Respect, Accountability, Adaptability
A discussion paper on the modernization of the *Privacy Act*

A public consultation about the future of the *Privacy Act*

The Government of Canada is consulting Canadians on potential ideas for modernizing the ***Privacy Act*** , Canada's personal information protection law for the federal public sector. The Act is Canada's **Quasi-constitutional** legal framework for the collection, use, disclosure, retention and protection of personal information held by federal public bodies.[1]

Since the Act first came into force in 1983, much has changed. Information today is largely digital, making it easier to gather, store and analyse. The continuing shift towards the digital holds great potential for making Canadians' interactions with the federal government easier and providing them with a more seamless experience when they seek a service or benefit. The Government's vision of offering services focussed on the user's experience, of being open and collaborative, and being digitally enabled requires some flexibility in the way information is used and shared within the federal government. As well, better **data integration** within the federal government can have clear benefits for Canadians. When the federal government has a better sense of public needs, it can be more efficient, better at coordinating public services, and able to make more informed decisions.

But the ability to gather, analyse and store more and more personal information also raises important privacy challenges. Canadians rightly expect that there should be good reasons for the federal government to access their data, limits on how it is used and shared, and clear protections in place for it. One key question the Government faces is how to update a decades-old law so that Canadians can benefit from the many promises of the digital environment, while respecting their modern expectations about how their information should be used, managed and protected.

The ideas put forward in this discussion paper have been informed by prior thoughtful examination of these complex issues by the **Office of the Privacy Commissioner of Canada**, the Standing Committee on Access to Information, Privacy and Ethics (**ETHI Committee)**, respondents to Justice Canada's 2019 **Targeted technical engagement** , discussions with federal departments and agencies, engagement with Indigenous stakeholders, and preliminary conversations with the broader Canadian public.

Public input on potential approaches to modernizing the *Privacy Act* is essential. This consultation will allow the Government of Canada to develop the most effective approach to legislative reform.

To learn more about the *Privacy Act* and how it affects you, visit the Justice Canada web pages on the public consultation to modernize the *Privacy Act*. We invite you to complete the online survey, upload a submission and participate in the discussion forum.

A vision for modernizing the *Privacy Act*

[1] The *Privacy Act* applies to more than 265 federal institutions. Federal institutions include core government departments and agencies, but also a variety of other federal public bodies that do not technically form part of the federal government. As such, this discussion paper will use the more inclusive term "federal public body" throughout.

A modern *Privacy Act* should enhance Canadians' trust in how federal public bodies treat, manage and protect their personal information. The Government of Canada's vision is for a modern Act that better reflects contemporary expectations about how federal public bodies should protect individuals' personal information and make better use of their information to keep Canadians safe, provide innovative solutions to the challenges Canadians face, and make Canadians' lives easier. A modernized *Privacy Act* should reflect how federal public bodies are effective stewards of the personal information Canadians entrust to them, while allowing them to improve and adapt to new changes in society and technology over time.

Three supporting pillars

This vision for modernizing the *Privacy Act* is supported by three pillars:

1. ***Respect*** for individuals based on well established rights and obligations for the protection of personal information that are fit for the digital age.

2. ***Accountability*** that is both meaningful and transparent. Being accountable means federal public bodies demonstrating that they have strong governance and oversight practices to help ensure they are responsible stewards of the personal information in their hands.

3. ***Adaptability*** to allow federal public bodies to innovate. New technologies, new business models, new capabilities, disruptive change, and unforeseen circumstances are the norm today. A modern Act should create a flexible framework that supports federal public bodies in effectively dealing with constant change. A one-size-fits-all approach to personal information regulation would reflect neither individuals' expectations nor the variety of contexts in which federal public bodies collect, use and share personal information.

Ensuring essential equivalence with other leading data protection regimes

The *Privacy Act* is only one component of an increasingly global framework that links regulation of personal information practices in both the public and the private sectors across many jurisdictions. The Act should strive to be consistent with other leading data-protection regimes in Canada and elsewhere to ensure a comparable equivalence with the core requirements of those regimes. At the same time, the *Privacy Act* has many unique features that have served Canadians well over the years and the Act remains a strong foundation for made-in-Canada enhancements.

One place to start is stronger alignment between the *Privacy Act* and the federal legislation that applies to the private sector, the ***Personal Information Protection and Electronic Documents Act*** . Coherence between these federal laws can simplify the personal information protection regime for everyone, enhance domestic **Interoperability**, prevent gaps in accountability where public and private sector entities interact, and further confirm the *Privacy Act*'s alignment with established global standards. Although they sometimes use different terminology and approaches, both Acts were influenced by the **OECD**'s foundational Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The **OECD Guidelines** were established in 1980 and updated in 2013 to reflect important developments

in international data protection, including the evolution of **Convention 108** , the **APEC Privacy Framework** and Europe's **General Data Protection Regulation** . A modernized *Privacy Act* should reflect important ongoing international developments as well.

Technological neutrality

A modern *Privacy Act* should emphasize technological neutrality. This will allow federal public bodies to explore different and new means of carrying out their roles and ensure the Act retains its relevance in the face of new technologies. It will also allow them to regulate new practices and respond quickly to change.

The *Privacy Act* and reconciliation with Indigenous peoples in Canada

The *Privacy Act* plays an important role in guiding the federal government's relationships with individuals. An additional objective of *Privacy Act* modernization is to advance reconciliation with Indigenous peoples in Canada as there are opportunities for the *Privacy Act* to acknowledge, affirm and empower Indigenous individuals, communities and governments.

While this public consultation offers an opportunity for all Canadians, including Indigenous people, to respond to some ideas for amending the *Privacy Act*, ongoing discussions with Indigenous governments and organizations have revealed some ways in which the Act may uniquely impact Indigenous individuals and communities. As well, addressing the control by Indigenous peoples over their information and data is an important step toward reconciliation. The Department of Justice Canada continues its discussions with Indigenous governments and organizations to gain further insight on some issues that have been highlighted through earlier discussions, such as:

- ***Reflecting the diversity of Indigenous governments***: Consideration is being given to replacing the current definition of "aboriginal government" with a more flexible definition that reflects the diversity of Indigenous governance models.
- ***Information-sharing partnerships***: In recognition of the unique nature, sensitivity and amount of personal information that federal public bodies may hold in relation to Indigenous people, a modernized *Privacy Act* might facilitate information-sharing with Indigenous governments and their institutions for a broader range of purposes than those currently recognized under paragraph 8(2)(f) of the Act. Addressing the need for such sharing of information with Indigenous governments and their communities is one way to help Indigenous peoples move towards self-governance.
- ***Continued disclosures for claims research***: Recognizing that advancing historical claims can require and justify the disclosure of personal information, the *Privacy Act* allows the federal government to disclose personal information for the purposes of "researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada." One issue to explore is the disclosure of personal information for such purposes.

- ***New governance mechanisms to support consultative approaches***: The protection of and access to the personal information of Indigenous people can raise particularly complex considerations. Indigenous organizations and governments want to exercise control over decisions involving the personal information of their members. New mechanisms and tools may help address these considerations.
- ***Special Indigenous interests in communal privacy protection***: Since individual and communal Indigenous privacy interests can be deeply intertwined, this raises the question of whether the *Privacy Act* could reflect the unique concept of communal privacy interests.

The modernization of the *Privacy Act* and the review of the *Access to Information Act*

Earlier this year, the Government of Canada launched a review of the *Access to Information Act.* This initiative will examine the legislative framework, consider opportunities to improve proactive publication to make information openly available, and assess processes and systems to improve service and reduce delays. The Government of Canada will engage Canadians on these important issues and will also seek the views of Indigenous peoples on aspects of the *Access to Information Act* that are of particular importance to them.

The *Privacy Act* and the *Access to Information Act* are both federal statutes that have **quasi-constitutional** status. There are similar provisions and elements in both Acts, including nearly identical exceptions and exemptions to providing access to records and personal information that share the same public interest rationales, such as security, confidentiality, and privacy.

These aspects of the *Privacy Act* will benefit from public input to the Government's review of the *Access to Information Act*. Accordingly, this discussion paper will not address some of these common elements, including the exceptions and exemptions to the right of accessing one's personal information. These will be reviewed at a later date.

Proposals for discussion for modernizing the *Privacy Act*

1. Changing the title of the Act

The title of the Act could be amended to more accurately reflect that it governs and regulates personal informational privacy

Despite its title, the *Privacy Act* is not the sole source of "privacy" protection in Canada, even at the federal level. Canadian law protects many different types of privacy interests through a combination of constitutional instruments, the *Criminal Code*, the *Civil Code of Quebec*, the common law, and other federal, provincial and territorial legislation.

For its part, the *Privacy Act* specifically addresses the privacy of personal information, as it governs the collection, use, disclosure, and retention of information that relates to identifiable individuals. In order

to reflect this underlying aim, the title of the Act could be changed to describe it as a personal information protection law, as is currently reflected in the Act's French title (*Loi sur la protection des renseignements personnels*).

2. Modernizing the purpose clause to better reflect the Act's broader objectives

The Act's purpose clause could reflect the important underlying public objectives of federal public-sector privacy legislation

The current purpose clause states that "[t]he purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a federal public body and that provide individuals with a right of access to that information." This statement reflects the Act's legislative history more than its broader public objectives. A modernized purpose clause could provide better guidance for interpretation by clearly stating the important underlying objectives of federal public sector data protection legislation, notably:

- protecting individuals' human dignity, personal autonomy, and self-determination;
- enhancing public trust and confidence in government;
- promoting the responsible use and sharing of data to advance government objectives in the public interest;
- promoting effective and accountable public governance;
- advancing reconciliation with Indigenous peoples in Canada by promoting improved data sharing with Indigenous governments and communities; and
- supporting sound, ethical and evidence-based public sector decision making.

3. Incorporating personal information protection principles from international models in the *Privacy Act*

The Act could include personal information protection principles similar to those under the *Personal Information Protection and Electronic Documents Act* to guide, support, and extend the protection of individuals' personal information

The *Privacy Act* could incorporate a number of internationally recognized principles for protecting personal information, such as: (i) Accountability; (ii) Identifying purposes; (iii) Consent; (iv) Limiting collection; (v) Limiting use, disclosure and retention; (vi) Accuracy; (vii) Safeguards; (viii) Openness and transparency; (ix) Individual access; and (x) Challenging compliance. Adding such principles to the *Privacy Act* would set the baseline expectations for Canadians and federal public bodies as to how personal information should be managed and protected in the federal public sector. As well, since these principles would be consistent with those of the ***Personal Information Protection and Electronic Documents Act,*** this would harmonize federal regulation of the public and private privacy sectors.

For additional details and a more in-depth discussion on the rationale for adding principles to the Act, and what these principles could entail, please consult our annex here.

