Department of Justice Canada
Ministère de la Justice Canada

PRIVACY ACT MODERNIZATION: A DISCUSSION PAPER

1. Privacy principles and modernized rules for a digital age

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

Contents

Renewing civic relationships in a digital age

Digital transformation has fundamentally altered Canadians' expectations, hopes, and fears about the ways in which their personal information may be used by a range of public and private actors. By profoundly expanding the scope of the possible, digital transformation has reshaped the ways we can flourish as citizens and human beings, how we pursue our personal and public relationships, how we communicate, how we access services, and how we can be supported, regulated, and protected by our government. In the digital age, flows of personal information are rapid, complex and ubiquitous. This information has new potential to both connect and distance us as citizens, aid and harm us as individuals, and foster and undermine our trust in government institutions. These developments have important implications for the civic relationship between individuals and their federal government that lies at the heart of the *Privacy Act*.

The *Privacy Act* is the legal framework governing personal information in the federal public sector. It explains how personal information must be protected in the relationships between individuals and the federal government. The Act expresses the legitimate, public purposes for which personal information may be collected, used, and disclosed by the federal government, both in relation to individuals and the broader public good. It also imposes a legal structure of limits and conditions on the use and disclosure of personal information by government.

Government institutions must adapt to meet Canadians' changing expectations about how their personal information may be used and respond to their concerns. For example, Canadians increasingly expect simple, seamless access to government services, available on platforms and devices they already use. This is why the Government of Canada is moving towards improving service delivery by, for example, having more integrated service offerings to optimize the service- delivery experience for Canadians. At the same time, Canadians have differing levels of comfort with how and in what circumstances personal information might be shared among and between government institutions.[1] Reviewing the *Privacy Act* in light of digital transformation, modern expectations, and the government's goals will be an essential element of meeting Canadians' changing expectations.

The objective of reviewing the *Privacy Act* is to ensure that individuals' interactions with government institutions are governed by fair, respectful and responsible practices with personal information that can address the challenges of today's society. A modernized *Privacy Act* can articulate a sound ethical framework to guide the careful and responsible management of personal information in the public sector in a way that is respectful of individuals' privacy rights. Supported by strong transparency, accountability and oversight mechanisms, such an Act would help Canadians trust their government to protect their rights and responsibly manage their personal information in the digital era.

This technical discussion paper asks experts to consider the specific question of introducing new privacy principles to guide government's interactions with individuals alongside modernized rules. The overarching question is whether and how to incorporate new privacy principles into the *Privacy Act* to enhance the protection of individuals' privacy rights. Renewed civic relationships grounded in a legal framework that reflects individuals' contemporary expectations is the ultimate aim.

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#toc2-6

A. New privacy principles to support a strong stewardship ethic to guide compliance

The pace and interaction of technological and societal change mean that the horizons of our concerns about personal information are constantly shifting. Individuals are increasingly engaging with government, and asking to engage with government, through digital networks. Introducing principles to embed the right norms into our federal privacy framework can help government institutions navigate the fluid challenges of digital transformation. Furthermore, a principled framework introduces essential outcomes that can establish a foundation for trust in how the Government of Canada will treat personal information.

Many privacy law regimes take their inspiration from the privacy principles articulated by the Organization for Economic Co-operation and Development's ("OECD") 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (updated in 2013). A principles-based approach to privacy regulation that includes more detailed guidance as necessary is increasingly seen as a best practice for both public and private sector entities.[2] Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA") reflects this type of approach, as does the European Union's General Data Protection Regulation ("GDPR") and Australia's recently updated *Privacy Act*, among others.

A number of witnesses that appeared before the House of Commons' Standing Committee on Access to Information, Privacy and Ethics ("ETHI Committee") during its most recent study on *Privacy Act* reform underscored the importance of including technologically neutral privacy principles in the Act. Some witnesses stressed the importance of writing legislation at a relatively high level, so as to ensure it is principle-based and technology-neutral. Other witnesses proposed updating the Act's purpose clause to explicitly recognize the underlying objectives of the Act. Ultimately, the ETHI Committee recommended that the Act be modified to include generally accepted and technologically neutral privacy principles similar to those contained in PIPEDA.

There are many roles new privacy principles could play in a modernized *Privacy Act*. They could:

- Explain a number of core commitments government can make to individuals relating to personal information that are not currently explicit legal requirements in the *Privacy Act*;
- Harmonize public and private sector privacy by imposing upon government the same style of regulation recognized and supported by the private sector;
- Facilitate Canada's interoperability with Europe, the UK, Australia, New Zealand and other states influenced by the OECD revised guidelines and those which are likely to follow suit in the future;
- Guide the exercise of discretion when decisions implicating personal information are made;
- Increase government's opportunities to innovate and find the best means to respect privacy while improving performance towards other goals; and
- Allow for public interest-based practices with information not explicitly pre-authorized in advance.

