Department of Justice Canada
Ministère de la Justice Canada

PRIVACY ACT MODERNIZATION: A DISCUSSION PAPER

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

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

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

Canada

Ensuring legislative clarity and accessibility

Clear and accessible statutory definitions play an essential role in achieving a predictable understanding of how legislation will operate. In addition to their role guiding the application of the law, definitions are an important transparency tool. With the benefit of clear and precise definitions, individuals can better understand their legal rights, and federal institutions can better understand when the legislation applies, what their obligations are, and more easily apply the law. In light of the recommendations made by the House of Commons' Standing Committee on Access to Information, Privacy and Ethics ("ETHI Committee") following its study on *Privacy Act* review, and of modern approaches being taken in other jurisdictions, certain key concepts and terms under the Act could be defined or updated.

Certain definitions in the Act play a fundamental role in determining the scope of the Act, that is, if it applies. For example, if information is not "personal information", then the *Privacy Act* does not apply, although other pieces of legislation or policy instruments may. Likewise, if personal information is "publicly available", then such information, if collected in accordance with the Act, can be used and disclosed without the need for the institution to obtain consent or rely on an applicable authority under subsection 8(2) of the Act. Given that these legal concepts effectively delineate the line between when legal obligations apply and when they do not, careful consideration should be given as to whether such legal concepts remain relevant for the digital age.

Other key terms do not determine whether the Act applies or not, but may benefit from greater clarity given the passage of time since they were first articulated. These terms could be modified to enhance clarity and ease difficulties that have arisen with practical application. Likewise, there are new concepts that could be introduced into the Act that may need to be defined.

Ultimately, defining certain concepts in a way that takes into account evolutions in expectations, the law, and developments elsewhere will help ensure greater clarity around the applicable legislative scheme, and make the Act a more accessible source of privacy protection in Canada.

A. Scope: concepts that impact whether the Act applies

The legal impact of a particular statute depends on the scope of core provisions that determine whether the statute applies in the first place. For example, the *Privacy Act* applies only to "federal institutions", a term which is defined under section 3 to include government institutions listed in Schedule 1 of the Act, or those added in the definitions section (e.g. Crown corporations). Even then, federal institutions may not have obligations under the Act depending on the type of information in their hands – if information is not considered "personal information", then the Act does not impose obligations.

There are many important concepts under the Act that have an incidence on whether it applies, or whether certain provisions of the Act apply. However, many of these concepts were defined in the early 1980's, when the world was a much different place. With the rise of our digital society, and with more advanced thinking about how to protect privacy rights in the modern era, many of these concepts could benefit from an update.

Additionally, some terms that might delineate when and how certain obligations apply under the Act could be introduced. For example, de-identification techniques, combined with re-identification risk measurement procedures, are a way to greatly reduce, if not eliminate, privacy risks relating to the use of personal information. The European Union's General Data Protection Regulation ("GDPR"), for example, creates incentives for covered entities to use de-identification, pseudonymization and encryption methods to protect personal data. There may be some value in introducing such concepts in the Act.

Personal information

Under section 3 of the *Privacy Act,* "personal information" is defined as "information about an identifiable individual that is recorded in any form" and includes a non-exclusive list of examples.

During the ETHI Committee's study of the *Privacy Act*, many witnesses commented on the need to revise the definition of "personal information". Much of this commentary related to whether unrecorded information needs to be included in the definition. Several witnesses suggested changing the definition of "personal information" to remove the reference to recorded information and the ETHI Committee ultimately recommended that the definition of "personal information" in section 3 of the Act be amended to ensure that it is technologically neutral and that it includes unrecorded information. This could include, for example, video footage that is monitored but not ultimately retained in recorded form.