4. Clarifying concepts

A number of definitions and concepts in the Act could be updated, and others could be introduced

There are a number of areas where the Act should provide clearer rules about its scope – what it covers and when its full protections are engaged. A risk-based approach to the protection of personal information has been emerging as an international best practice. Changes under consideration include:

- ***Applying the Act to "federal public bodies"***: Currently, the *Privacy Act* applies to "government institutions" as defined under the Act. While this term covers a comprehensive range of governmental institutions headed by a minister, it also includes many federal public bodies that are not core government departments or agencies. Changing "government institution" to "federal public body" would make it clear that many non-governmental federal entities are also subject to the Act.
- ***Updating and clarifying the definition of "personal information"***: The current *Privacy Act* defines "personal information" as "information about an identifiable individual that is recorded in any form." It includes a number of examples of what constitutes personal information, and also exempts certain information for the purposes of the use and disclosure provisions of the Act (and for access requests under the *Access to Information Act* for records that contain personal information). Proposed changes could include:
    - ***Including unrecorded personal information***: Removing the current requirement that personal information be "recorded" could simplify the definition. Many stakeholders have recommended this amendment as it would make the Act consistent with the ***Personal Information Protection and Electronic Documents Act*** and with the approach taken in many other jurisdictions. However, since the Act is organized around the concept of a "record," it is unclear what practical benefits would follow from expanding the definition to include unrecorded information. Many rights and obligations under the Act could not possibly apply to unrecorded information, such as an individual's right to access and correct their personal information, a federal public body's obligations to retain such information, and certain rules for use and disclosure. Additional input on the practical benefits of such a change is needed.
    - ***Clarifying when an individual is "identifiable"***: The Act could provide criteria for determining when information is about an "identifiable individual" and thus subject to the Act's requirements. Sensitivity to context would be particularly important, as different considerations might be appropriate depending on the circumstances. For example, could someone reasonably be identified from information that is restricted to confidential internal use, as opposed to greater public disclosure?

- ***Introducing a balancing approach where personal information reflects the views and opinions of one individual regarding another***: Currently, the definition of "personal information" identifies individual A's stated views or opinions about individual B as individual B's personal information, not just individual A's. This means individual B has, subject to some exceptions, a right to access individual A's views or opinions about them and to know the identity of the individual who made those statements. This is an important right in many situations, especially where one person's opinions can negatively impact another's rights. However, in some circumstances, it might be more important to protect the confidentiality of a person's opinion about someone else – for example, in the context of harassment allegations and investigations. The Act could include a provision outlining a more nuanced and flexible balancing approach to apply in such cases, rather than the current fixed and firm rule.
- ***Removing exemptions from within the definition itself***: Paragraphs (j) to (m) of the current definition exempt certain types of information that would otherwise be considered "personal information" for the purposes of sections 7, 8, and 26 of the Act (and section 19 of the *Access to Information Act*). These exemptions ensure that some information can be accessed by individuals other than the individual to whom the information relates, largely for reasons of public interest. However, these exclusions have been difficult to interpret and administer in practice. As well, the public-interest rationale justifying greater use, sharing and access to such personal information might be better reflected elsewhere in the Act and in the *Access to Information Act*. Therefore, to simplify the definition, this list of exemptions could be removed and sections 7, 8, and 26 amended as necessary.

- ***Defining business contact information***: Currently, the Act does not clearly indicate that business information is not personal information, which can lead to challenges in certain cases, such as where a business is operated by a sole proprietor. The Act could make it clear that information that relates primarily to a business is not "personal information."

- ***Outlining factors for valid consent***: The Act could include factors or standards to help ensure that individual consent provided under the Act is specific, informed, and voluntary, and able to be revoked.

- ***Setting out an updated framework for publicly available personal information***: The *Privacy Act* applies to publicly available personal information, except its rules governing subsequent uses and disclosures of personal information. However, the Act does not specifically define the term "publicly available." A modernized Act could define personal information as being "publicly available" in three instances: first, when it has been made manifestly public by the individual the information relates to; second, when it is broadly and continuously available to all members of the public and the individual has no reasonable expectation of privacy in the information; and third, when another act of Parliament or a regulation requires the information to be publicly available. As well, the current exclusion under subsection 69(2) could be eliminated so that all

the Act's rules would apply to publicly available personal information, while provisions to permit the use and disclosure of such information in specific cases could be added, along with a related exception to the right to have personal information collected directly from the individual.

- ***Broadening the concept of administrative purpose***: Certain protections in the *Privacy Act* apply to personal information that is used for an "administrative purpose." Under the Act currently, an administrative purpose relates to the use of personal information in a decision-making process that directly affects the individual the information is about. However, where it is not used for an administrative purpose, some of the standard requirements relating to notification, correction and retention are relaxed. The Act could be amended to broaden the scope of administrative purpose to capture any practice involving personal information that could directly affect the individual, whether or not a decision-making process was involved. This would ensure that the full suite of protections in the Act applied to the design and development of artificial intelligence systems, for example.

The Government is not currently considering specifying categories of personal information to which special rules would apply (such as "sensitive" personal information or information relating to minors), though some other jurisdictions do so. A flexible principles-based approach, along with some of the other proposed changes, would ensure the appropriate protection of personal information according to context. The Government also agrees with the **Privacy Commissioner** that the Act is not an appropriate place for defining "metadata," since many forms of metadata will simply not be information about an identifiable individual.

5. Updating rights and obligations, and introducing new ones

Existing rights for individuals and obligations for federal public bodies could be updated and new ones introduced.

The *Privacy Act* currently set outs a number of rights for individuals. Canadians and individuals present in Canada have the right to access their personal information. They also have rights related to notification and the correction of their information where a federal public body uses it to make a decision about them.

The Act also imposes certain obligations on federal public bodies when they intend to use the personal information to make a decision about that person. These obligations include: (i) collecting personal information directly from the individual where possible (subject to certain exceptions); (ii) retaining personal information for at least two years from the last time the personal information was used (unless the individual consents otherwise) or until the individual has had the opportunity to exercise all his or her rights under the Act; (iii) maintaining the accuracy of such information; and (iv) including it in a personal information bank (among other information).

These existing rights and obligations could be updated, and new rights and protections could be added to address expectations that have evolved in the digital era. Such changes could include:

- ***Expanded access rights***: The Act could extend the right to access one's personal information to foreign nationals who are not present in Canada, provided there are adequate procedures to verify the identity of the person requesting the information. This would eliminate the current need for foreign nationals to rely on third parties present in Canada to make requests for their personal information on their behalf under the ***Access to Information Act***. It would also bring Canadian law in line with other jurisdictions' practices of providing universal access to personal information and enhance interoperability with the European Union in particular. However, given that a number of federal government institutions have noted that expanding access rights could have important resource implications, it might be prudent to first pilot a limited expansion of access rights to test its impact on public resources and the system as a whole, and to provide an opportunity to develop effective procedures for identity verification.
- ***A right to have personal information collected directly from the individual for all intended purposes, unless an exception applies***: Exceptions allowing a federal public body to collect personal information in ways other than directly from the individual would include those already set out under the Act. Other exceptions might be:
    - where the individual provides consent to indirect collection of their personal information;
    - where the information is "publicly available" and is being collected for a purpose other than making a decision directly affecting the individual;
    - where the information is collected for the purpose of an investigation by a law enforcement or national security agency;
    - where collection from another source is authorized or required under another act of Parliament; or
    - where the information is received from another federal public body pursuant to a disclosure authorized under the *Privacy Act*.
- ***A right for the individual to be notified when his or her personal information is collected by a federal public body, unless an exception applies***: The Act could also include a right for individuals to be notified of when their personal information is collected by a federal public body. The Act could set out the minimal elements that would have to be included in a notice to individuals. However, the Act could also set out reasonable limits to this right, such as:
    - where the individual already has been notified;
    - where the federal public body is authorized to collect personal information from a source other than the individual;
    - where the purpose of the collection relates to a law enforcement or national security matter; or

  - where providing notice would be practically impossible or would defeat or prejudice the purpose of the collection or result in the collection of inaccurate information.

- ***A right to request that inaccurate personal information be corrected in a timely manner***: The Act could broaden the existing obligation to ensure the accuracy of personal information to require that all personal information that could have a direct impact on an individual be kept accurate, in line with a potentially newly broadened definition of an administrative purpose. As well, the right to require correction of personal information could extend to all personal information used for an administrative purpose and it would have to be corrected within a reasonable amount of time.

- ***Certain rights relating to enhanced public awareness of interactions with automated decision-making systems (such as artificial intelligence tools)***: Aligning *Privacy Act* transparency and accountability requirements with leading federal public sector policy instruments guiding the use of automated decision-making systems could help ensure that individuals know when they are interacting with these systems, what types and sources of personal information these systems use, and general information on how they function. It would be important to retain flexibility and technological neutrality in any new framework for automated decision-making, so that any new rules could be adjusted as government experience in this area grows. As well, exceptions could be made for certain contexts, such as law enforcement and national security, where providing details on such information could harm the public interest.

- ***A specific principle to protect personal information with appropriate technical, administrative and physical security safeguards***: The Act could include a "Safeguarding" principle, as the ***Personal Information Protection and Electronic Documents Act*** does, to ensure that Canadians benefit from the same level of data security protections regardless of which sector or Canadian jurisdiction they are dealing with **Treasury Board Secretariat ("TBS")** policies could translate high-level legal requirements into more detailed operational policies and directives suitable for federal public sector institutions.

- ***An obligation to contain personal information breaches and to subsequently notify the Privacy Commissioner and affected individuals in certain cases***: The Act could include obligations for federal public bodies to minimize and mitigate impacts of material breaches and to notify the Privacy Commissioner and affected individuals where there is a risk of significant harm to an individual. The obligation to notify the Privacy Commissioner and affected individuals would arise as soon as practically possible after making efforts to contain and assess the breach.

- ***An obligation to retain information about any personal information breach***: The Act could include a new obligation to retain information about all personal information breaches, whether they create a real risk of significant harm to an individual or not. This obligation would allow the Government to more effectively monitor trends and address potential risks that go beyond any single federal public body. It could also allow the Privacy Commissioner to effectively verify compliance.

6. Updating rules on the collection, use, disclosure, and retention of personal information

The Act could include updated and new obligations that relate to the collection, use, disclosure and retention of personal information

While many stakeholders have expressed broad support for a shift towards a principles-based *Privacy Act*, many have cautioned that principles need to be supported by more detailed rules that can offer specific direction about what the Act requires or allows federal public bodies to do. Rules governing the collection, use, sharing and retention of personal information could be updated and new ones added. These could include:

- ***Limiting the collection of personal information to where it is reasonably required for a federal public body's functions or activities:*** In line with a new "Limiting collection" principle, the Act could provide that a federal public body can only collect personal information where it is reasonably required for the federal public body's functions or activities, or where it is otherwise expressly authorized by another act of Parliament.

  In order to provide a more contextual approach to determining what may be "reasonably required," the Act could include a list of key considerations that federal public bodies would have to take into account in determining whether a collection is "reasonably required," including: (i) the specific purpose for the collection, particularly whether it was for law enforcement or national security purposes; (ii) the mechanisms or means employed to collect the information; (iii) whether there are less intrusive means of achieving the purpose at a comparable cost and with comparable benefits to the public; and (iv) the degree of intrusiveness of the collection compared to the public interests at play.

  This approach would place an emphasis on making collection of the information reasonable and proportionate, while addressing concerns and risks that an explicit necessity requirement could unduly hamper the ability of federal public bodies to carry out their mandates effectively. It would also allow Parliament to adapt to other specific scenarios or technologies in the future where the general "reasonably required" standard might actually impede the government's ability to carry out its work in the public interest. This approach would also shift the orientation of the collection framework away from specific programs, activities and institutional silos to better accommodate federal public bodies and ministers who have overlapping mandates, and help make programs more efficient within federal public bodies.

- ***Making it clear that created or derived personal information is a "collection"***: The Act could specify that personal information that a federal public body creates or derives by making inferences based on an individual's personal information, or information about other individuals, would qualify as a collection of personal information.

- ***Addressing unsolicited collections of personal information***: There is uncertainty about what obligations federal public bodies have when they unintentionally receive personal information they do not want or do not reasonably require. For example, sometimes individuals will provide sensitive personal information on unrelated matters through the free text feedback forms in online consultations. To address such scenarios, the Act could include specific obligations for cases where federal public bodies receive unsolicited personal information they do not require, such as the obligation to delete it or return it. The Act could also make it clear that retention obligations do not apply to unsolicited personal information.