Some principles could express the norms or goals behind some of the existing rules. Others would express concepts wholly new to the legislative regime. Some could impose substantive obligations of outcome while others could be best positioned as considerations to inform the exercise of discretion. Precisely what new principles might be incorporated into the Act and how would depend on many considerations, including the ways in which the existing rules are eventually modernized.

[2]See, for example, the Australian Law Reform Commission's Report 108, *Australian Privacy Law and Practice* https://www.alrc.gov.au/publications/report-108 at chapters 4 and 18.

What can new privacy principles do to improve the *Privacy Act*?

Articulate core commitments to meet expectations	Encourage responsible decisions in novel situations	Support innovation in how to achieve outcomes
Ensure government institutions' practices with personal information reflect individuals' expectations and affirm core Canadian values central to effective governance.	*Enable the Privacy Act to effectively guide government institutions through rapid, continuous and transformative change*	*Facilitate individualized, innovative and continuously improving approaches within a principled framework*

(i) Meeting individuals' expectations

NEW PRIVACY PRINCIPLES WOULD ASSIST GOVERNMENT INSTITUTIONS TO MEET INDIVIDUALS' EXPECTATIONS AND AFFIRM CORE CANADIAN VALUES CENTRAL TO EFFECTIVE GOVERNANCE

The *Privacy Act* regulates the personal information individuals entrust to government. It sets out a number of rules to determine when government can collect, use and disclose personal information and how this information must be treated, once collected. This rules-based approach describes *when* a particular practice with personal information is permitted but does not explain *why* the rules are important or what considerations should guide their application. The purpose clause of the Act is also primarily descriptive – it does not explicitly state the core values animating the *Privacy Act*. This means the *Privacy Act* is largely silent about what values or desired outcomes should guide decision-making.

There may be value in explicitly articulating a supplemental, principles-based framework, particularly one that draws attention to the things that matter most to individuals – are practices with personal information reasonable, proportionate, fair, ethical, in the public interest and highly protective of privacy? New privacy principles can articulate new responsibilities and commitments to Canadians in support of these goals.

(ii) Succeeding in the face of constant and disruptive change

NEW PRIVACY PRINCIPLES WOULD ENABLE THE PRIVACY ACT TO EFFECTIVELY GUIDE GOVERNMENT INSTITUTIONS THROUGH RAPID, CONTINUOUS AND TRANSFORMATIVE CHANGE

Fixed and firm prescriptive rules, which say more or less precisely what to do in any given situation, may work well when the exact dimensions of a regulatory challenge are known and remain relatively static across time. But in the world of privacy, ongoing uncertainty about future privacy pressures is certain; rapid and disruptive change is the only constant; and regulatory solutions will necessarily lag behind emerging technologies.

Principles are typically general statements that articulate an abstract value or desired outcome. They allow for a range of valid outcomes across an indefinite range of situations. When principles express foundational norms that will withstand the test of time, their generality and flexibility is their regulatory strength. By requiring institutions to ask themselves how they can achieve the necessary outcome when new scenarios present, they can generate institutional capacity and thoughtful privacy responses, whatever the challenge.

For example, citizens increasingly expect simple, seamless access to government services, available on platforms and devices they already use. The Government of Canada is committed to improving service delivery by providing a "tell us once" user experience and seamlessly integrating Government of Canada service offerings into Canadians' lives, characterized in part through service integration with existing platforms. A modernized Privacy Act could articulate the right foundational norms to enable the government's digital transformation in a way that supports the protection of personal information held by the government while also supporting the delivery of digitally enabled services and results.

Similarly, the Government of Canada has articulated a new Digital Charter "to provide the framework for continued Canadian leadership in the digital and data-driven economy. This principles approach will not only protect Canadians' privacy and personal data but also leverage Canada's unique talents and strengths in order to harness the power of digital and data transformation."[3]

(iii) Supporting innovation within a paradigm of respect and accountability

BUILDING PRIVACY PRINCIPLES INTO THE ACT CAN FACILITATE INDIVIDUALIZED, INNOVATIVE AND CONTINUOUSLY IMPROVING APPROACHES WITHIN A LEGAL FRAMEWORK

Specific and detailed rules can deter government institutions from doing anything more than the rules explicitly require. For example, a rule that requires information to be published in a particular way, can discourage new and better ways of communicating the information. Principles can allow for and encourage adaptability in both privacy and business practices, subject to compliance with a legal, principled framework. The right privacy principles can assist innovation and privacy protection to be mutually supportive and advance in tandem.

What are some of the challenges associated with introducing new privacy principles?

New privacy principles will not be sufficient in themselves to modernize the Act. In fact, many of the benefits of moving towards a principles-based regime may also cause some discomfort. Stressing a requirement to achieve outcomes individuals expect instead of articulating specific steps an institution must take can introduce the potential for inconsistencies in approach. Additionally, principles-based regulation can complicate oversight and enforcement, as the lines delineating appropriate accountabilities and institutional roles around identifying specific compliance requirements can be blurred. An appropriate balance between new principles and modernized rules would be necessary. Related adjustments to oversight mechanisms would also require careful thought.

[3] See https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/minister-bains-announces-canadas-digital-charter.html

What principles could be added to the *Privacy Act*?