Several witnesses before the ETHI committee also mentioned some of the challenges posed by metadata. Generally speaking, metadata is information associated with or about a communication, but not the informational content of the communication itself. It is the contextual information surrounding a communication that can be used to identify, describe, manage or route the communication. Some of the witnesses were of the view that metadata met the definition of personal information. Others pointed out that one of the challenges of defining metadata in the Act was ensuring that such a definition is technologically neutral, since metadata might mean something different in the future. In his May 7, 2019 appearance before the ETHI Committee, the Privacy Commissioner shared his view that the Act should set out some basic rules governing when institutions would be able to collect and share metadata, as opposed to a setting out a prescriptive approach. The ETHI Committee ultimately recommended that metadata be defined in the Act, in a technologically neutral way and with an emphasis on the information it can reveal about an individual.

However, defining "metadata" separate and apart from the definition of "personal information" could suggest, as a matter of statutory construction, that metadata is something other than information about an identifiable individual. And not every individual piece of metadata, by itself, may reveal information about an individual, even though such information, when amassed over time or viewed along with other available information, can potentially provide a picture of one's personal activities, views, opinions, and lifestyle. The Office of the Privacy Commissioner has also stated that the notion of metadata "is undeniably broad". Given this context, defining metadata could pose some practical difficulties and, if defined as something other than "personal information", could open up the application of the Act to the collection, use, disclosure, retention and management of information that may not actually be, depending on the context, about an identifiable individual.

Other elements of the definition of "personal information" also warrant discussion, including the concept of "identifiability". While "identifiability" is one of the critical conditions ultimately determining whether the Act will be engaged or not, there is no statutory definition clarifying what it means. Other data protection acts define the concept of identifiability. For example, the European Union's GDPR defines personal data as follow:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

In the absence of a statutory definition, the Canadian courts have determined that an individual will be "identifiable" in relation to information about them when "there is a serious possibility that [the] individual could be identified through the use of that information, alone or in combination with other available information."[1]

[1] *Gordon v. Canada (Health),* 2008 FC 258 at paras. 33-34.

This largely fact-driven approach to "identifiability" has proven difficult to apply in practice and raises additional questions: (i) who bears the burden of searching out "other available information" and what degree of effort is required?; (ii) what sources of "other available information" must be considered, and do they include only public or also internal government sources?; (iii) is identifiability by a member of the public, an expert investigator or a single government employee the relevant standard; and (iv) how do changes over time impact the analysis?

Particularly in an era in which government is seeking to proactively make much more of its information holdings publicly available, government institutions could benefit from clearer guidance on the meaning of "identifiability".

Q.3(a). Should the definition of personal information be grounded in the concept of identifiability, and if so, should this concept be defined?

Q.3(b). Does metadata require a separate definition altogether, or can the privacy issues relating to such information be addressed by an updated definition of personal information (including by adding an example)?

De-identified, anonymized, pseudonymized, and encrypted personal information

One important definitional issue is whether the *Privacy Act* should recognize new subsets of personal information in order to facilitate the application of a more nimble and context-sensitive rule set. For example, to create something akin to a "data trust" that differentiated in its treatment of identifiable and de-identified information, it would be important to be able to effectively and with sufficient certainty determine which rule set applied to which data elements. The current "in or out" approach to personal information does not accommodate more nuanced rules that may be organized around different levels of risk and foster compliance. Defining de-identified, anonymized, and pseudonymized information could support the development of new compliance incentives, allow for a more targeted and nuanced application of certain rules, and assist to ease some of the difficulties of practical application that arise under the current approach.

Generally speaking, "anonymized" information has been irreversibly stripped of personal identifiers, whereas "de-identified" information has been modified so that it can no longer be attributed to a specific individual without the use of additional information. "Pseudonymization" is a special form of de-identification where new data elements are substituted for identifying information. Encryption involves taking information and making it appear unintelligible through the use of an encryption "key", without which the information either cannot be accessed or understood. In its study of the *Privacy Act*, the ETHI Committee did not address the role that effectively anonymized personal information or pseudonymized personal information could play in a modernized *Privacy Act*. It also did not address the role encrypted information could play.

Currently, other data protection regimes provide an important role for the use of de-identified personal information, and limit some obligations where encryption is employed. For example, in the GDPR, several provisions create incentives for data controllers to use de-identification, pseudonymization, or encryption methods, which can have an impact on how obligations apply, or even provide relief from certain obligations.