- ***Clarifying the meaning of "consistent" uses and disclosures***: The Act currently allows federal public bodies to use or disclose personal information where this is done for the same purpose the information was collected for or a use consistent with that purpose. This particular provision has caused some uncertainty among federal public bodies as to whether an intended use or disclosure is for the same purpose for which it was collected, or whether another purpose is "consistent" with the original purpose.

  The Act could continue to permit federal public bodies to use or disclose personal information for a purpose that is compatible with the original purpose for which the information was collected. However, to provide greater clarity around the concept of a "consistent use", the Act could define this term and set out a non-exhaustive list of examples to better guide federal public bodies in applying it. Examples could include using or disclosing personal information when it is needed to assess eligibility for a service or benefit or to make it possible to provide a service or benefit, which would limit the situations where individuals would have to provide the same information to different federal public bodies for the same purpose.

- ***Updating the provisions that allow for the use and disclosure of personal information for other purposes***: In line with a new "Limiting use, disclosure and retention" principle, the Act could continue to set out a list of authorized circumstances where personal information may be used or disclosed for a purpose other than that for which it was originally collected. The Act could distinguish between authorities for using and for disclosing personal information and modify the current section 7 to clarify when internal uses of personal information are permitted, since the way certain disclosure authorities under subsection 8(2) are framed make them ill-suited for internal uses of personal information.

  The list of circumstances in which personal information may be used or disclosed could continue to include when an individual has given their consent, as well as many of the currently listed authorities. Others authorities would be specified, including using or disclosing personal information in emergencies, to ensure public safety or the safety of an individual, to notify next of kin, and for **Data integration** purposes in some circumstances, subject to certain limits and conditions.

  The Act could also eliminate the current "public interest" authority under paragraph 8(2)(m) and replace it with a new framework that could permit a further use or disclosure of personal

information for a purpose not specifically identified in the Act where the head of a federal public body determined that doing so would be "reasonably required" in the public interest, with an associated record-keeping requirement for such decisions to allow review by the Privacy Commissioner. As with the possible updated collection threshold, the Act could identify key considerations that the head of a federal public body would have to take into account in determining whether another use or disclosure was "reasonably required."

- ***Introducing a principles-based approach to retaining personal information***: In line with a new "Limiting use, disclosure and retention" principle, the Act could require federal public bodies to retain personal information for no longer than reasonably needed to effectively carry out the purpose for which it was collected. This would provide federal public bodies with flexibility to adapt their retention practices to the unique circumstances of each collection. This framework could be complemented by a list of specific provisions allowing for longer retention periods, including for archival purposes, to respond to requests for access to personal information and to comply with other legal obligations.

For additional details and a more in-depth discussion on the rationale for these potential changes, please consult our annex here.

7. Allowing a greater role for "de-identified" personal information

Federal public bodies could be provided with greater flexibility to use and disclose personal information that has undergone an established process for removing personal identifiers

There is great promise for the use of **de-identified personal information** to allow federal public bodies to innovate in the public interest, while still protecting personal privacy. Despite some well-known anecdotes of **de-identified personal information** being subsequently re-identified, the use of de-identification as a privacy-enhancing technique is well supported, even by regulators. De-identification does not completely eliminate the risk of re-identification, but when done appropriately, it significantly reduces that risk. As such, a framework focussed on reducing risks by removing personal identifiers *and* protecting later uses of de-identified information would allow federal public bodies more flexibility to use data for public benefit, while minimizing risks to personal information.

To create a greater incentive for federal public bodies to use and share de-identified personal information, instead of information that identifies individuals, the Act could:

- ***Define "de-identified" personal information;***
- ***Clarify that the process of de-identifying personal information is not a separate "use" of the information***;
- ***Allow federal public bodies to use and disclose de-identified personal information in a greater variety of circumstances***: The Act could allow federal public bodies to use or disclose de-identified personal information without consent where the information is used or shared in the

public interest, where the information has been de-identified according to a process set out in regulations or Government policy, and where appropriate technical, administrative and/or contractual protections, which could vary depending on the context, have been applied to the de-identified information;

- ***Create a specific offence for re-identifying personal information that has been de-identified, or for wilful attempts to do so.***

8. Introducing stronger accountability mechanisms in the Act

Specific obligations could be added in the Act to help federal public bodies demonstrate how they are accountable for their personal information practices

The Act could introduce obligations to support the principle that each federal public body is responsible for personal information under its control. The Act could also set out tools to assist federal public bodies in demonstrating to Canadians, and to the Office of the Privacy Commissioner where required, that they have effective measures in place to comply with the Act and protect personal information. These could include:

- ***An obligation to ensure that personal information sent outside of Canada is appropriately protected***: The Act could impose legal requirements for federal public bodies to ensure that appropriate privacy-protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information, consistent with current Government policy. A flexible, risk-based approach to this requirement would take into account the various contexts in which information can be shared outside of Canada, as well as the variety of frameworks for protecting personal information outside of Canada. The Act could require that flows of personal information outside of Canada be governed by a written agreement or arrangement that would include safeguards appropriate to the context of the disclosure, including whether there is already an applicable agreement or arrangement, the nature of the privacy-protection regime where the information is flowing to, and the sensitivity of the personal information being disclosed. Regulations or policy could support this obligation.
- ***An obligation to design programs and activities with the protection of personal information in mind***: The Act could impose a process for proactively protecting personal information by integrating considerations of how to protect such information into the early stages of the development and implementation of an initiative, such as a new program or service offered by a federal public body. This is also known as **privacy by design**. Government policies already require federal public bodies to assess and mitigate privacy risks when they develop new or modified government programs and activities. Making this a legislative requirement would reflect the Government's current practices and commitment to addressing privacy issues from the outset.

- ***An obligation to undertake a Privacy Impact Assessment***: The Act could impose an obligation on federal public bodies to undertake an analysis to identify and mitigate privacy risks. This type of analysis is commonly known as a **Privacy Impact Assessment (PIA)** and is currently framed by policy. This obligation would apply to new programs or activities or substantially modified existing programs that involve the collection, use or disclosure of personal information for administrative purposes, for automated or manual profiling activities that involve sensitive personal information, or as otherwise mandated by Government policy. The Act could define "substantially modified" to clarify the circumstances in which such an analysis needs to be undertaken, and the requirements of the Act could be supported by updated policy.
- ***An obligation to have a Privacy Management Program***: The Act could also impose a new requirement for federal public bodies to create and maintain a **Privacy Management Program** . This is essentially an organizational plan for protecting personal information that a government public body can use to identify, organize, review and improve its practices relating to personal information. It would serve as an individualized guide for compliance with the Act. The Act could identify the minimal components of what a **Privacy Management Program** had to include, along with a requirement that they be regularly reviewed and updated. These requirements would be supplemented by supporting regulations or Government policy.
- ***Clarifying which federal public body is accountable when multiple public bodies are involved***: The Act could clarify which federal public body, or bodies, would be responsible for personal information where two or more federal public bodies have access to the same datasets, such as where a shared database is accessed by a number of federal public bodies.

9. Modernizing transparency practices

Specific obligations could be added to the Act for federal public bodies to provide readily available explanations of their personal information protection practices and the information they have about individuals.

The *Privacy Act* could require each federal public body to publish key information in an online, accessible, searchable personal information registry. Such a registry could contain the same type of information that is available through the current personal information bank regime, but in a more user-friendly format. It could also add further information such as summaries of privacy impact assessments, details about information-sharing agreements, and up-to-date personal information notices detailing how the information is used and disclosed in the context of specific programs and activities. In addition, to ensure that the information currently included in a personal information bank is easier to access and understand, federal public bodies could be required to publish an overview of their general practices that is accessible and in plain language in the personal information registry, similar to a privacy policy. Many federal public bodies already follow this best practice, publishing on their websites a general description of their privacy practices and commitments.

Other new obligations aimed at ensuring greater transparency could include:

- ***Enhancing transparency around indirect collections and secondary uses***: The Act could contain new rules to clarify how a federal public body could satisfy a new "Identifying purposes" principle when there is no opportunity to notify an individual of the purposes for collecting personal information (for example, when indirect collection of personal information is authorized or when personal information is collected for new purposes not known or foreseen at the time of a direct collection). In these cases, a federal public body could be required to publish an updated "personal information notice" in the registry.
- ***New proactive publication requirements***: Federal public bodies could be required to publish their privacy management programs and any privacy impact assessments they carry out. As well, they could be required to publish annually information prescribed in regulations or government policy pertaining to all new information-sharing agreements entered into and all existing information-sharing agreements actively utilized each year.

Some exceptions to these transparency requirements would be necessary for specialized public sector activities such as law enforcement investigations, intelligence gathering, and national security activities. Where the publication of sensitive operational information is not possible, specific record-keeping requirements could be imposed to allow the Privacy Commissioner or other relevant review or regulatory bodies to play an oversight role.

For additional details and a more in-depth discussion on the rationale for these suggested changes aimed at modernizing the Act's transparency regime, please consult our more detailed annex here.

10. Fostering open dialogue and providing publicly accessible guidance

The Privacy Commissioner could be given additional powers to provide the public with information and guidance on what the* Privacy Act *requires and how it is enforced

Openness about the operation of the *Privacy Act* and how it is enforced is important. All key participants in the system – the public, federal public bodies, and the **Privacy Commissioner** – benefit when clear information about what the Act requires and how it is enforced is widely available.

The *Privacy Act* could provide the Privacy Commissioner with the authority to engage in public education, as the Commissioner does under the ***Personal Information Protection and Electronic Documents Act***. The Act could also provide the Commissioner with the power to issue guidance on the interpretation and enforcement of the Act, while ensuring that the Commissioner consults with the Government when developing such guidance.

The Privacy Commissioner could also be given the discretion to issue, on request, a non-binding opinion on what position or interpretation the Commissioner would adopt when assessing compliance with the *Privacy Act* in an investigation. Additionally, the Commissioner could be allowed to provide federal public bodies with a "**Regulatory sandbox** " environment, which would allow them to test (with the

Commissioner) whether novel activities would satisfy the Act or could be improved to address potential issues relating to the protection of personal information.

The Privacy Commissioner could also be empowered to disclose more information in the public interest, including decisions on processing access requests and the outcomes of complaint investigations, while ensuring the protection of confidential and sensitive information.

For additional details and a more in-depth discussion on the rationale for these potential changes, please consult our more detailed annex here.

11. Creating an enhanced compliance framework to address unresolved issues

The Privacy Commissioner could be provided with greater powers to more effectively address complaints and the matters for which individuals can seek legal remedies could be expanded

There are a number of reasons to revisit the Act's compliance model. Comprehensive, efficient, and accessible legal remedies are essential for situations where compliance cannot be assured. Moreover, a stronger oversight model could better support new principles-based flexibility for novel scenarios involving personal information. Certain of these suggested changes would mirror amendments made to the *Access to Information Act* in 2019, which provided similar powers to the Information Commissioner of Canada. Aligning the powers of the two commissioners where possible would provide consistency in the processing of requests under both Acts, as well as in the complaint mechanisms for access requests. Proposed changes could include:

- ***Giving the Privacy Commissioner the discretion to decline to investigate a complaint or to discontinue an active complaint investigation***: The **Privacy Commissioner** could be provided with the discretion to decline to investigate a complaint in a number of circumstances, including where a complaint was vexatious, frivolous or made in bad faith, or where the Commissioner deems an investigation to be unnecessary. These could include cases where a complaint was already the subject of an investigation or had already been the subject of a report by the Privacy Commissioner.
- ***Giving federal public bodies the discretion to decline to respond to vexatious or abusive requests for access to personal information***: The Act could also authorize federal public bodies, with the Privacy Commissioner's approval, to decline to process requests for access to personal information under the *Privacy Act* where the request is vexatious, made in bad faith, or otherwise an abuse of the right to make such a request. This would allow federal public bodies to direct resources away from vexatious or abusive requests.
- ***Giving the Privacy Commissioner the power to audit the personal information practices of federal public bodies***: Currently, section 37 of the Act gives the Privacy Commissioner the power to review compliance with the provisions of the Act that govern the collection, use, disclosure, and management of personal information. The Act could replace this with the power to audit the personal information management practices of a federal public body on reasonable notice.