1. *Reasonableness and proportionality*

PERSONAL INFORMATION PRACTICES MUST BE REASONABLE AND PROPORTIONATE, INCLUDING BY MINIMIZING ANY NEGATIVE IMPACTS ON OR RISKS TO INDIVIDUALS AND APPROPRIATELY BALANCING INTERESTS.

When it comes to privacy, context matters. There may be value in having an underlying principle of reasonableness and proportionality that applies to all personal information practices, including collection, use, disclosure and retention. Such a principle could rely on the well-established Canadian legal standards of reasonableness and proportionality to accomplish the aims of related principles used elsewhere. For example, the "data minimisation" principle in the GDPR requires regulated entitles to ensure personal data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Introducing a reasonableness and proportionality principle into the *Privacy Act* could apply known and essentially equivalent standards to federal government institutions' practices with personal information – legal standards with strong roots in existing administrative and *Charter* law.

Certain witnesses before the ETHI Committee specifically recommended the adoption of an overarching proportionality obligation that would apply to all collection, retention, use and disclosure of personal information by federal institutions and others proposed subjecting collection and secondary uses of personal information to a principle of proportionality.

A "reasonableness and proportionality" principle would call on institutions to consider and mitigate privacy impacts and risks, even when an action with personal information (e.g. disclosure) may be specifically authorized. This principle would require institutions to implement personal information practices, such as an authority to disclose personal information in the public interest, in a reasonable and proportionate way. To be reasonable and proportionate, privacy impacts must be minimized. But no single means of minimizing impacts would be required, nor would strict minimal impairment be the standard. The reasonableness and proportionality principle would aim to place a contextually sensitive, holistic and balanced approach to privacy impact and risk minimization at the heart of an institution's decision-making.

Q.1(a): Could a reasonableness and proportionality principle achieve the same purpose (reasonable data minimization) as a "necessity" standard, but in a way that is more sensitive to contextual considerations? (see also the portion of this paper addressing the Threshold for collection, for related discussion and analysis)

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

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

2. *Privacy by design*

A GOVERNMENT INSTITUTION MUST DESIGN FOR PRIVACY WHEN CREATING OR MODIFYING PROGRAMS, SERVICES, SYSTEMS AND BUSINESS PRACTICES.

It is now broadly recognized that considering privacy during the design phase is a very good practice, as initial design decisions can have a significant impact on privacy outcomes. Doing so is typically more effective and less costly than attempting to fix privacy problems after the fact. As was recently recognized in the 2018 Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service, when data usage raises privacy implications, departments and agencies should incorporate privacy by design.

A design for privacy approach could support the integration of privacy values into systems design, preventing privacy from being treated as a source of friction on a system after it is implemented. A "privacy by design" principle could also support the development of better and more trustworthy government systems, resulting in an enhanced stakeholder experience. For example, this could foster greater trust for more innovative service delivery approaches by ensuring that the right privacy protections are in place from program inception.

Q.1(d): Could introducing a requirement for a "privacy by design" approach effectively advance privacy protection? If yes, would such a requirement function best as an overarching principle, a specific and/or supporting rule elsewhere in the Act, or as a matter of policy guidance?

Q.1(e): Would it make sense that compliance with a privacy by design principle also be subject to a reasonableness and proportionality standard? In other words, a design that is maximally protective of privacy would not be absolutely required if another reasonable and proportionate alternative were adopted in light of broader or competing considerations?

3. *Data security*

A GOVERNMENT INSTITUTION SHALL IMPLEMENT TECHNICAL, ADMINISTRATIVE AND ORGANIZATIONAL DATA SECURITY MEASURES PROPORTIONATE TO THE SENSITIVITY OF PERSONAL INFORMATION AND THE RISKS OF UNAUTHORIZED ACCESS OR OTHER MISUSE.

Data security is fundamentally about protecting individuals against potential harm from unauthorized access to or misuse of personal information. While federal government policies address data security, the *Privacy Act* itself is silent on this matter. However, certain data protection statutes, such as the GDPR, include principles aimed at ensuring that personal information is appropriately safeguarded to ensure the integrity and confidentiality of such information. The ETHI Committee's report also recommended that the Act include a principle addressing safeguards, and include an explicit requirement for institutions to safeguard personal information with appropriate physical, organizational and technological measures commensurate with the level of sensitivity of the data.

The "data security" principle proposes an obligation to take appropriate care, which will ensure institutions regularly review and improve their data security measures as new technologies and risks emerge. Government institutions would be expected to implement contextually appropriate data security measures, the intensity of which would be based on the sensitivity of the information and level of risk.

When the *Privacy Act* came into force in 1983 we lived in a paper based world where storing information in silos served as protection for privacy and the power of modern digital technologies was not even imagined. Digital technologies offer new mechanisms and approaches to keep personal information secure.

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

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

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

Q.1(i): How might new technology be leveraged to protect personal information?

