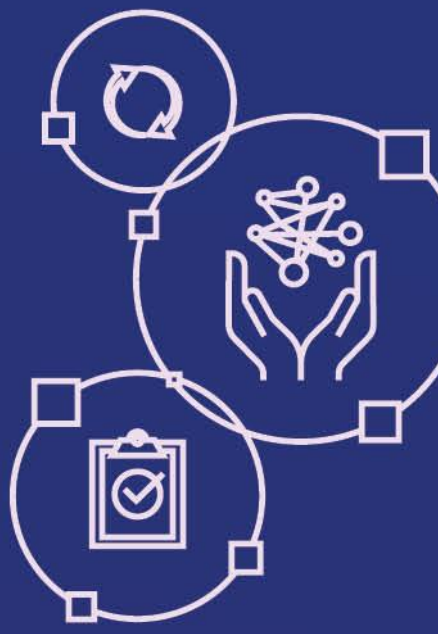
Government of Canada / Gouvernement du Canada



Modernizing
Canada's *Privacy Act*

WHAT WE HEARD REPORT

Justice Canada's Online Public Consultation on *Privacy Act* Modernization

Fall 2020 to Winter 2021

Canada

Cat. No. J2-494/1-2021E-PDF
ISBN 978-0-660-37476-5

Contents

INTRODUCTION

About the *Privacy Act* Modernization Initiative

The *Privacy Act* is Canada's federal legislation that governs how personal information is collected, used, disclosed and managed by Government of Canada departments, agencies and commissions, and other federal public bodies.[1] The Act came into force in 1983 – almost four decades ago. Much has changed since then. Information technology has become an increasingly important part of everyday life. Innovation and growth across major government initiatives and the private sector depend on data. Profound technological advances and social changes only begin to explain the evolution in Canadians' expectations of how federal institutions collect, use, share and store their personal information.

The Department of Justice Canada is leading an initiative to modernize the *Privacy Act* so that it will adequately protect Canadians' personal information in the digital age while allowing for responsible public sector innovation for the public good. As an important element of Canada's personal information protection framework, a modernized Act would continue to be an important piece of the overall regime for protecting Canadians' privacy in the twenty-first century.

Over the past few years, Justice Canada has heard from a number of stakeholders – within and outside the federal government – on how to update the personal information protection framework that applies to federal public bodies. This input includes the 28 recommendations for modernizing the Act from the Standing Committee on Access to Information, Privacy and Ethics, the Privacy Commissioner of Canada's recommendations for modernizing the Act, and calls from other stakeholders for modernizing the Act, including the Canadian Bar Association. As well, in 2019, Justice Canada led a preliminary targeted technical engagement with expert stakeholders.

This *What We Heard* report summarizes the main insights Justice Canada gained through the online public consultation that took place from November 16, 2020, to February 14, 2021. The main purpose of the public consultation was to gather public and stakeholder input on how to best update the Act so that Canadians can benefit from the many promises of the digital age while trusting in a renewed framework for government activities involving their personal information.

[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 was the case in the discussion paper, this report will use the more inclusive term "federal public body" throughout.

Format of the Online Public Consultation

A discussion paper outlining a possible vision for modernizing the *Privacy Act* was at the heart of the consultation exercise. This discussion paper set out ideas to bring the Act into the 21st century, enhance public trust in the Government of Canada's activities involving personal information, and better align the Act with more recent privacy frameworks, both within Canada and internationally.

Canadians and interested stakeholders were provided with various means to participate in the online public consultation. Through a dedicated website, stakeholders could comment on parts of the discussion paper that were of particular interest to them on an interactive forum. Stakeholders also had the opportunity to provide more formal, detailed submissions through the website, by emailing them to Justice Canada or by sending them by mail. Participants could also complete an online survey. This survey included a series of questions dealing with familiarity with the Act, trust in federal public bodies' activities involving personal information, and comfort with hypothetical activities involving personal information.

Ongoing Engagement with Indigenous Partners

Although the online public consultation was open to all Canadians, including Indigenous individuals, Justice Canada launched a parallel process for engaging directly with a number of Indigenous partners across Canada. Following the 2019 preliminary targeted technical engagement, which included participants such as the First Nations Information Governance Centre and the National Claims Research Directors, Justice Canada sought to engage directly with a number of Indigenous governments and organizations to better understand the unique impacts the modernization of the *Privacy Act* could have on Indigenous Peoples in Canada. Though the public consultation has closed, Justice Canada's engagement with Indigenous partners is ongoing.

Justice Canada has met with a number of Indigenous governments and national and regional Indigenous organizations as part of these engagement efforts since August 2020. The focus of these discussions has been to learn about Indigenous partners' perspectives on what is working well with the Act, what can be improved, and how the Act could be modernized to better reflect the specific needs and expectations of First Nations, Metis, and Inuit in Canada. Through bilateral engagement sessions, participating Indigenous partners have provided valuable insights for the modernization of the *Privacy Act*, and have raised a number of topics that require further discussion and consideration. Justice Canada will continue to engage with Indigenous partners to gain their perspectives on potential ideas for changing the Act.

HIGHLIGHTS OF THE ONLINE PUBLIC CONSULTATION

The input Justice Canada received through this consultation process reflects a wide and diverse range of contributors. The Department received 57 written submissions from such stakeholders as the Office of the Privacy Commissioner of Canada (OPC), the Office of the Information Commissioner of Canada (OIC), and the Privacy and Access to Information Law Section of the Canadian Bar Association (CBA), as well as federal public bodies, Canadian and international academics, Canadian citizens, private sector entities, non-governmental organizations, civil liberties advocates, and Indigenous partners. In addition, more than 1,100 individuals responded to the online survey, with almost 300 providing additional written comments on various topics, including access to personal information, privacy breaches, information-sharing agreements, and consent.