- ***Giving the Privacy Commissioner the power to collaborate with regulatory counterparts in Canada***: The Act could provide the Privacy Commissioner with the power to collaborate with and share information confidentially, including personal information, with other data-protection regulators in Canada and other federal review bodies, where doing so is necessary to advance the Privacy Commissioner's mandate in the public interest.
- ***Requiring the Privacy Commissioner to consult with relevant oversight bodies***: Before issuing findings in a complaint or an audit concerning federal public bodies regulated by other oversight entities, the Privacy Commissioner could be required to consult with relevant oversight bodies to ensure a coherent oversight approach and to avoid duplication of efforts.
- ***Creating an impartial oversight process for complaints against the Office of the Privacy Commissioner of Canada under the* Privacy Act**: The Act does not currently contain an impartial process for complaints made against the Privacy Commissioner's office itself under the Act. To address this legislative gap, the Act could set out a process for independent reviews of such complaints.
- ***Providing the Privacy Commissioner with the power to enter into binding compliance agreements with federal public bodies*:** The Act could provide the Privacy Commissioner with the power to enter into compliance agreements with federal public bodies, consistent with his power to do so under the ***Personal Information Protection and Electronic Documents Act*.** This would be a strong tool to ensure a federal public body met commitments made to the Privacy Commissioner in the context of a complaint investigation, and the Privacy Commissioner could initiate court proceedings if a federal public body failed to comply with a compliance agreement.
- ***Imposing clear statutory timelines for proceedings before the Privacy Commissioner***: The Act could set out clear statutory timelines and other procedural rules to support the efficient resolution of complaints, the conducting of investigations, and the negotiation of compliance agreements.
- ***Providing the Privacy Commissioner with the power to issue orders similar to those of the Information Commissioner***: Where complaints relating to refusals of access to personal information could not be efficiently and effectively resolved through updated resolution mechanisms, the Act could grant the Privacy Commissioner the same order-making powers the Information Commissioner was recently provided with to resolve access complaints under the *Access to Information Act*. This would allow the Commissioner to address the bulk of complaints filed with the Office of the Privacy Commissioner.
- ***Expanding the Federal Court's* de novo *review jurisdiction***: Currently, only refusals to provide access to personal information can be brought before the Court following an investigation by the Privacy Commissioner. The Act could be amended to empower the Federal Court to hear, in addition to refusals of access, matters relating to the collection, use, disclosure, retention or safeguarding of personal information where these could not be successfully negotiated or resolved through the Privacy Commissioner's updated suite of processes and tools.

- ***Adding new offences for serious intentional violations of the Act***: The Act could include offences for wilful violations of the Act that result in harm to individuals.

For additional details and a more in-depth discussion on the rationale for these potential changes to the compliance model under the Act, please consult our more detailed annex here.

Moving the conversation forward

The ideas for public consideration set out in this discussion paper are intended to ensure a strong but flexible public sector personal information protection framework grounded in three foundational pillars: *respect, adaptability* and *accountability*. The ultimate goal is a modernized law that earns and maintains Canadians' trust in respectful and effective digital governance, while positioning federal public bodies to achieve and demonstrate compliance with the strengthened rights and obligations within it.

We welcome your views. You may participate in this consultation by sending general comments in the official language of your choice to privacyactmodernization-modernisationdelaLPRP@justice.gc.ca, or by regular mail to:

Privacy Act Modernization Initiative
Department of Justice Canada
284 Wellington Street
Ottawa, ON
K1A 0H8

ANNEX 1: Introducing new personal information protection principles

1.1 Overview

This annex provides additional detail on integrating new personal information protection principles in the *Privacy Act*. These would largely mirror the ***Personal Information Protection and Electronic Documents Act*'s** 10 principles.

Many stakeholders support introducing principles to the *Privacy Act*. Notably, the **ETHI Committee** recommended that the *Privacy Act* be modified to include generally-accepted and technology-neutral principles similar to those contained in the ***Personal Information Protection and Electronic Documents Act***. As well, Justice Canada's 2019 targeted technical engagement confirmed broad stakeholder support for amending the *Privacy Act* to include personal information protection principles that could support a flexible, outcomes-based compliance regime able to accommodate innovative practices with personal information, diversity in government functions, and risk-based approaches.

A principles-based approach would significantly enhance the *Privacy Act*'s alignment with other domestic and international regimes, support effective regulation of novel situations or innovative practices with personal information, and ensure the *Privacy Act* was clear about its fundamental commitments to individuals. Adding principles would place the foundational concerns that matter most to individuals – whether practices with personal information are reasonable, proportionate, fair, ethical, in the public interest and protective of privacy – at the heart of the legislation.

Personal information protection principles could also assist in addressing unique situations or novel practices in cases where the application of standardized general rules would not lead to the most desirable or appropriate results. New principles could offer a more flexible approach to these kinds of unique situations, which may require a more contextually-sensitive approach to personal information regulation than general rules can offer.

Given important differences between the public and private sectors, however, these principles would be tailored to reflect considerations that are unique to the federal public sector. As such, the Government is not proposing to import precisely the same legal requirements that apply to private sector entities into the federal public sector regime. However, the public and private sectors in Canada would be regulated on the basis of the same core and foundational objectives that the ***Personal Information Protection and Electronic Documents Act*'s** 10 personal information protection principles seek to achieve, namely: proactive accountability; clear specification of purposes; strong consent standards; meaningful collection, use, retention and disclosure limitation standards; protective accuracy and related measures; robust and context-sensitive safeguarding requirements; openness requirements that empower individuals; broad rights of access; and effective oversight mechanisms. The content of the specific rules and requirements supporting the realization of these objectives would be informed by a range of leading domestic and international standards.

1.2 New personal information protection principles based on internationally recognized data protection principles

The protections in Canada's private sector personal information protection legislation, the ***Personal Information Protection and Electronic Documents Act***, reflect established international standards such as those in found in the **Organization for Economic Co-operation and Development's ("OECD")** Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and inspired some key revisions to those guidelines in 2013. These principles are also largely reflected in the European Union's General Data Protection Regulation. They also form the foundation of the ***Personal Information Protection and Electronic Documents Act's*** "substantially similar" regime, which supports consistency in private sector data protection across Canada. The ten core concepts around which the ***Personal Information Protection and Electronic Documents Act*** protections are structured represent a useful starting point for new public sector personal information protection principles.

New *Privacy Act* personal information protection principles could be organized around the 10 principles set out under the ***Personal Information Protection and Electronic Documents Act***. Aligning new principles in the *Privacy Act* with the objectives that animate the ***Personal Information Protection and Electronic Documents Act's*** 10 principles would confirm equivalent protections across the public and private sectors in Canada. This approach also offers an opportunity to: (i) align Canada's public sector personal information protection framework with leading international standards; (ii) simplify the federal personal information protection framework for individuals by organizing it around the same core objectives; and (iii) introduce into the *Privacy Act* the foundational and broadly recognized data protection principles that inspired many of its more precise rules.

1.3 Personal information protection principles for the *Privacy Act*

As mentioned above, the idea of adding federal public sector personal information protection principles to the Act is grounded in certain design principles – interoperability with leading international and domestic standards; consistency with broader Canadian legal frameworks applicable to public sector institutions; and strong technological neutrality. The objectives addressed by the personal information protection principles in the ***Personal Information Protection and Electronic Documents Act*** are a starting point. However, the specific standards that new personal information protection principles would set for federal public bodies could be modified from those that the ***Personal Information Protection and Electronic Documents Act*** imposes on private sector organizations to reflect the unique public sector context in which the *Privacy Act* operates, the current provisions of the Act, and its legislative role and history. Doing so could ensure a strong underlying informational privacy protection framework that reflects Canadian values and norms, does not unduly hamper innovation or practices, and is ultimately in the public interest.

Accountability

An "Accountability" principle could be introduced to support new accountability mechanisms that would require federal public bodies to proactively demonstrate the approaches they take to ensuring compliance with the Act. An Accountability principle could confirm a federal public body's accountability for all personal information under its control, including personal information transferred to third parties for processing on its behalf. A new Accountability principle would, however, have to be compatible with the legal and policy frameworks that already guide accountability in the public sector context.

Identifying Purposes

A new "Identifying purposes" principle could require a federal public body to clearly indicate the purposes for which personal information will be collected, used and shared. The *Privacy Act* currently contains a rule requiring government institutions to inform individuals of the purpose for which the information is being collected, with some exceptions for cases where personal information may be collected indirectly. In the public sector context, federal public bodies currently typically communicate their purposes for collecting personal information through a "Privacy Notice". Introducing a new "Identifying purposes" principle would support existing approaches, ensure principles-based compliance was equally transparent, and confirm the need to identify and communicate this important information to individuals in clear and accessible ways.

Consent

In the federal public sector personal information protection framework, the authority to collect, use or disclose personal information comes primarily from laws, rather than individual consent. This is, in part, because there are many public functions for which it would be impossible to secure meaningful and voluntary consent, or inappropriate to ask for consent (e.g. the information sought is mandatory or seeking consent would defeat the purpose of the collection, such as in the context of a law enforcement investigation). However, the *Privacy Act* recognizes an individual's consent as a valid source of authority in certain circumstances, such as for new uses of personal information or for a particular disclosure. Introducing a "Consent" principle into the *Privacy Act* could confirm the general standards associated with securing a valid consent for *Privacy Act* purposes in these circumstances.

Limiting Collection

The *Privacy Act* could add a "Limiting collection" principle to restrict the types and amount of personal information federal public bodies may collect. A federal public body would be limited to collecting only the personal information reasonably required to achieve a purpose relating to its functions and activities, unless otherwise authorized by Parliament. The principle would be complemented by more specific provisions outlining a collection threshold, and providing factors to assess whether a collection was "reasonably required" that would emphasize the need for a proper balance between effectively accomplishing a federal public body's legitimate public objectives, and respecting the rights and interests of individuals. Despite using different language from what is found in other data protection instruments, in practice, this collection standard would be essentially equivalent to leading international

standards. It would also recognize and accommodate the unique roles and responsibilities of federal public bodies, relative to private sector organizations.

Limiting Use, Disclosure and Retention

A new "Limiting use, disclosure and retention" principle in the *Privacy Act* could be organized around the baseline requirement that all uses and disclosures of personal information would have to be specifically authorized by the Act, and where it was not, would have to be reasonably required for a purpose in the public interest. As a result, consent and other authorities for using or disclosing personal information set out in the Act would be examples of specifically authorized practices that would satisfy this principle.

The principle could also be based on what is reasonably required in all the circumstances and supported by specifically authorized retention practices. Specialized rules to support appropriate retention practices could specifically authorize retention in accordance with regulations under the Act, to facilitate individual access rights, to satisfy archival requirements, and in accordance with other legal requirements, for example.