4. *Openness and transparency*

A GOVERNMENT INSTITUTION SHALL BE OPEN AND TRANSPARENT ABOUT ITS PERSONAL INFORMATION PRACTICES AND MAKE INFORMATION PUBLICLY AVAILABLE IN CLEAR, ACCESSIBLE AND SERVICE-ORIENTED FORMATS.

Openness and transparency are central features of many modern data protection acts that apply to public-sector entities, including the GDPR. Transparency is a touchstone of good privacy practice. It helps institutions to be accountable, allows individuals to exercise their rights and make meaningful choices, and can promote trust. Indeed, enhancing transparency was one of the key elements of the ETHI Committee's report on *Privacy Act* review, and the ETHI Committee's report recommended that the Act include a principle addressing openness.

Transparency alone, however, does not generate meaningful openness: the information that is available should also be communicated in ways that can be readily understood. The "openness and transparency" principle is intended to require meaningful transparency and encourage the use of creative methods and new technologies to organize, display and share information about personal information practices to better communicate with individuals. Government institutions would be expected to be open, clear and straightforward about their treatment of personal information including: the purposes for which information is collected, used, retained or disclosed; the sources of privacy guidance; the nature of any automated activities, including systems that gather information, and the administration of privacy practices.

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

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

When considering the openness and transparency principle and the related questions, it may be useful to refer to the discussion paper entitled *Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust.*

5. *Accountability*

A GOVERNMENT INSTITUTION IS ACCOUNTABLE FOR THE PERSONAL INFORMATION UNDER ITS CONTROL AND SHALL DEMONSTRATE ITS ACCOUNTABILITY THROUGH TRANSPARENT AND ONGOING REVIEW AND IMPROVEMENT OF ITS PERSONAL INFORMATION PRACTICES.

Demonstrable accountability is taking hold as a regulatory best practice, and is an important element underlying many data protection regimes.[4] The ETHI Committee's report on *Privacy Act* review recommended that the Act include a principle addressing accountability. Demonstrable accountability would make institutions responsible for taking proactive steps to comply with the *Privacy Act* and to regularly demonstrate to the public and the Privacy Commissioner that they are acting in compliance with the law. It would not be enough for institutions to rely on unpublished internal practices or to wait for a complaint and investigation before taking action. Instead, institutions would be required to actively and transparently conduct internal reviews of their own practices and update and improve them as necessary. The "accountability" principle would also confirm ongoing compliance obligations with respect to personal information for as long as it remains under an institution's control.

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

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

When considering the accountability principle and the related questions, it may be useful to refer to the discussion paper entitled *Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust.*

B. Applying new privacy principles and modernized rules

A key question is how would new privacy principles interact with modernized versions of the existing rules?

Taking the principles proposed in this paper as an example, government institutions could be expected to satisfy *both* modernized rules and the proposed privacy principles.

The rules and principles would serve largely different functions. The rules would continue to delineate *when* particular practices with personal information – e.g. collection, retention, maintaining accuracy, use and disclosure – were specifically authorized or required. And new privacy principles would guide institutions' determinations as to *how* to exercise these authorities or comply with these requirements (e.g. openly, in reasonable and proportionate ways, with strong data security, etc.).

However, in designing for the future, it is not always clear what technology and possible privacy risks will exist, nor how government institutions' business practices may evolve. Because specific rules will not be able to provide for all scenarios, it is advisable to consider how principles might play a role in authorizing novel or

[4] See, for example, 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).

innovative practices with personal information that are in the public interest but were not foreseen when the rules were drafted. Some jurisdictions have ensured this type of legal adaptability by recognizing certain situations in which the need to comply with specific rules may be overridden by public interest considerations.

For example, the Australian *Privacy Act,* 1988 allows the Privacy Commissioner to make a "public interest determination", which "is a determination that an act or practice of an agency or organization, which would otherwise breach an Information Privacy Principle, National Privacy Principle, or an approved privacy code, is to be regarded as not breaching the principle or code" because an exception is in the public interest.

Other jurisdictions are exploring the concept of regulatory sandboxes in the data protection context. In essence, a regulatory sandbox is a controlled and supervised environment in which business models, structures or processes can be tested for compatibility with a single or multiple legal regimes.

The United Kingdom's Information Commissioner is currently implementing a data protection regulatory sandbox to support the use of personal information in innovative services in the public interest; forge a shared understanding of what compliance in particularly innovative areas looks like; and support the realization of an innovative economy. These outcomes will be achieved within the parameters of the *General Data Protection Regulation* and domestic law.[5]

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

Q.1(o): How can the Privacy Act be best positioned to effectively encourage and regulate novel practices with personal information that might not be captured by rules authorizing certain practices in advance?

C. Modernized rules to support individual's reasonable expectations in a digital age

The existing rules in the Act were inspired by and derived from the original OECD fair information principles. There are, however, gaps in the way the OECD principles were introduced into the *Privacy Act.* The original OECD fair information principles were updated in 2013. In addition, the passage of time invites us to reconsider how our Canadian rules might be updated to reflect and respond to the new opportunities and optimism, and the new challenges and concerns, that digital transformation presents.

