necessary to satisfy them, and demonstrate to Canadians how their personal information is protected.

Introducing enhanced transparency and accountability mechanisms into the *Privacy Act* would support individuals to gain a more meaningful awareness of what government institutions are doing with personal information and to understand how institutions are protecting it. The ultimate goal is to position government institutions to earn, rather than merely ask for, individuals' trust. This trust can be earned when government institutions openly communicate information about their privacy practices and proactively demonstrate to Canadians what measures they take to protect personal information and comply with a strong and modern law, all in a way individuals can understand.

It is important that the possibilities digital transformation presents for enhanced governance also be integrated into government institutions' communications with Canadians. This means that new and more effective means of communicating information can be used to better support individuals to be aware of and understand how their personal information is used and protected by government institutions. There should be reciprocity in government institutions' use of new technologies – just as these technologies help government institutions to use personal information to more effectively perform their functions, they can equally help government institutions to better communicate with Canadians about these practices in an open and accountable way.

The key question is *how* the *Privacy Act* might be updated so that Canadians can best gain an enhanced understanding of and have trust in how government is using and protecting their personal information in the digital age.

One key consideration is ensuring that a modernized Act is structured to support meaningful engagement with accountability measures. When the practical benefits of implementing a particular accountability measure become clear, a renewed culture of compliance can take hold.

As well, successfully achieving the Privacy Commissioner's vision of accountability will require ongoing dialogue with the Commissioner's office of the right sort. The Privacy Commissioner cannot be responsible for telling government institutions what to do in every circumstance. A truly accountable institution must be able to come to and explain strong privacy decisions on its own. This capacity is particularly important when making day-to-day operational decisions within a principled legal framework. At the same time, the Privacy Commissioner's office can provide invaluable guidance and support to government institutions, particularly in more complex or novel scenarios. Strong and independent accountability is not incompatible with seeking the support of experts. Assistance from the Privacy Commissioner's office can effectively support government institutions to develop their own internal expertise.

[1] https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf

Having an Act that clearly delineates institutional roles can also assist government institutions to effectively execute strong and accountable decision-making. The President of the Treasury Board is the designated Minister responsible for developing directives and guidelines concerning the operation of the *Privacy Act.* While government institutions are guided by Treasury Board policy instruments, they remain independently accountable for ensuring their institutional practices are compliant with the Act. The Privacy Commissioner, through investigations and reviews, assesses compliance and makes recommendations. In addition to seeking a broadened authority to disclose information about investigations in the public interest, the Privacy Commissioner has also sought a public education and research mandate. A richer ecosystem of complementary compliance support in the form of policies, guidance documents, and investigation reports could assist institutions to enhance their own accountability.

A. Privacy management programs to support a new Accountability principle

The Accountability principle finds expression in many national jurisdictions (including in Canada's federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and leading international privacy instruments, such as the Organization for Economic Co-operation and Development's ("OECD") revised *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the Asia Pacific Economic Cooperation (APEC) Privacy Framework, the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108),* and the European Union's *General Data Protection Regulation* (GDPR).

The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia have published joint guidance about how privacy management programs can support accountability.

A privacy management program may be characterized as a comprehensive and evergreen privacy governance tool. It is scalable to the size of an organization and to its activities. And it can take many forms and include a flexible range of elements that would be expected to evolve over time. The Commissioners' guidance suggests that core elements could include administrative structures, processes and tools that work to champion privacy compliance within an organization; "program controls" such as policies, technical tools, training and other protocols that support compliance; and mechanisms to ensure ongoing assessment and revision. Ultimately, a privacy management program is a customized tool to support organizations to proactively take ownership of their privacy responsibilities and effectively meet them.

The benefits of a strong privacy management program are clear. Integrating privacy management programs into the *Privacy Act* could:

- empower individuals to better understand and exercise their rights;
- enhance the confidence of the Privacy Commissioner and information sharing partners in institutions;
- build internal capacity and increase awareness of privacy compliance within institutions;
- promote strong privacy compliance;
- support a transition away from a reactive oversight model to a more efficient proactive one; and
- encourage holistic data governance by networking, or linking, a wide range of policies and governance tools together, through a privacy management program hub (e.g. the new Treasury Board Algorithmic Impact Assessment tool).