Accuracy

The existing accuracy provision in the *Privacy Act* is already quite "principle-like". Under the current Act, a government institution must "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" (subsection 6(2)). An "Accuracy" principle could broaden the application of this requirement to personal information that could have a direct impact on an individual, consistent with an expanded definition of an administrative purpose.

Safeguards

The *Privacy Act* does not currently contain express provisions requiring security safeguards to be applied to a federal public body's personal information holdings, although such requirements are found in TBS policy. The Act could include a principle for federal public bodies to apply appropriate physical, organizational and technological measures, depending on the sensitivity of the data and the potential risk to individuals. This approach could be supplemented by more detailed statutory rules, new regulations and/or operational guidance from the designated Minister.

Openness and Transparency

An "Openness and transparency" principle could ensure that individuals are able to obtain specific information about a federal public body's policies and practices with respect to the management of personal information, presented in the most straightforward manner possible. A public sector "Openness and transparency" principle could be supported by a range of mandatory requirements that would give consistent effect across government to its important goals. New transparency requirements in support of this principle would complement and not replace federal public bodies' existing obligation to respond to specific requests for information under the *Privacy Act* and the *Access to Information Act*.

Individual Access

The *Privacy Act* already contains a complete code of mandatory rules governing individuals' rights to obtain access to their personal information. Further to these rules, the government receives and responds to about 75,000 personal information requests per year. Existing rules would be retained and eventually aligned to the extent appropriate with the mirror provisions under the *Access to Information Act*, as the review process of that legislation progresses. Federal public bodies' compliance with these rules would continue to be mandatory. A new public sector "Individual access" principle could, however, confirm and complement the right of access to personal information already recognized in the Act, and allow corollary rights to challenge accuracy and completeness.

Challenging Compliance

The *Privacy Act* already contains a complete code of mandatory rules to guide federal public bodies when complaints are filed with the Privacy Commissioner. These rules could be retained and federal public bodies' compliance with the specialized procedures set out under the Act would continue to be mandatory. A public sector "Challenging compliance" principle could confirm the importance of effective recourse mechanisms under the Act.

1.4 Personal information protection principles working with supporting provisions

While there has been broad support for a shift to a principles-based approach to *Privacy Act* compliance, many stakeholders have cautioned that broad principles should be supported by more detailed rules that can offer clearer and more specific direction with respect to compliance requirements. This can provide federal public bodies with greater regulatory certainty and support their compliance efforts.

The existing rules in the *Privacy Act* offer the strongest and most obvious starting point. These rules are very comprehensive, they have been in place for more than 35 years and they offer strong certainty around compliance requirements. While some of the existing provisions could be modernized and there are opportunities to introduce into the Act new individual rights and institutional responsibilities, the proposed shift to a principles-based approach would be designed to retain and work in tandem with the current framework.

Modernized versions of the current provisions in the *Privacy Act* along with some new legal requirements would supplement new personal information protection principles. This modernized framework of rules would provide detailed guidance about how to undertake particular practices in compliance with the Act and a related principle.

For example, the Act could expressly identify particular collection practices that, where followed, would meet the requirements of a new "Limiting collection" principle. This approach would allow the principles and the rules to work together effectively. The role of the principles would be to state the foundational and core requirements of the Act and provide space to address novel scenarios. The role of the rules would be to identify, in a clear and express way, how the requirements of the principles could be met in the context of commonplace scenarios and standard practices.

Under this approach, modernized versions of the existing rules would no longer state the only ways in which federal public bodies could comply with the law. Rather, these provisions could identify specific practices that comply with the associated principles or that constitute necessary, specific, and limited exceptions. The Act could also explicitly state that compliance with modernized rules would satisfy the requirements of the associated principle, or be accepted as a specifically authorized exception.

1.5 Reliance on new principles for novel scenarios: principles-based compliance

In order to gain the advantages that a principles-based approach offers, new personal information protection principles for the *Privacy Act* could allow federal public bodies to help address unique or unforeseen circumstances, with supporting provisions in the Act, such as when the rules could not be effectively applied to new technologies or when highly unusual situations arose.

This would support innovation in government, help to ensure effective regulation of novel practices or unusual situations, and position the *Privacy Act* to be a highly adaptive and future-oriented personal information protection law consistent with the principles-based approaches that are common internationally. Enhanced oversight and new accountability requirements would support federal public bodies to carefully manage complex and novel scenarios, as long as federal public bodies were respecting the Act's overarching personal information protection principles.

1.6 Public reporting and dialogue around principles-based compliance

In addition to the Privacy Commissioner's oversight of principles-based practices with personal information, annual reporting and centralized tracking could support important public dialogue around how the *Privacy Act* might be updated over time. As clarity around legal compliance for novel practices eventually settled around the Act's foundational principles, new supporting rules could be added to integrate a once novel practice's regular use through future legislative reviews.

ANNEX 2: A new and updated framework on the collection, use, disclosure and retention of personal information

2.1 Overview

This annex provides additional discussion about the ways in which the *Privacy Act*'s rules on the collection, use, disclosure and retention of personal information could be modernized to promote respect for individuals and their informational privacy rights.

2.2 A strengthened framework for the collection of personal information

To support compliance with a new "Limiting collection" principle, the current collection rule under section 4 of the Act could be updated to reflect longstanding government policy, ensure essential equivalency with international approaches and provide federal public bodies with more flexibility to carry out their missions in a responsible manner.

Section 4 of the *Privacy Act* currently reads as follows: "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution." In line with a new "Limiting collection" principle, the Act could update the current collection threshold that requires a direct link to an operating program or activity to provide that a federal public body could only collect personal information where the personal information was reasonably required for a federal public body's functions or activities. The Act could also permit the collection of personal information under another threshold that is outlined in another act of Parliament.

This framework could also include key considerations that federal public bodies would have to take into account in determining whether a collection was "reasonably required", including: (i) the specific purpose for the collection, including whether the collection is for law enforcement purposes; (ii) the mechanisms or means employed to collect the information; (iii) whether there are less intrusive means of achieving the purpose at a comparable cost and with comparable benefits to the public; and (iv) the degree of intrusiveness of the collection as compared to the public interests at play.

There are potential risks to including a "reasonably required" standard in the collection threshold. Using terms such as "required" or "necessary" could lead to a strict interpretation by the courts or the Privacy Commissioner of the ordinary meaning of such terms, such that they may not sufficiently accommodate or guide the use of important emerging technologies. For example, some Canadian commissioners have queried whether a test requiring personal information for a specific purpose can have meaningful application in the context of big data[2] and artificial intelligence applications.[3] A leading international

[2] https://www.ipc.on.ca/wp-content/uploads/2017/05/bigdata-guidelines.pdf : "To allow for big data-type practices in general, a new or modified legislative framework is needed."

[3] https://priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/: "Based on our own assessment, AI (artificial intelligence) presents fundamental challenges to all foundational privacy principles as formulated in PIPEDA (*Personal Information Protection and Electronic Documents Act*). For instance, the data protection principle of limiting collection may be incompatible with the basic functionality of AI (artificial intelligence) systems."

think tank[4] has also identified this concern. Given the ways in which big data and artificial intelligence work, more and more information may very well be reasonable for the best and most reliable public outcomes but nevertheless not be in any way "required" or "necessary".

At the same time, interpreting what is "required" too narrowly may mean that larger societal interests supported by technological advancements are not well served. Some stakeholders have made the point that it is not always clear that a piece of personal information may be required, or necessary, for a federal public body to effectively carry out its functions. For law enforcement investigations specifically, it is not always possible to know or identify in advance what information is required, and is an example of a specialized activity that may require dedicated rules.

In light of this tension, a more flexible and creative approach to interpreting what is "reasonably required" is being considered. A new framework that includes a list of factors to consider to determine whether personal information is "reasonably required" should be sufficiently flexible to address the inherent interpretive challenges of using unqualified terms such as "necessity", and to allow federal public bodies to collect personal information for more innovative purposes. As well, providing Parliament with the flexibility to authorize the collection of personal information through other legislation could be an additional tool to allow federal public bodies to adapt to new circumstances. It could allow the government to adapt to other specific scenarios or technologies in the future where a "reasonably required" standard could impede the government's ability to carry out its work in the public interest.

Such an approach could also shift the orientation of the collection framework away from specific programs and activities, and assist in breaking down institutional silos. Such a shift would better accommodate federal public bodies and Ministers responsible for cross-cutting mandates and would support program efficiencies within federal public bodies. As well, an updated collection threshold should support approaches to the delivery of public services based on a "tell us once" model for information collection that limits the amount of information collected by government in the first place and is more efficient for individuals. Allowing for more integrated and efficient collection activities across programs and between departments could help ensure that an individual's personal information remains relevant, current and accurate both within and across federal public bodies.

Finally, unintentional, unsolicited and temporary collections could be addressed by way of specialized rules clarifying how to ensure compliance with a "Limiting collection" principle in these specific circumstances. The Act could clarify that, for cases where federal public bodies unwillingly or unknowingly receive personal information they do not require, they would be required to delete the information or return it.

[4] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf: "For AI, particularly at the development and training stages, what is necessary is a considerable amount of data, and having too little data can hinder the development of an algorithm. For instance, the collection and retention of significant amounts of data, including sensitive data, may be necessary to mitigate the risks and ensure fairness in certain AI applications. This is a contextual trade-off which organizations will need to assess carefully in order to strike an appropriate balance between competing requirements." (p. 18).

2.3 Updating the framework for secondary uses and disclosures of personal information

The proposed "Limiting use, disclosure and retention" principle could also be supplemented by specifically authorized uses and disclosures updated to ensure consistency with this new personal information protection principle.

The circumstances in which personal information may be used and disclosed without seeking an individual's consent are currently set out in sections 7 and 8 of the *Privacy Act* respectively. These provisions reflect the complex public policy choices Parliament confronted when seeking to craft a legislative framework of general application to govern the protection of personal information by what are now approximately 265 federal institutions with unique mandates, informational needs and inter-jurisdictional partnerships. Through these provisions, Parliament made public policy choices seeking to reconcile the importance of protecting individuals' informational privacy and the need to permit responsible uses and disclosures of information in support of legitimate public purposes. Furthermore, transparency measures will be key to ensuring individuals understand how their personal information will be used, disclosed and retained – these are further discussed in the Annex entitled *A renewed accountability model and new tools for meaningful transparency*.

Clarifying "consistent use" in the use and disclosure framework: The *Privacy Act* could define "consistent use" flexibly, in a way that aligns this Canadian concept with the European approach to "compatible uses". A consistent use would thus be determined with reference to criteria designed to highlight the appropriate considerations, including the link between the original and the updated purpose; the context in which personal information was originally collected; the nature of the personal information; possible consequences and benefits for individuals; and the existence of appropriate safeguards or risk mitigation measures. The Act could provide a list of examples of what would constitute a consistent use, which could include where the use or disclosure is required to more effectively assess eligibility for a service or benefit requested by an individual, or to be able to effectively provide that service or benefit (which would limit the instances individuals would have to provide the same information to different federal public bodies for the same purpose), or to confirm an individual's identity by verifying and authenticating information against other personal information held either elsewhere in the federal public body, or within another federal, provincial or territorial public body.

Clarifying 8(2)(c): Paragraph 8(2)(c) permits the disclosure of personal information in support of the operations of courts and tribunals. Paragraph 8(2)(c) could be amended to clarify that a federal public body may disclose personal information for these purposes both: (i) where it is legally required to do so (e.g. when it is a party to such proceedings); and (ii) where a federal public body wishes to exercise discretion to disclose personal information that is relevant to an ongoing or reasonable anticipated court or tribunal process, even though the institution may not be legally bound to do so.