Changes to the informational environment

The *Privacy Act* regulates the government's treatment of personal information primarily by means of rules set out in sections 4 to 8 of the Act. These rules have not been modernized since they came into force in 1983. They therefore reflect some dated assumptions about information flows regulated under the *Privacy Act.* For example, it is assumed as a default that personal information will follow a linear life cycle that starts with a known and direct collection between an individual and government institution. The assumption behind the requirement to retain information for a prescribed minimum amount of time is based on the risk that government institutions would be too eager to dispose of personal information, before individuals could exercise a right of access to it. The Act also does not speak to security safeguards, possibly because the physical security of buildings was the primary focus.

Obviously, the information environment has undergone a profound transformation since 1983. Human interaction is no longer required for personal information to be created, collected, analyzed and shared. Few

[5] https://ico.org.uk/media/about-the-ico/documents/2614219/sandbox-discussion-paper-20190130.pdf

institutions are in a rush to dispose of personal information given the existing and potential roles data can play in informing complex public policy challenges. For example, data can be used to assess how or which populations are benefiting or not from a particularly program, whether a government activity is having its intended effect or unforeseen consequences, or whether there is a new problem that government could or should address. Digital data security is now also arguably paramount over physical security concerns with respect to information. These are just a few of the radical changes to the information landscape.

Changes in the way government institutions perform their functions

Our current rules also reflects a number of presumptions about the role of government and the ways government institutions will perform their functions and relate to individuals and the public.

When the *Privacy Act* came into force in 1983, storing information in silos was one way to protect privacy. At that time, the full potential of the power of modern digital technologies could not be imagined. Today, Government institutions work with each other to perform public functions – whether it is delivering services to the public, regulating a particular area or administering or enforcing laws – and digital technologies present opportunities for greater innovation in the public interest.

Keeping information in one place is no longer the primary means to protect personal information. In certain circumstances, new and protective technological, administrative or governance measures might be capable of offering equal protection with fewer implications for broader public policy goals. As a result of the Internet of things and “ambient” data flows, the concept of institutions always exercising clear and certain “control” over all of the personal information they may encounter is under threat. And it is no longer clear that publicly available information should be wholly exempted from use and disclosure rules in light of the new ways in which this personal information may be used.

Some assumptions in the *Privacy Act* about how government institutions perform their functions are in tension with individuals’ modern expectations about the role of government and how their individual and social needs will be met. The scale, complexity and intersectional nature of the public policy challenges confronting government institutions requires multi-institutional, multi-jurisdictional and multi-faceted action; effective public policy interventions are more data-driven; and the public expects consistent, coordinated and convenient service delivery across life events, life stages and functional zones, not narrow, internal administrative lines. And at the same time, many individuals are increasingly concerned about how to assert control over their personal information, including public information. It would be useful to test our existing rules for assumptions and considerations that are no longer relevant or sound.

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

Consent

Given the public discussions on the role of consent in relation to privacy, one key question is how consent should operate in the context of government and the public sector.

The current *Privacy Act* does not require consent for the collection of information. A fundamental aspect of consent is that it is free and informed. In the public sector context, it can be very difficult to ensure consent meets these essential requirements. Some individuals might fear adverse consequences and feel compelled to consent to the collection of personal information. Collection is therefore based on the link to a legal activity by government. This is consistent with most public sector privacy legislation and the approach to public authorities under the GDPR.

"Consent will not usually be appropriate if there is a clear imbalance of power between you and the individual. This is because those who depend on your services, or fear adverse consequences, might feel they have no choice but to agree – so consent is not considered freely given. This will be a particular issue for public authorities and employers"[6]

"In order to ensure that consent is freely given, consent should not provide a valid legal ground for processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."[7]

There is also a concern that models based on consent can effectively and inappropriately "offload" an important accountability measure and responsibility from well-resourced organizations to over-burdened individuals. Individuals may be ill-placed to meaningfully understand, question and decide issues that arise in relation to the myriad consents they may be asked to provide in the course of a day – an issue that could be particularly acute in light of the power imbalances inherent in the public sector.

Robust alternatives to consent exist in the public sector. For example, public law requires that public institutions only undertake activities that fall within the bounds of their statutory mandates. The *Privacy Act* adds to this the additional requirement that institutions only collect personal information with a sufficiently direct connection to these legally authorized programs and activities. And consent by an individual to provide personal information cannot expand the scope of an institution's legal mandate beyond what it has been duly empowered to do. The *Privacy Act* is a model based fundamentally on lawful authority or legal authorization.

The *Privacy Act* does, however, recognize individuals' ability to provide a valid and meaningful consent in some circumstances, including for a specific use or disclosure of personal information. After a government institution has satisfied the requirements that must be met to validly collect information, the Act permits an individual to authorize a subsequent use or disclosure by way of consent. This recognizes individual autonomy and capacity to control the use and disclosure of their personal information in certain circumstances.