Government institutions already implement many of these best practices and realize the related benefits. This is because a range of Treasury Board policies already set expectations similar to those that would form part of a privacy management program (e.g. privacy impact assessment, and breach response and notification guidance).

In many ways, the discussion around accountability is about determining which elements of existing Treasury Board policy might be appropriately integrated into the law and coordinated through a privacy management program, which are best suited as independent policy instruments, and whether there are any gaps.

Q.2(a): Should a privacy management program be formally required of government institutions under the Privacy Act or should institutions be given greater flexibility to independently structure their own compliance efforts?

Q.2(b): Are there any existing transparency measures that could be replaced by or integrated into a publicly available privacy management program?

Q.2(c): What core issues should be required to be addressed in a privacy management program?

B. The Privacy Commissioner of Canada's collaboration with other oversight bodies

Modern uses of personal information are increasingly making national boundaries practically inconsequential. Personal information travels frequently, far and fast. International flows of personal information will very often engage different national data protection laws.

PIPEDA was amended to facilitate information sharing among data protection regulators. The goal was to gain efficiencies in overlapping investigations and ultimately enhance privacy protection. The Privacy Commissioner has sought similar authorities in the public sector context. The House of Commons' Standing Committee on Access to Information, Privacy and Ethics ("ETHI Committee") agreed and recommended that "the *Privacy Act* be amended to expand the ability of the Office of the Privacy Commissioner of Canada to collaborate with other data protection authorities and review bodies on audits and investigations of shared concern in connection with *Privacy Act* issues".

Practices with personal information can transcend more than geographical boundaries. They can also cut across regulatory regimes. For example, automated decision-making practices have been associated with the potential for bias and discrimination that could be contrary to human rights protections in Canada. This raises the question of whether the Privacy Commissioner should also be empowered to work closely with other oversight bodies whose mandates may increasingly overlap with Canadians' privacy concerns. This could ensure the most coordinated and efficient investigation of multi-faceted matters and promote a broad and holistic approach to data governance and accountability.

Q.2(d): Are specific provisions addressing investigative information sharing with provincial privacy oversight bodies and privacy oversight bodies in foreign states necessary to support coordinated oversight in the federal public sector context?

Q.2(e): Would it also be useful to empower the Privacy Commissioner to coordinate his investigative and enforcement activities with a broader community of federal regulators and oversight bodies, such as the Canadian Human Rights Commission?

C. Transparency around the work of the Office of the Privacy Commissioner to promote accountability

The Privacy Commissioner has recommended that he be empowered to report publicly on government privacy issues where he considers it in the public interest to do so. The ETHI Committee supported this recommendation and, since this time, Bill C-58 has proposed to similarly empower the Information

Commissioner of Canada. It would authorize the Information Commissioner to exercise discretion to publish her reports of findings after the period for initiating any judicial review has expired.

The Privacy Commissioner's current confidentiality obligations are a hallmark of the ombuds-model that inspired the current Act. While confidentiality has traditionally been seen as important to the success of such an oversight model, it may be important for the role of the Privacy Commissioner of Canada to evolve in this regard. Enhanced transparency with respect to the Privacy Commissioner's work may be of significant benefit to all affected by it, provided the privacy of individual complainants is respected.

Q.2(f): How can the privacy of individual complainants be best protected if the Privacy Commissioner's confidentiality obligations were amended?

Q.2(g): Are the mechanisms currently in place to protect the confidentiality of sensitive government information (e.g. s. 65) sufficient if the Privacy Commissioner's confidentiality obligations were amended to support enhanced knowledge transfer between the Privacy Commissioner, government institutions and the public?

D. Specific transparency measures

The *Privacy Act* sets out a number of accountability and transparency measures. The requirement to publish an annual report on the administration of the *Privacy Act* within the institution is one example. However, its implementation has been criticized by the Privacy Commissioner as typically constituting "an elaborate collage of statistics…with little or no explanation".[2] In response, the ETHI Committee has recommended that federal institutions be required to include "a descriptive element so as to make the information in the reports accessible and relevant". Additional provisions imposing other general transparency and accountability obligations create the "personal information bank," "personal information index," and "exempt bank" regimes.