Aligning 8(2)(e) with analogous provisions in the Personal Information Protection and Electronic Documents Act: Paragraph 8(2)(e) permits a government institution to disclose personal information to

prescribed investigative bodies for law enforcement and investigation purposes. Regular reorganization and restructuring within government organizations has made this model, which depends on designations by way of regulations, difficult to maintain from an operational perspective. A legislated definition of an "investigative body", as opposed to a list in a schedule to the Act, could be added to the Act. This paragraph could also be amended to enhance its consistency with the requirements of the ***Canadian Charter of Rights and Freedoms*** that may be triggered where an individual has a reasonable expectation of privacy in the personal information at issue.

Strengthening accountability for information sharing under 8(2)(f): Currently, paragraph 8(2)(f) of the Act permits the disclosure of personal information in accordance with information sharing agreements or arrangements between a number of the entities identified in that section, for the purpose of administering or enforcing any law or carrying out a lawful investigation. These entities include provincial and territorial governments, certain councils of First Nations, foreign governments, and foreign organizations of states.

The information-sharing framework under this provision could be modified to distinguish between information sharing with other federal public bodies, provincial and territorial governments, Indigenous governments and foreign governments for purpose of administrating or enforcing a law. Furthermore, an obligation to have all information-sharing agreements or arrangements in writing could be imposed, although there would be an ability to share personal information in urgent or *ad hoc* cases where an information-sharing agreement could not reasonably be drafted in advance, as long as certain specific requirements were met.

The types of clauses that information-sharing agreements or arrangements would have to include at a minimum could be set out in either the Act, regulations or enshrined in government policy, and they would vary depending on whether the recipient entity was another federal public body, another government in Canada, or a foreign government. Such clauses could include, for example, the purpose for sharing the information, a description of the personal information being shared, the safeguards that will apply to protect the information and minimise interference with privacy, limits on further use and disclosures, and penalties for non-compliance.

Strengthening accountability under 8(2)(g): Paragraph 8(2)(g) authorizes the non-consensual disclosure of personal information by a government institution to a Member of Parliament. It is generally used to support MPs to assist their constituents to interface with federal public bodies. With the speed and ubiquity of digital communications today, it is no longer clear that individuals require this support on a non-consensual basis in order to obtain timely assistance from their MPs – in most cases, an individual could now readily provide or confirm their consent to such a disclosure. As such, this exception could be removed from the Act.

Broadening "audit purposes" under 8(2)(h): Paragraph 8(2)(h) enables disclosures to support (i) internal, (ii) centralized (e.g. through the **Office of the Comptroller General**), and (iii) external auditing of government institutions. In view of the importance of facilitating the review of federal public bodies' compliance with a broad range of horizontal policy and program responsibilities beyond just sound

financial management, paragraph 8(2)(h) could be broadened accordingly. It could be extended to support compliance with other important public sector commitments like program effectiveness and integrity, gender-based plus (GBA+) analysis, results and delivery outcomes, and risk management results, for example. The relevant centralized and prescribed recipients would need to be modified as applicable and appropriate.

Mirroring paragraph 8(2)(i) for Statistics Canada: Statistics Canada could benefit from the same type of clear and express provision that exists in paragraph 8(2)(i) of the Act to support disclosures to the Library and Archives of Canada for archival purposes. A specific provision could be added to include Statistics Canada as an analogous recipient institution of personal information for "statistical and research purposes".

Strengthening clarity and accountability under 8(2)(j): Paragraph 8(2)(j) permits the disclosure of personal information to any person or body for research and statistical purposes. This provision could be amended to clarify the scope of its intended application, particularly in light of the scale and breadth of data analytics that are possible today. In addition to this clarification, the head of an institution authorized to approve disclosures under 8(2)(j) could also be required to specify conditions relating to data security and confidentiality in disclosure agreements. These amendments would better align 8(2)(j) with approaches in many other jurisdictions.

Adding an additional authority permitting data integration activities for certain purposes: There is enormous public benefit to allowing the Government to share, link, and analyze data to obtain new insights to support service-delivery initiatives, policy development, system planning, resource allocation and performance monitoring. Doing so can provide the Government with higher quality evidence, can lead to better public policy development and more sound uses of public funds, and can minimize cases of abuse or fraud.

In order to support these goals, the Act could add a specific authority to use or disclose personal information to a dedicated unit within another federal public body to allow for the analysis of information in relation to the management or allocation of resources, the planning for the delivery of programs and services provided or funded by the Government of Canada, and the evaluation of such programs and services in certain circumstances. This type of information sharing could be subject to certain limits and conditions, including that other information could not serve the specified purposes and only the personal information that is reasonably required for the specified purposes could be used or disclosed, and that the head of federal body using or receiving the information for such purposes would have to certify that the use or disclosure would be in the public interest.

Adding additional authorities for emergencies, to prevent threats to public safety and individuals, and to contact next of kin: Unlike many other public sector personal information protection acts, the *Privacy Act* does not expressly authorize the use or disclosure of personal information in emergencies, to ensure public safety or the safety of individuals, or to notify next of kin in certain circumstances. To address this, the Act could add additional authorities permitting use or disclosure where doing so is reasonably required in cases of emergency, to prevent or reduce a serious threat to public, or an individual's, safety

or health, to protect the safety or health of an individual, and to contact a relative or any other person whom it would be reasonable to contact when an individual is injured or ill.

Using or disclosing publicly available personal information: The Act could add specialized rules for using or sharing "publicly available" personal information to clarify and support the application of new personal information protection principles to publicly available personal information, and to align public sector use and disclosure of publicly available personal information with individuals' reasonable expectations of privacy. At the same time, the Act could ensure sufficient consistency between its approach to publicly available personal information and that of the *Access to Information Act* – the *Privacy Act* should not protect publicly available information in a way that is incompatible with the public's right to access it under the *Access to Information Act*.

Amendments to accommodate changes to the definition of "personal information": In line with the idea of removing the current list of exemptions under paragraphs j) to m) of the definition of "personal information", additional authorities could be added to allow federal public bodies to use and disclose the type of information covered by the current exemptions. This includes information that relates to the position or functions of an employee or agent of the federal public body, certain information about ministerial staff, information about an individual performing services under a government contract where the information relates to the services performed, information relating to discretionary benefits of a financial nature, and information about an individual who has been deceased for more than 20 years.

Providing flexibility for unforeseen circumstances: Currently, paragraph 8(2)(m) of the Act permits the head of a federal public body to disclose personal information for any purpose where: (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or; (ii) the disclosure would clearly benefit the individual to whom the information relates. In order to ensure that the Act can provide flexible protection in the face of ever changing circumstances and technology, a reorientation around this approach could be considered. Potential new authorities for using or disclosing personal information in emergency circumstances, to protect public safety and to notify family in certain cases would address many of the scenarios contemplated by the current subparagraph 8(2)(m)(ii) of the Act.

For instance, paragraph 8(2)(m) of the Act could be eliminated and replaced with a new framework for further uses and disclosures not specifically authorized under this part of the Act, but that would respect the new "Limiting use, collection and retention" principle. A new provision could be added to permit a further use or disclosure of personal information for a purpose not specifically authorized under the Act where the head of a federal public body determined that doing so would be "reasonably required" in the public interest. As with the Act's updated collection threshold, this framework would identify key considerations that the head of a federal public body would have to take into account in determining whether another use or disclosure was "reasonably required", including: (i) the nature and specific purpose for the use or disclosure; (ii) the mechanisms or means employed to share the information; (iii) whether there are less intrusive means of achieving the purpose at a comparable cost and with comparable benefits to the public; (iv) the degree of intrusiveness of the use or disclosure as compared

to the public interests at play; (v) and how the information would be safeguarded to mitigate potential privacy impacts. Associated record-keeping requirements for such decision could be imposed to allow the Privacy Commissioner the opportunity for meaningful review.

2.4 Introducing a principles-based approach to retaining personal information

The current rules around the retention of personal information are inflexible – they require federal public bodies to retain personal information used in a decision-making process affecting the individual for typically two years. The intent behind this requirement was to ensure that the individual to whom the information relates has a reasonable opportunity to obtain access to this information.

However, experience has shown that complying with strict prescribed retention periods can sometimes prevent federal public bodies from safely disposing personal information when doing so may be more privacy protective than hanging on to the information. The Act could impose an obligation for federal public bodies to retain personal information for only as long as reasonably required to effectively carry out the purpose for which it was collected in the first place, providing flexibility to adapt their retention practices to the unique circumstances of each case.

This new obligation could be supported by including a list of specifically authorized retention practices that confirmed when it would be appropriate for a federal public body to retain personal information for longer than required for the purposes for which it had been collected. Examples of such authorized practices could include archival purposes, responding to access to personal information requests, and complying with other legal obligations.

ANNEX 3: A renewed accountability model and new tools for meaningful transparency

3.1 Overview

Enhancing accountability through new and regularly updated data governance mechanisms, improved transparency measures, a supportive compliance framework and stronger oversight is the third foundational pillar of a modernized *Privacy Act*. These improvements can help federal public bodies enhance their internal decision-making processes, capacity and expertise; promote effective dialogue between federal public bodies and the Privacy Commissioner; and ultimately promote trust in the operations of the *Privacy Act* as a whole.

This annex discusses a range of new tools for meaningful accountability and transparency, responsibility, and oversight that could be introduced into the *Privacy Act* in support of enhanced accountability.

3.2 New mechanisms for strong data governance grounded in continuous improvement

The following could support federal public bodies to develop strong internal privacy expertise and capacity so they are well positioned to proactively manage their own unique data protection issues, including novel scenarios that may present. Integrating into the *Privacy Act* a preventive, proactive, and systematic approach to compliance and risk mitigation would ensure federal public bodies can learn and continuously improve, even absent complaints or investigations.

Demonstrating accountability: The *Privacy Act* could be amended to introduce an "Accountability" principle modeled on best practices supported by other domestic and international data protection instruments. This principle could form the basis of new requirements for federal public bodies to proactively demonstrate the approaches they take to ensuring compliance with the personal information protection principles. As in the case under the ***Personal Information Protection and Electronic Documents Act***, it could also confirm that a federal public body is accountable for all personal information under its control, including personal information transferred to third parties for processing on its behalf.

Developing and maintaining privacy management programs: The Act could introduce a requirement for federal public bodies to create and maintain a privacy management program. This would constitute a concrete mechanism that federal public bodies could use to proactively take charge of and demonstrate their own compliance in accordance with an "Accountability" principle. A privacy management program could serve as the main and organizing mechanism to guide compliance with other accountability measures, like new **privacy impact assessment** requirements. It would allow federal public bodies to demonstrate that they act in accordance with new and existing accountability requirements. The Act could include the minimal components of a privacy management program, such as a list of officials responsible for privacy within the federal public body, inventories of personal information under the control of the federal public body, the policies and procedures in place to protect personal information. Elements of a privacy management program could also be supplemented or added to by **Treasury Board Secretariat** policy instruments. Federal public bodies could also be responsible under the Act for

transforming the elements of a privacy management program into an individualized data governance tool that was reflective of an institution's size, structure, and role, along with the volume and nature of its personal information holdings. A legislative requirement to regularly review and update privacy management programs could also be included.