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

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

Defining consent is also addressed in the discussion paper entitled: *Greater Certainty for Canadians and Government - Delineating the Contours of the Privacy Act and Defining Important Concepts.*

Collection

The starting point for how governments obtain personal information is collection. Typically, the questions that arise focus on the purpose for the information and the conditions that need to be met before collection. Section 4 of the *Privacy Act* regulates the collection of personal information. It provides that "[n]o personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution". This rule prevents the collection of personal information that is not fundamentally required to further the program or activity a collecting institution is undertaking.

[6] When is consent appropriate, UK Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/
[7] GDPR, Recital 43, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

This approach is based on a concept of a government composed of separate departments that do not work together towards joint objectives. It is also rooted in the idea that privacy is most effectively protected by establishing narrow silos of information protected within the contours of a single government program or activity. However, increasingly, efficient government programs and departments work with each other to avoid duplication of efforts and streamline interactions with individuals. For many individuals, the efficiency of the process for obtaining benefits, applying for licences or notifying government about important life events is more important than which specific government department plays which role and which departmental program is being used.

Our objective in designing a law for collection is to minimize privacy impacts. Keeping this objective in mind, we need to consider how to frame a collection authority for framework legislation in a modern society.

Threshold for collection

A key issue is what conditions must the government meet before personal information may be collected. Whatever threshold is used must be able to work across all of the government's roles, which can range from service delivery to research and statistics to policy analysis to regulation and law enforcement.

The current threshold for collection – personal information must relate directly to a government institution's operating program or activity – is viewed as too permissive by some stakeholders.

Concerned with the potential for over-collection, facilitated in a digital environment by the ease with which information now flows, the Privacy Commissioner has recommended that the *Privacy Act* be amended to introduce a "necessity" threshold for collection. He has suggested in testimony before the ETHI Committee on March 22, 2016 that a "necessity" criterion would be met where personal information was "demonstrably necessary for operation of a program or activity". Demonstrable necessity would be defined, in turn, through reference to the *Charter*-based "*Oakes* test":

> "…personal information would be collected under the necessity test if: the information is rationally connected and demonstrably necessary to an operating program or activity; the information is likely to be effective in meeting the objectives of the program or activity; there are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity; and the loss of privacy is proportional to the objectives of the program or activity."[8]

Other witnesses that appeared before the ETHI Committee during its study on *Privacy Act* review expressed the view that proportionality could be an appropriate threshold. One individual witness framed the question this way: "Is the benefit to government operation or the country as a whole proportional to any trade-off in privacy? I think those are the questions that should be asked on a regular basis". In its December 2016 report, *Protecting the Privacy of Canadians: Review of the Privacy Act,* the ETHI Committee recommended that the collection standard require both necessity and proportionality.

It is clear that the impact of introducing a necessity threshold into the *Privacy Act* would turn on how necessity is defined and determined on the ground.

There is ongoing uncertainty in relation to at least two key aspects of this issue. The first question is how to distinguish between "absolute necessity", which no stakeholder appears to be advocating, and "reasonable or demonstrable necessity". The second question is what, exactly, should personal information be necessary for. In theory, the higher the threshold, the less information the government may be able to collect. Whether this is true in practice would depend on the interrelated issues of how the threshold and the scope of a program or activity the collection is intended to advance were defined. For example, what is necessary to evaluate an

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

individual's eligibility for a program may be more limited than what is necessary to assess a program's success across different demographics, for program evaluation or for research into social determinants.

Collecting no more personal information than is necessary has long been recognized as a primary example of how to minimize privacy impacts and risks in many cases. However, it is the outcome of minimizing privacy impacts that is key, not the means of achieving it. It is possible that in some cases, strictly limiting the quantity of information collected and shared may not be the best way to protect privacy. This approach could even undermine important public objectives, like supporting evidence-based policy interventions and avoiding data gaps or deficits that may be harmful on a broader scale. It may also impede or delay investigations by law enforcement agencies by raising questions as to whether information collected through the use of a particular investigative technique is "necessary" to advance the agency's investigation, or legislative mandate. A necessity threshold, which essentially mandates a particular and prescriptive means of respecting the goal of "minimal impairment," can also be at odds with the fact that many individuals may be comfortable with their personal information being used in furtherance of the public interest, even if not absolutely "necessary", provided privacy impacts and risks are minimized and there is transparency about how the information is being protected, analyzed and used.

Ultimately, "necessity" means very little in and of itself. It is therefore essential that the *Privacy Act* be clear about what exactly a collection of personal information should be "necessary" for. Is the goal strictly the bare implementation of a program? Or is there room within a necessity threshold to ensure the effective implementation of a program, consistent with broader government obligations and commitments?

In addition, rather than using the phrase 'operating program or activity', it may be preferable to refer more broadly to collection for specified, explicit and legitimate purposes that, for public authorities, will tend to be authorized by law. For example, under the GDPR, processing by public authorities will be considered lawful when it is for "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Article 6). This approach avoids an emphasis on internal administrative divisions within a government institution.

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

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

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

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

Other collection considerations

Government institutions' experience under the *Privacy Act* also underscore some questions that warrant consideration.