Annual reports to Parliament

Given some of the criticisms of institutions' annual reports that emerged at the ETHI Committee and the potential for the inclusion of new accountability and openness principles, it may be useful to reconsider the overall purpose of and role of these reports. As an accountability measure, the requirement to prepare an annual report on the administration of the *Privacy Act* offers a useful internal review and reporting mechanism. However, it's not clear these reports are working effectively as a transparency measure accessible to individual Canadians.

Q.2(h): Should the Act specify any key information that should be included in public reports of institutions?

Q.2(i): Would a privacy management program requirement eliminate the need for separate annual reports?

Personal information bank regime

The *Privacy Act* requires that the government share information about its personal information holdings through the "personal information bank" (PIB) regime. "Personal information banks" are published descriptions of an institution's personal information holdings organized by program area. They are not physical repositories of information. The description contains prescribed information elements such as a statement of the purposes for which personal information in the bank was collected and consistent uses and disclosures. The President

[2] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322

of the Treasury Board and Minister of Digital Government, as designated Minister, is responsible for overseeing the implementation of the PIB regime, including the registration of new PIBs and the coordination of the "personal information index" – a published compilation of all personal information banks.

The PIB regime helps to regulate the collection of personal information through centralized oversight and controls; provide transparency to Canadians about what personal information is collected by the government, how the information is used and with whom it is shared; and assist individuals seeking access to their personal information.

However, the PIB regime is not particularly user friendly for Canadians. There are approximately 9,000 PIBs published across the websites of approximately 250 government institutions. The language, format and organization of PIBs are complex, making them difficult to understand. And most access requesters do not make reference to PIBs in their personal information access requests.

The PIB regime also fails to reflect the modern realities of government. For example, the Act defines a PIB as "a collection or grouping of personal information", suggesting a physical repository of information. While this would have been accurate in 1983, technological developments make it more accurate to say that a PIB is a *description* of personal information grouped by program area. There can be backlogs in the centralized registration of new PIBs and the updating of existing PIBs, resulting in inaccurate information being made available to Canadians. And while the PIB regime seems to serve an important accountability check within government institutions, it is not clear its potential as a transparency tool for individual Canadians is being effectively realized. Individual Canadians may be more likely to review privacy notices associated with the programs through which they are interacting with government, which contain very similar information.

Q.2(j): How can the transparency requirements of the Privacy Act be positioned to ensure the right information at the right level of detail is provided to Canadians in user friendly formats that will improve as new means of presenting information to Canadians become available?

E. Privacy breach notification

In addition to concerns about ensuring that Canadians can see, understand and trust in how their information is handled within government, the same transparency and accountability outcomes are important when there is a privacy breach. Although it is important to set out clear principles and rules and put strong measures in place to guard against any breaches, they can nevertheless occur. In those circumstances, what are the essential next steps and consequences?

Consistent with the Privacy Commissioner's recommendations for reform and those of a number of witnesses that appeared before it, the ETHI Committee recommended that the *Privacy Act* be amended to create an explicit requirement for government institutions to report material breaches of personal information to the Office of the Privacy Commissioner in a timely manner. The ETHI Committee also recommended that the Act be amended to ensure affected individuals are notified in appropriate cases, provided notification would not compound any damage to individuals. In its report, the ETHI Committee noted that most of the government officials who testified said they did not expect that a requirement to report material privacy breaches would be problematic. It is noteworthy that a policy requirement to report privacy breaches has been in place since 2014.

Since the ETHI Committee's report, PIPEDA's new mandatory breach notification and reporting regime has come into effect. The Office of the Privacy Commissioner has published detailed guidance for the private sector. And the Privacy Commissioner has also conducted a thorough review of government breach reporting and made a number of recommendations.

These developments have made clear that an effective and informative privacy breach notification regime depends on many factors. It will be important to properly define the relevant legal concepts and the circumstances in which these concepts are engaged; it is essential that institutions are properly supported to understand and follow the rules; continuous training and monitoring is critical as will be ensuring that the new mandatory breach notification regime gives rise to productive dialogue and does not informally or unduly penalize institutions for compliance. Consistency of understanding and approach across government institutions is particularly important if a useful picture is to develop from information that is emerging from the current policy-based approach to breach notification.

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

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

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

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