Chief Privacy Officers: While the head of a federal public body would ultimately be accountable for the administration of the Act within that institution, the Act could nonetheless require a federal public body to designate an individual or individuals responsible for supporting its compliance with the Act. Some government institutions have already taken the step of naming a Chief Privacy Officer in recognition of the important role internal expertise and leadership plays in supporting a culture of compliance. While the particular job title and relationship with other officials' functions could differ by federal public body, a consistent approach to designating a particular official to guide an institution's compliance with the Act and undertake certain functions would foster benefits within every federal public body. This will be particularly important in the context of a *Privacy Act* undergoing comprehensive modernization that will introduce a range of new compliance obligations with flexibility around how they may be met.

New record-keeping requirements: In keeping with a new "Accountability" principle, existing requirements to notify the Privacy Commissioner of "consistent use" and "public interest" disclosures could be transformed into record-keeping requirements. In addition, federal public bodies could be specifically required to document a range of other matters, including requests made to private sector organizations under paragraph 7(3)(c.1) of the ***Personal Information Protection and Electronic Documents Act***. These records could be subject to the right of access under the Act, and the Privacy Commissioner's oversight powers.

3.3 More meaningful government transparency

Transparency can mean openness – namely, that an individual can easily obtain information about how personal information is collected, used, retained and disclosed by an institution. But openness alone does not generate meaningful transparency: the information that is available should also be written, organized, and presented in ways that can be readily understood by the people to whom it relates or who might need or want it.

The following discussion centres on introducing new openness requirements that are specifically designed to meet the needs and interests of individuals who are seeking to understand an institution's practices with personal information.

Making transparency measures more accessible and user-friendly – a new Personal Information Registry: Current requirements for institutions to publish information about their collection and holdings of personal information ("personal information banks" or "PIBs") date from the time when personal information was secured in paper files. To modernize the transparency regime, the *Privacy Act* could include a broad requirement for each federal public body to publish key information in an online, accessible, searchable Personal Information Registry, which could contain:

- Descriptions of personal information that is collected by federal public bodies, the legal authority under which it is collected, how that information is used within a federal public body, and with which other entities it is shared;
- Summaries of Privacy Impact Assessments;
- Summaries of information sharing agreements and supporting details; and
- Other information, such as Privacy Notices where direct communication with individuals is not required (e.g. for indirect collection or legally authorized secondary uses of personal information).

The Personal Information Registry could be designed to offer a comprehensive and standardized compilation of important information, which federal public bodies would be free to complement or supplement through other, individualized transparency measures.

Maintaining a proper balance between legislative requirements and supplemental policy instruments is important. The Act could identify a requirement to contribute designated information to a Personal Information Registry and/or the core information that federal public bodies might be required publish in a new Personal Information Registry. Additional elements for publication in a Personal Information Registry could be specified in policy instruments under the authority of the Designated Minister. Supporting a foundational requirement to contribute documentation to a Personal Information Registry with additional requirements and operational details to be set out in policy could allow flexibility over time as approaches and tools change.

A layered and user-friendly summary of personal information protections: To ensure that technical information of the sort currently included under the existing "personal information bank" regime is made more comprehensible and accessible to individuals, federal public bodies could be required to publish a plain language and accessible overview of their general practices in the Personal Information Registry. Many government institutions already follow this best practice, publishing on their websites a general description of their personal information practices and commitments. This information is akin to an institution-specific privacy policy or charter. This practice could be coordinated across government and included in the Personal Information Registry. The goal would be to offer a preliminary source of general and accessible information under which the more detailed and technical information available through the Personal Information Registry could be layered.

Enhancing transparency around indirect collections and secondary uses: The *Privacy Act* could contain new rules to clarify how an institution could satisfy a new "Identifying purposes" principle when the opportunity to provide a Privacy Notice directly to an individual does not arise. This would occur when the Act authorized an indirect collection of personal information or in some cases when personal information was collected for new purposes that were not originally foreseen at the time of a direct collection. In such cases, an institution could be required to publish an updated Privacy Notice in the Personal Information Registry according to the same accessible communications standards that would apply when communicating with an individual directly.

Publishing Privacy Management Programs: Since privacy management programs would constitute a core component of a government institution's compliance regime, a new transparency regime could require that they, or parts of them, be published or otherwise made available to the public for review within the Personal Information Registry framework.

Completing and publishing Privacy Impact Assessments (PIAs): **Privacy impact assessments,** or as they are generally called, PIAs, are detailed reviews of identified privacy risks and the measures aimed at mitigating them. However, PIAs take a lot of time and public resources to undertake. Introducing into the *Privacy Act* a risk-based legal requirement to complete a PIA could help enhance compliance with the Act. The Act could impose an obligation on federal public bodies to conduct a PIA with respect to new programs or activities, or substantially modified programs, that involve the collection, use or disclosure of personal information for administrative purposes, for automated or manual profiling activities, where sensitive personal information is involved, or other activities involving a high risk for personal information as otherwise mandated by Government policy. The Act could also require federal public bodies that prepare a PIA to provide a copy to the Privacy Commissioner for views and recommendations, which the Privacy Commissioner would have to provide within a mandated timeline. Federal public bodies would have to include an explanation in their finalized PIAs, or in their annual reports, as to why recommendations from the Privacy Commissioner were not adopted. Given that some PIAs are quite lengthy, and some may not be published for operational reasons relating to law enforcement, intelligence gathering or protecting national security, or other sensitive government functions, summaries of PIAs could be proactively published. Government policy could further delineate the form and specific content of what would be included in a PIA.

Transparency around information-sharing agreements: Information-sharing agreements facilitate flows of personal information and legal protections around them. Given the key role information-sharing agreements play in the federal public sector, enhanced transparency around them is important. The *Privacy Act* could require a federal public body to publish, on an annual basis, prescribed information pertaining to all new information-sharing agreements it entered into and all existing information-sharing agreements it actively utilized each year. This information could be made available to the public by way of the Personal Information Registry.

Exceptions for sensitive government functions: If they were uniformly imposed for all government functions, many of the foregoing transparency measures could compromise the integrity of sensitive public sector activities like law enforcement investigations, intelligence gathering, and national security activities. Targeted exceptions to new transparency requirements would be required. Where proactive publication of information was not possible because of its sensitive nature, record-keeping requirements subject to the Privacy Commissioner's oversight could serve as an accountability substitute. The "exempt bank" regime and the Privacy Commissioner's powers to oversee it could also remain as a model, with appropriate modifications in light of changes to the personal information bank regime being considered.

ANNEX 4: A new oversight framework for the *Privacy Act*

4.1 Overview

A supportive compliance framework and stronger oversight forms part of the third foundational pillar of a modernized *Privacy Act*. Certain improvements to the Act could help promote effective dialogue between federal public bodies and the **Privacy Commissioner**, and where required, provide the Privacy Commissioner with additional powers to ensure compliance.

The **Privacy Commissioner** is an agent of Parliament. This means that the Privacy Commissioner is responsible directly to Parliament rather than to the government or a federal minister, which emphasizes his or her independence from the government of the day. The Privacy Commissioner is also an "ombudsperson". This means that the Privacy Commissioner has broad powers to receive and investigate complaints, but does not have the authority to issue mandatory orders. The Privacy Commissioner's existing ombuds-role has served Canadians well for over 35 years. It has provided a relatively efficient and resource-friendly way to address complaints under the Act, it supports important dialogue between the Privacy Commissioner and federal public bodies, and has resulted in effective, negotiated solutions to complex issues in the vast majority of cases complaints have been made under the Act. It also supports access to justice for individuals, who benefit from a less formal process before the Privacy Commissioner to advance their complaints, and the possibility of having the Privacy Commissioner advance proceedings before the Federal Court on their behalf.

However, there are a number of reasons why the Act's enforcement model might be revisited. Comprehensive, efficient, and accessible legal remedies are essential for situations where compliance cannot be assured by other means. A stronger oversight model is also appropriate in an Act that could include new principles-based flexibility for novel scenarios and new practices with personal information.

This annex describes a range of new tools for meaningful oversight that might be introduced into the *Privacy Act*.

4.2 Fostering open dialogue and publicly accessible guidance

Greater openness around the operation of the *Privacy Act* and how it is enforced is important. All key actors in the system – the public, federal public bodies, and the Privacy Commissioner - could benefit when clear information about what the Act requires is broadly and consistently available. Some of these ideas for changes to the Act would align the Privacy Commissioner's powers with those under the ***Personal Information Protection and Electronic Documents Act***, while others are more novel ideas to help foster greater dialogues between federal public bodies and the Privacy Commissioner in the federal public sector context. Such potential changes could include:

A public education mandate for the Privacy Commissioner: The *Privacy Act* could include a formal power for the Privacy Commissioner to engage in public education activities aimed at the general public,

as the Commissioner currently can under the ***Personal Information Protection and Electronic Documents Act***.

Providing the Privacy Commissioner with the power to issue guidance: The *Privacy Act* could include a power for the Privacy Commissioner to issue non-binding guidance on how the Commissioner interprets the *Privacy Act* and approaches investigations under the Act, to make individuals and federal public bodies aware of the Commissioner's views. Other information and privacy commissioners and ombudspersons across Canada, and at the international level, issue guidance for both private and public sector entities.

Permitting federal public bodies to seek the Privacy Commissioner's views outside an investigation context: The Privacy Commissioner could also be given the power to issue, on request by a federal public body, a statement of the legal position or interpretation the Privacy Commissioner would adopt when assessing compliance with the *Privacy Act* in a complaint investigation or similar context, similar to the power that the Commissioner of Lobbying has to issue non-binding advisory opinions. A similar power could enable the Privacy Commissioner to advise a requesting federal public body of the position the Privacy Commissioner would take in relation to a specific compliance question the federal public body put before the Privacy Commissioner, solely on the basis of the information provided. The Commissioner could also have the discretion to refuse to investigate a complaint on the basis that an advance opinion had sufficiently addressed a matter, where appropriate.

Introducing a "regulatory sandbox" environment: A regulatory sandbox is a controlled and supervised environment in which particularly novel business models, structures or processes can be tested for compatibility with legal requirements in cooperation with an oversight body, and outside of an adjudicative or coercive compliance environment. While a range of policy-based mechanisms currently support dialogue between the Privacy Commissioner and federal public bodies exploring new initiatives, neither the Act nor related policy instruments recognize any mechanism by which presumptive compatibility with legal requirements could be confirmed by the Privacy Commissioner in advance. While necessary limitations and caveats would be important, including an individual's continued ability to file a complaint and the courts' ultimate oversight, the Act could include the possibility for federal public bodies to engage the Privacy Commissioner, upon request, for more collaborative discussions aimed at supporting compliance. The United Kingdom has implemented a regulatory sandbox mechanism that could be used as a model.

Enhanced transparency for complaint investigations and oversight powers: To assist all federal public bodies in learning from the experiences of some, the Privacy Commissioner could be empowered to disclose more information in the public interest. This discretionary authority would be supplemented by a statutory direction to publish advance opinions, decisions around processing access requests, and complaint investigation outcomes, including decisions to decline to investigate, final reports and orders, and compliance agreements. This new authority could be made subject to the Privacy Commissioner's existing obligation to protect the confidentiality of certain categories of sensitive information protected from disclosure under the Act (e.g. s. 65) and include protections for a complainant's personal information.

Transparency in the procedures of the Office of the Privacy Commissioner: The *Privacy Act* could include new provisions clarifying the Privacy Commissioner's authority to publish information about how the Privacy Commissioner will exercise enforcement powers under the Act. This could assist to ensure transparency and consistency in the processes and procedures that guide the Privacy Commissioner's exercise of oversight powers.