First, regulating collection at the level of individual programs and activities *of a single institution* is not always consistent with more modern ways in which government operates and Canadians expect to be served. If a

government institution may only collect personal information that is necessary for its own programs, integrated and more efficient approaches to the delivery of overlapping or related public services can be frustrated.

Second, evolution in the nature, format and flow of information has meant that personal information may be inadvertently collected in non-compliance with the Act in the case of unsolicited personal information or other means of passive receipt. The Act contains no guidance or exceptions for these scenarios. For example, new, "off the shelf" technologies like autonomous vehicles might, as a core and unavoidable design feature, collect more personal information about passengers, pedestrians and other drivers than a government institution wants or needs to discharge its mandate. Rather than seeing this as a violation of the collection rule, a new Act could articulate what should be done with this inadvertently collected information. Under what conditions would destruction or retention be appropriate?

Third, direct collection constitutes an important transparency, accountability and safeguarding measure. Under the direct collection rule, government institutions must, wherever possible, collect personal information to be used in a decision-making process about a person directly from that person. Exceptions are made in cases where an individual has consented to indirect collection or another institution has a legal authority to disclose it to the collecting institution. However, the existing requirements around direct collection may be difficult to maintain in light of new ways in which personal information is created and flows (e.g."ambient" personal information flowing from sensors). Additionally, some individuals may not always wish to be approached directly for their consent in every situation.

Q.1(w): Could new accountability and openness requirements be a sufficient substitute for direct collection in certain circumstances?

Q.1(x): In what circumstances might notice be an adequate substitute for direct collection?

Retention

Subsection 6(1) of the *Privacy Act* requires government institutions to retain personal information that has been used for an administrative purpose for the period of time prescribed by regulation. This is "to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information". Regulations under the *Privacy Act* set the default retention standard at "at least two years" after the last use in a decision-making process directly affecting the individual, unless the individual consents to a different disposal schedule.

These retention rules are highly prescriptive, centralized and indifferent to context. They impose a minimum retention period without specifying any criteria to govern decision-making around identifying an appropriate time for disposal. This recognizes the fundamental importance of the right to access one's own personal information and the express policy goal of ensuring that individuals have a meaningful opportunity to exercise this right, particularly where personal information has been used in a decision-making process directly affecting them.

While it serves to protect the efficacy of access rights, this approach to retention stands in tension with the best practice of minimizing personal information holdings and disposing of personal information that is no longer required. The current rule of keeping information for two years has no flexibility in situations where privacy may be best protected by destroying personal information more quickly after use.

It may be that, in the digital age, retaining personal information for longer than is necessary to serve the purpose for collection poses greater privacy risks to individuals than the risk of a thwarted right of access. At

the same time, hypothetical future uses of personal information in the public interest can support a cautious approach to disposal.

The trade-off between access rights and prudent disposal practices is most stark in cases where personal information has been collected indirectly. In these cases, an individual would not necessarily know what, how and why information they had not provided may have informed a decision-making process directly impacting them. In such a case, it may be that protecting access rights should prevail. In other cases where an individual had knowingly provided personal information to a government decision-maker directly for identified purposes, it would seem that prudent data disposal practices could carry more weight.

These considerations suggest that the current approach to retention could be recalibrated to improve its sensitivity to context.

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

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

Accuracy

Subsection 6(2) of the *Privacy Act* sets out government institutions' obligations with respect to the accuracy of personal information under their control. This provision is currently very outcome-oriented and principle-like. It imposes the following obligations: "[a] government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible." Its provisions mirror much of the OECD data quality principle.

The ETHI Committee's 2016 report did not address the issue of data accuracy in significant detail. However, it notes one individual witness' view that institutions' obligations with respect to accuracy should extend beyond their own administrative uses and apply equally to any personal information that is used or disclosed for all purposes. The witness was of the view that inaccurate information can have grave consequences for fundamental rights and freedoms.

In Canada, federal public sector privacy legislation began with provisions in the *Canadian Human Rights Act*. It is clear that there are strong continuing links between privacy and other rights, especially those related to equality, autonomy and human dignity. This is a useful history to draw on in a review of the current accuracy requirement. This is because important concerns are emerging about the potential for data-driven systems to learn and reinforce existing patterns of discrimination and exclusion, and to perpetuate new and as yet unknown risks to individuals and their fundamental interests. The increasingly mainstream public discourse about the risks of algorithmic decision-making is good evidence of a significant degree of public concern. These concerns are closely linked to data accuracy and data integrity but also engage broader ethical and anti-discrimination norms.

Q.1(aa): What role should the Privacy Act play in response to the ethical and human rights-based concerns that are arising in relation to new analytical tools and decision-making processes?

Q.1(bb): When they are engaged, are the current accuracy requirements sufficient to mitigate the bundle of risks that data-driven systems pose to individuals or do these requirements need to be adjusted in light of digital transformation?