Q.3(c). What role could de-identified, pseudonymized, or encrypted personal information play in a modern Privacy Act, and how should such terms be defined?

Publicly available personal information

Subsection 69(2) of the *Privacy Act* exempts "publicly available" information from the rules regulating the use and disclosure of personal information. If information was publicly available in 1983, it was available in limited

quantities and existed in a form that could make the application of use and disclosure rules generally unnecessary (e.g. paper-based public registry records).

The digital revolution and social media has changed all of this. Because of the increased digitization of information, it is now easier to locate, collect, use, or disclose publicly available information, especially online. As well, determining how information was made public is also becoming more and more difficult to assess – careless or malicious actors can make personal information publicly available, without the knowledge of the individual concerned. Thus, the amount, nature, and type of personal information that was publicly available in 1983 fundamentally differed from today.

These developments suggest a need to reconsider our reliance on practical obscurity where the legal treatment of publicly available personal information is concerned. Introducing a definition that seeks to protect individuals' reasonable expectations in context is one possible approach. In practice, this might mean considering the nature of the information, the source of the information and how and why it was made publicly available in the first place. Integrating these types of considerations into the current factual approach to determining when personal information is publicly available could better meet Canadians' reasonable expectations in a digital age.

PIPEDA does not specifically define "publicly available information", but allows for the collection, use and disclosure of personal information without knowledge and consent if the information "is publicly available and is specified by the regulation". The *Regulations Specifying Publicly Available Information* then set out a list of certain types and classes of information that are specified for these purposes. Another existing Canadian model is the statutory definition of "publicly available information" in Bill C-59 for proposed inclusion in the *Communications Security Establishment Act.* This definition would effectively exclude from the definition of publicly available information "information in respect of which a Canadian or a person in Canada has a reasonable expectation of privacy".

Q.3(d): What do you foresee to be the public's expectations concerning publicly available personal information?

Q.3(e): How could "public available personal information" be defined under a modern Privacy Act?

B. Defining other key concepts

Clear and accessible statutory definitions play an essential role in achieving a common and predictable understanding of how legislation will operate. In addition to their role guiding the substantive application of the law, definitions constitute an important transparency tool. With the benefit of clear and precise definitions, the public can better understand their legal rights and institutions can more easily apply the law. Several terms in the Act may benefit from updating, in light of more modern thought on privacy issues and approaches taken in other jurisdictions.

Consent

Currently, the Act recognizes consent as a basis upon which a federal institution can use or disclose personal information for a purpose other than that for which it was collected. However, consent is not defined in the Act. The notion of consent is an example of a term that has been interpreted by courts in various contexts, with the common law articulating a number of clear, broadly accepted, and rigorous requirements that must be satisfied for consent to be considered valid. Generally speaking, valid consent will be unambiguous, fully informed, and freely given.

While many personal information protection statutes that apply to public-sector entities identify consent as a basis for further uses or disclosures of personal information, not many actually define consent. Of those that do, the scope of definitions vary. The GDPR, for example, defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". By contrast, the Australian *Privacy Act* defines consent as meaning "express consent or implied consent."

Elements that have been identified through the common law can be useful in delineating the meaning of consent. Defining consent in the Act could help mitigate ambiguities around the concept of consent. In addition, defining consent in a manner consistent with Canadian common law requirements could improve transparency by codifying in statute existing legal requirements for the benefit of both government institutions and individuals navigating them. It could help individuals to better know what is required for their consent to be considered valid, and would help clarify for institutions what is required to obtain valid consent and how to design initiatives to accommodate such considerations. It could also provide a more rigorous standard that could alleviate some of the concerns associated with relying on consent in the public sector context, such as the power imbalance between individuals and the government.

Q.3(f): Should consent be defined under a modern Privacy Act, and if so, what elements would it include?

The issue of how consent should operate in the context of the public sector is also addressed in the discussion paper entitled: *Privacy principles and modernized rules for a digital age.*

Administrative purpose

The Act currently defines an administrative purpose as "the use of [personal] information in a decision making process that directly affects that individual". Ultimately, the definition interacts with the provisions of the Act to create two levels of privacy obligations: full and partial. Where an administrative purpose is present, all of the requirements of the Act must be fully met. Where there is no administrative purpose at issue, for example, the use of personal information for research, statistical, audit and evaluation purposes, institutions have more flexibility with respect to certain issues, such as direct collection, retention and accuracy.