4.3 Empowering the Privacy Commissioner with enhanced powers

The following discussion explores how to ensure that new oversight powers complement and maintain the strengths of Canada's existing oversight model. Many of these ideas would seek to align the Privacy Commissioner's powers in the private sector as appropriate in the public sector sphere, as well as with the Information Commissioner's powers.

Facilitating early dialogue to prevent issues: Many of the transparency measures under consideration above would facilitate the proactive publication of information about federal public bodies' practices with personal information. This information could be accessible to both the public and the Privacy Commissioner, to facilitate useful dialogue between federal public bodies and the Privacy Commissioner outside of a complaint investigation or audit process. It would, however, be important to ensure that federal public bodies were supported in, and not prejudiced by, their efforts to be transparent and proactively accountable if compliance issues were identified.

Maintaining informal complaint resolution: Other jurisdictions' experiences indicate that informal complaint resolution, including mediation of complaints, can be combined with stronger enforcement powers in a way that protects a fair decision-making process for all parties. The Privacy Commissioner's existing informal complaint resolution processes could be maintained and formally affirmed in the Act.

New authority to decline or discontinue an investigation: To enhance the efficiency of the Privacy Commissioner's oversight role and direct limited resources to high impact or systemic compliance issues, the Privacy Commissioner could be given a new discretion to decline to investigate a complaint or to discontinue an active complaint investigation. The Privacy Commissioner could be provided with the discretion to decline to investigate a complaint in a number of circumstances, including where a complaint was vexatious, frivolous or made in bad faith, or where the Privacy Commissioner deemed an investigation to be unnecessary, including cases where a complaint was already the subject of an investigation or had already been the subject of a report by the Privacy Commissioner.

New authority to approve requests to decline to process a request for access to personal information: Consistent with new provisions recently introduced into the *Access to Information Act*, federal public bodies could be authorized to decline to process certain access requests under the *Privacy Act* with the Privacy Commissioner's approval. This would allow federal public bodies to direct resources away from vexatious or abusive requests.

Facilitating cooperative action with other oversight bodies: The *Privacy Act* could be amended to allow the Privacy Commissioner discretion to share information about complaints and enforcement action

with a range of other federal, provincial, and international oversight bodies operating in related spheres. Provisions in the ***Personal Information Protection and Electronic Documents Act*** that facilitate information sharing with public bodies having similar functions and duties would serve as a model.

Requiring the Privacy Commissioner to consult other relevant oversight bodies: The Act could be amended to ensure that the Privacy Commissioner takes into the perspectives and expertise of other relevant oversight bodies before closing an investigation. Before issuing findings for a complaint against federal public bodies regulated by other oversight bodies, such as those overseeing the activities of law enforcement or national security agencies, the Privacy Commissioner could be required to consult with those other oversight bodies to ensure a coherent approach to the oversight of such federal public bodies, and to minimize duplication of regulatory efforts.

Introducing an authority to enter into binding and enforceable compliance agreements: The Privacy Commissioner could be authorized to enter into binding compliance agreements with federal public bodies. These provisions could be modeled on the same powers under the ***Personal Information Protection and Electronic Documents Act*** that allow private sector organizations to enter into compliance agreements. This could give the Privacy Commissioner a powerful new tool to work through complaints raising public policy issues of significant legal, technological and operational complexity with federal public bodies – a legally binding and enforceable compliance agreement would be the result. Concerns around ensuring that agreements would be reached in a timely manner could be addressed through provisions supporting appropriate incentives for meaningful engagement, including statutory timelines, evidentiary requirements, and appropriate burdens of proof in subsequent court proceedings should the process fail.

Granting order-making powers for access complaints: In the last fiscal year, approximately 85% of the Privacy Commissioner's complaint investigations addressed issues individuals had experienced when seeking to obtain access to their own personal information. Given the close legislative linkages between access requests under the *Privacy Act* and the *Access to Information Act,* the nature of access issues, and their importance to individuals, the *Privacy Act* could be amended to grant the Privacy Commissioner the same order-making powers the Information Commissioner has to resolve access complaints under the ***Access to Information Act*****.** Like the Information Commissioner, the Privacy Commissioner could be empowered to issue orders where access complaints could not be resolved through more informal means. Parties to an access complaint would have 30 days to challenge the Privacy Commissioner's order before the Federal Court. After this time, the Privacy Commissioner's order would take effect and the respondent federal public body would be legally bound to comply with its terms.

This approach would empower the Privacy Commissioner to issue binding orders in respect of the vast majority of complaints his office receives. This would respect the ***Access to Information Act*** and the *Privacy Act*'s substantive legislative interactions in relation to access issues and promote consistency in oversight. No particularly costly or disruptive changes to the Privacy Commissioner's existing processes would be required – the same investigative powers and reporting procedures could be maintained and be augmented by the Privacy Commissioner's new authority to include an order in an investigation report where circumstances warranted. Access to justice for individuals would be materially enhanced

and individuals would not be newly required to advance their own complaints through a tribunal model. The Privacy Commissioner's orders would bind and be enforceable against federal public bodies, and the Information and Privacy Commissioners could readily cooperate under the same enforcement frameworks where their legislative mandates overlapped.

Comprehensively broadening the scope of the Federal Court's current review powers: For any matters that could not be resolved through new enforcement powers, the scope of the Federal Court's current authority to conduct *de novo* reviews would be broadened to address complaints relating to the collection, use, disclosure, retention or safeguarding of personal information. For the reasons set out in a technical engagement paper, *A modern and effective compliance framework with enhanced enforcement mechanisms*, very few matters are likely to reach this stage of the graduated enforcement ladder being considered. For those that do, a public adjudicative process led and informed by the expertise of the Privacy Commissioner with results that are broadly binding could be particularly beneficial to the system as a whole. Maintaining the *de novo* nature of the Federal Court's review powers would ensure strong access to justice – this feature enables the Privacy Commissioner to continue to serve as an advocate for complainants and most effectively advance their complaints on their behalf. Again, as experience is gained with a comprehensively modernized *Privacy Act* and the system matures, consideration could be given to replacing this process with alternative administrative approaches should evidence arise that supports a clear need for their adoption.

Addressing the application of the Privacy Act to the Privacy Commissioner: The Privacy Commissioner is subject to the *Privacy Act*. This raises some complexities, particularly in the area of enforcement – an individual must file a complaint about the Privacy Commissioner's practices to the Privacy Commissioner, for example. To date, this has been addressed by the Privacy Commissioner through the creation of a Privacy Commissioner *ad hoc* to whom investigation and reporting functions are delegated. New enforcement powers and adjudicative functions may threaten the continued feasibility of this approach. The *Privacy Act* could formally recognize a Privacy Commissioner *ad hoc,* and in cases where a negotiated resolution could not be reached with the Privacy Commissioner, or a complainant was dissatisfied with the results, remedies like those that could bind federal public bodies would be available in the case of complaints against the Privacy Commissioner. Another potential option would be to appoint a single office holder capable of overseeing the Information Commissioner's compliance with the *Access to Information Act* and the Privacy Commissioner's compliance with the *Privacy Act*.

New offences to deter serious violations of the Act: Some jurisdictions have created offences to combat "snooping" into government records by employees and to deter unauthorized attempts to re-identify information that has had personal identifiers removed to protect individual privacy. Similar measures could be introduced into the *Privacy Act*.

ANNEX 5: Glossary

Access to Information Act refers to the *Access to Information Act*, RSC 1985, c A-1, federal legislation which gives Canadian citizens, permanent residents and any person or corporation in Canada a right to access records of government institutions that are subject to the legislation.

APEC Privacy Framework refers to the principles and implementation guidelines established by the Asia-Pacific Economic Cooperation (APEC) to protect privacy and to enable regional transfers of personal information and electronic commerce throughout the Asia Pacific region.

Canadian Charter of Rights and Freedoms refers to the *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, *1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, which protects the fundamental rights and freedoms of Canadians.

Consistent Use refers to the use of personal information for a purpose other than the original purpose for which the information was collected where that additional purpose is compatible with that original purpose.

Convention 108 refers to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108), a legally binding, international instrument introduced by the Council of Europe in January 1981 for the protection of individuals regarding the automatic processing of personal data. In May 2018, the Council of Europe introduced the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, which proposes certain updates to Convention 108.

Data integration refers to the comparison, combination or consolidation of multiple data sets to facilitate the use of that data for public benefit.

De-identified personal information refers to personal information that has been modified so that it can no longer be attributed to a specific individual without the use of additional information.

Elections Act refers to the *Canada Elections Act*, SC 2000, c 9, federal legislation which regulates federal elections in Canada.

ETHI Committee refers to the Standing Committee on Access to Information, Privacy and Ethics which studies matters relating to the Office of the Information Commission of Canada, the Office of the Privacy Commissioner of Canada and the Office of the Commissioner of Lobbying of Canada, and certain issues related to the Office of the Conflict of Interest and Ethics Commissioner.

General Data Protection Regulation refers to the General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, which regulates the processing of an individual's personal information by another individual, company or organization within the European Union.

Interoperability of legislation refers to the ability of legislation from different jurisdictions to be as compatible as appropriate.

OECD refers to the Organization for Economic Co-operation and Development, an international organization, which establishes international standards and policies for a range of social, economic and environmental topics.

Office of the Comptroller General refers to the office responsible for supporting the Comptroller General of Canada, an officer of Parliament appointed by the Governor in Council, in providing functional direction and assurance across the federal government for financial management, internal audit, investment planning, procurement, project management, and the management of real property and material.

Personal Information Protection and Electronic Documents Act refers to Part 1 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, federal legislation which governs the collection, use and disclosure of personal information by private-sector organizations across Canada in the course of commercial activity.

Privacy-by-design refers to the concept of planning and implementing the protection of personal information at the design stage of an initiative, program or service.

Privacy Act or the Act refers to the *Privacy Act*, RSC 1985, c P-21, which governs the collection, use and disclosure of personal information by federal public bodies in Canada. It also establishes the Office of the Privacy Commissioner.

Privacy Commissioner or **the Commissioner** refers to Privacy Commissioner of Canada, the officer of Parliament appointed by the Governor in Council to oversee compliance with the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

Office of the Privacy Commissioner of Canada refers to the office responsible for supporting the Privacy Commissioner of Canada, who is an officer of Parliament appointed by the Governor in Council to oversee compliance with the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

OECD Guidelines – means the Organisation for Economic Co-operation and Development (OECD) Revised Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013). Initially introduced in 1980, the OECD's statement of core information privacy principles have served as the basis for national and international privacy instruments. The revised guidelines were published in 2013.

Privacy Impact Assessment or **PIA** refers to an formal analysis to identify and mitigate an organization's privacy risks.

Privacy Management Program refers to an individualized organizational plan for protecting personal information in compliance with legal requirements.

Quasi-constitutional refers to a legal principle which mandates that the rights provided by a piece of legislation are to be interpreted broadly, and any exceptions to those rights must be clearly stated by the legislation.

Regulatory sandbox refers to a controlled and supervised environment in which particularly novel business models, structures or processes can be tested for compatibility with legal requirements in cooperation with a regulator, outside of an adjudicative or coercive compliance environment.

Targeted technical engagement refers to Justice Canada's June 2019 initial discussion with privacy, data and digital experts and certain government stakeholders on a number of technical and legal considerations for modernizing the *Privacy Act*.

Treasury Board Secretariat or **TBS** refers to Treasury Board Secretariat of Canada, the administrative arm of the Treasury Board, which is responsible for providing advice and recommendations on government management regarding accountability and ethics; financial, personnel and administrative management; comptrollership; and approving regulations and most Orders-in-Council.