Use and disclosure

Sections 7 and 8 of the *Privacy Act* govern the use and disclosure of personal information by government institutions. These provisions strike a balance between the fundamental importance of protecting individuals' privacy and the need to permit responsible uses and disclosures of personal information in the public interest. Thirteen scenarios in which personal information may be used or disclosed without consent are recognized. Each is purpose-driven and some contain contextually sensitive safeguards and accountability mechanisms.

The existing list of purposes for which personal information may be used and disclosed in accordance with the *Privacy Act* include: the original purpose for collection and consistent uses; the exercise of a federal legislative authority; compliance with the rules of court; facilitating the Attorney General's litigation role; investigative and law enforcement purposes; under information sharing agreements that further the administration of the law; constituent support; supporting Indigenous claims against the Crown; debt collection and, finally, when use or disclosure is "in the public interest".

Are any of the provisions unnecessary in light of changed circumstances since the Act was originally passed?

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

To what extent and how should the existing provisions be modernized to reflect over 35 years of use?

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

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

Many of the existing provisions are necessarily flexible in scope and application. This is to be expected in a legislative framework of general application that applies to over 250 federal institutions with unique mandates, informational needs and interjurisdictional partnerships. Some might therefore argue that recognizing any new use and disclosure authorities is unnecessary. However, after over thirty-five years of experience, some potential gaps – or at least a need for greater certainty – may yet exist.

For example, changes could allow Canadians to benefit from a "tell us once" approach so key client information is collected once and shared across authorized programs that require the information for the delivery of a benefit or service by:

- Ensuring personal information on file is relevant, current and accurate across programs and services, without the need for the client to provide the same updates to multiple departments and agencies
- Re-using existing information previously provided to the Government of Canada, including to pre-populate new applications from information already held by government, to simplify services for Canadians and to proactively offer benefits and services to clients by re-using their information.

Allowing greater sharing of information between authorized services, in carefully-defined circumstances, could also support better services for Canadians by enabling research and statistical analysis to improve service

design and delivery, and could improve program integrity (for example, preventing fraudulent receipt of government benefits). In moving towards greater sharing of information between services, transparency to Canadians about the information the government holds about them, and how it is used would be an important consideration.

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

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

Q.1(hh): If the government were to share and re-use personal information between authorized services and programs in defined circumstances in order to improve service delivery, what factors would need to be considered? What protections and limitations should be placed on such re-use of information?

The government's national security, intelligence and law enforcement functions are also often top of mind when people think about the use and disclosure of personal information by government.

The *Privacy Act* – including the role and powers of the Privacy Commissioner – does apply to national security, intelligence and law enforcement functions of government. However, the *Privacy Act* works in tandem with other specialized legal regimes in this context. For instance, particular legal powers are required to do national security, intelligence and law enforcement work, and these are set out in laws such as the *Canadian Security and Intelligence Service Act*, the *Customs Act* and the proposed *Communications Security Establishment Act*. The unique powers of police organizations are subject to specific safeguarding mechanisms with very close oversight by courts, such as warrant requirements under the *Criminal Code* for searches and seizures. In addition, there are specialized laws that govern information sharing in this context.

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

Access

Currently, the *Privacy Act* permits Canadian citizens, permanent residents and persons physically present in Canada to make personal information access requests. Canada is somewhat unusual in circumscribing categories of individuals with a right to access their own personal information. The Information Commissioner has noted that within a very broad cohort of comparable jurisdictions[9], only Canada, New Zealand and India limit who may have access to government information in this way

The ETHI Committee recommendation is that the Government of Canada consider extending the right of access to personal information to foreign nationals.

[9] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/: "Among the provinces and territories, Commonwealth countries, the U.S., in model laws, and those jurisdictions with access legislation ranked in the top 10 on the Global Right to Information Rating, only Canada, New Zealand and India limit who may have access to government information. All of the other jurisdictions reviewed provide a universal right of access…"

Through the use of an agent in Canada and the provision of consent that their personal information may be disclosed to a requesting agent, foreign nationals may and do use the *Access to Information Act*, rather than the *Privacy Act*, to obtain their own personal information. In addition, some institutions may treat access requests from foreign nationals on a discretionary basis, outside of either regime.

The increasingly global flows of personal information and the recent coming into force of the European *General Data Protection Regulation* also raise important considerations. Given the significance of the right of access, Canada's current regime gives rise to interoperability issues. *Ad hoc* and individually negotiated information sharing agreements that recognize a right of access for foreign nationals would not appear to represent the best and most efficient approach.

However, witnesses before the ETHI Committee expressed concern that broadening rights of access could consume significant system resources. Some expressed the view that response times for existing rights holders should be improved before the scope of the right to access personal information was expanded. While this is an important consideration, it is also conceivable that new technologies and processes could eventually assist to alleviate system pressures.

Q.1(jj): Given the uncertainty around the practical implications of broadening access rights but the compelling reasons to consider it, is this an area where regulatory experimentation might represent a middle ground? For example, would it be useful to pilot broadened access rights in certain cases on the basis of policy instruments to gather evidence to inform future legislative change?

Q.1(kk): Are there other relevant policy considerations in thinking about broadening the right of access to personal information?