Generally speaking, this approach makes good regulatory sense. This approach allows institutions to concentrate compliance resources where there are direct consequences for an individual, with a view toward better protecting the public from the greatest risks. One important element for discussion is whether a decision making process that directly affects only the individual whose personal information is at issue remains the best threshold for imposing a full suite of privacy protections. New technologies, new types of harm and new ways of making decisions suggest that there might be a better way of channeling the application of the Act.

For example, when the current definition is applied to the use of artificial intelligence in the public sector, it leads the inquiry along technical lines that may ultimately miss the mark for individuals. One such inquiry is whether the creation of an artificial intelligence system with personal information is an "administrative purpose" or is it only the artificial intelligence system's application in individual cases that gives rise to an "administrative purpose"? If it is the latter, then the requirement in the Act to use accurate personal information may not be adequately engaged at the design stage. While purposive legal interpretation might be sufficient to ensure due diligence is employed in the creation of artificial intelligence systems, it may be preferable if the relevant legal considerations were clearer on their face.

The current definition of "administrative purpose" aims to get at the ultimate question of whether individuals are exposed to a sufficient risk of harm that the full suite of legal protections should apply. Or put the other way, it

aims to recognize some obligations in respect of personal information that can be relaxed where individuals are not significantly impacted. One approach to ensuring the *Privacy Act* prompts the right questions would be to be clearer about this role. For example, the definition of "administrative purpose" could be reduced to first principles and reframed in terms of a harm threshold (e.g. certain requirements of the Act could be relaxed where there was no or only negligible risk of harm to any individual, using subjective or objective criteria, or both, for determining harm). Alternatively, an alternative approach more suited to the digital age could be developed (e.g. if a technological protection were available and applied to eliminate the need for a particular legal protection, compliance requirements could be relaxed or eliminated). A third approach would be to reconsider the inclusion of the concept at all.

Q.3(g): Should a modern Privacy Act still make distinctions between administrative and non-administrative uses, and if so, how should an "administrative use" be defined?

Consistent use

The concept of a "consistent use" is another example of a concept that could benefit from additional clarity. Under the *Privacy Act*, a government institution is permitted to use and disclose personal information for new purposes when those new purposes are consistent with the purposes for which personal information was collected – in other words, for a "consistent use". The Supreme Court of Canada has affirmed that the test for identifying a valid consistent use turns on an individual's reasonable expectations: where an individual "would reasonably expect that the information could be used in the manner proposed" because of a sufficiently direct connection with the purpose for which it was collected, it is a consistent use.[2]

This definitional approach is respectful of individuals' reasonable expectations in context but is also difficult to apply in practice. It can be challenging to ascertain what individuals would reasonably expect in any given context and the Act currently provides no guidance. Institutions are typically reluctant to base new programs and activities on such an uncertain legal foundation. And the existing accountability and transparency measures place the onus on individuals to search out information about institutions' reliance on this authority without providing any indicia of validity that individuals could test institutions against.

Article 6 of the GDPR identifies a number of considerations regulated entities must take into account when determining whether a practice with personal information is "compatible" with the purpose for which it was originally collected. These factors include the link between the original and the proposed purposes, the context in which personal information was collected with reference to the relationship between the individual and the regulated entity, the nature of personal information at issue, the consequences to the individual of the proposed new use, and the existence of appropriate safeguards, which could include encryption or pseudonymisation.

Q.3(h). Should the concept of a "consistent use" be defined under the Privacy Act? If so, how?

Q.3(i): Could the criteria-based approach to "compatible uses" under the GDPR assist to clarify the proper scope of a "consistent use" under the Privacy Act? If so, what factors should institutions consider?

[2] *Bernard v. Canada (Attorney General),* 2014 SCC 13, [2014] 1 S.C.R. 227 at para. 31.