More than three quarters of the respondents who chose to provide demographic information were residents of British Columbia, Alberta, Ontario or Quebec, and almost three quarters were residents of urban areas. What follows is a discussion of the issues that emerged as being top-of-mind for most stakeholders.

Clarifying Key Definitions and Concepts in the *Privacy Act*

The definitions and concepts in the *Privacy Act* have remained the same since the Act was first enacted in 1983. For nearly 40 years, federal public bodies, Canadians and other stakeholders have had to rely on findings of the OPC and court decisions to interpret key definitions and concepts in the Act. The modernization of the Act provides an opportunity to revisit and update these definitions and concepts to provide clearer rules about what the Act covers and when its full protections are engaged.

There was general support among stakeholders for updating and clarifying certain definitions and concepts in the Act. In particular, the OPC supported modernizing the Act's central concepts to take into account the rapid evolution of digital technologies and enable interpretations to "adapt to the times." The OIC also supported providing greater clarification of key concepts, including "personal information" and "publicly available," in order to find an appropriate balance between privacy rights and access to government information.

Updating the Definition of "Personal Information"

The idea of updating the definition of "personal information" garnered substantial interest from a number of stakeholders, including the OPC, the OIC, the CBA, several federal public bodies, Canadian and international academics, and a number of non-governmental organizations. The current definition centres on the notion of an individual's "identifiability" – personal information is generally defined as "information about an identifiable individual."

Several federal public bodies and academics stressed the importance of clarifying the definition such that it is sensitive to context. However, stakeholders differed on whether the concept of "identifiability" could be expressed through a set list of criteria in the Act or whether a more general and overarching standard might be needed. The OPC cautioned against setting out overly narrow criteria for identifiability, to ensure that the concept remains relevant in the face of rapidly evolving technology and that it reflects well-accepted jurisprudence. The OPC recommended that the Act codify the existing test on identifiability set out by the Federal Court, namely that information will be considered to be about an "identifiable individual" where there is a serious possibility that an individual could be identified by that information, either alone or in combination with other information. The OIC recommended that the concept of "identifiability" should take into account the existing jurisprudence and be consistent with it. The CBA noted the challenges in recognizing and determining what constitutes "identifiable" information and stated that it was effectively impossible to establish an exhaustive set of criteria for doing so. Further, the CBA emphasized the benefits of occasional judicial consideration of this concept, which can help reveal "nuances or criteria that are difficult to anticipate."

Stakeholders' views also varied as to whether the Act should expand the definition of personal information by removing the existing requirement that information be "recorded in any form." The OPC argued that this requirement should be removed from the definition to reflect the realities of the digital age. According to the OPC, doing so would be more in keeping with a principles-based Act and would ensure that important obligations under the Act would apply to the handling of unrecorded personal information, such as the collection and use of such information (e.g. where a federal public body searches, views, monitors, accesses, or otherwise uses personal information but stops short of creating a record).

The OPC also recommended that the Act set new record-keeping obligations for the use and disclosure of personal information in a manner that directly affects the individual. Another stakeholder urged removing the reference to "recorded" information to recognize that privacy expectations are context-sensitive and unrelated to how information is "captured." On the other hand, some federal public bodies raised concerns about removing the Act's requirement that information be recorded, arguing that the practical benefits of bringing "unrecorded" information under the purview of the Act remained unclear.

Many stakeholders also commented on the non-exhaustive list of examples of what constitutes personal information under the Act. For example, the OIC and several other stakeholders supported a more nuanced and flexible balancing approach to assessing whether an individual's views and opinions of others are the personal information of the

individual who expresses them or of the subject of those views and opinions. They also supported an approach that would clarify what business information should be considered personal information under the Act.

Many Canadian and international academic stakeholders also supported aligning the Act's definition of personal information more closely with that of the European Union's *General Data Protection Regulations* (GDPR), including recognition of a special category of "sensitive personal information." There was general support among stakeholders for providing additional clarity and protection in the Act for specific types of sensitive personal information, including health and biometrics information. Finally, one government institution suggested that the Act's definition of personal information should expressly apply to "unique research, intellectual and creative works or ideas of the individual."

The OIC also specifically highlighted the importance of maintaining the existing list of exceptions under paragraphs j) to m) of the Act's definition of personal information.

Clarifying the Concept of "Consistent Uses"

The Act permits federal public bodies to use or disclose personal information without consent for purposes that are "consistent" with those for which it was originally collected. The OPC, along with several federal public bodies and many stakeholders, welcomed the opportunity to clarify the concept of "consistent use" under the Act. The OPC supported the addition of criteria to highlight the appropriate considerations for assessing whether a use is "consistent." A Canadian academic noted that federal public bodies had given the concept an "expansive interpretation" over the years. This academic was in favour of clarifying the meaning of this concept in the Act, suggesting it could be supported by a list of examples and informed by the reasonable expectations of individuals. In addition, an international academic stakeholder expressed support for a flexible definition aligned with the GDPR's approach to "compatible uses."

Outlining the Scope of "Publicly Available" Personal Information

Currently, the rules under the Act relating to use and disclosure of personal information do not apply to "publicly available" personal information. However, the Act does not define what "publicly available" means. Over time, it has become apparent that information can become public in a variety of ways, sometimes without the knowledge of the individual to whom it relates, especially in the digital realm. There was broad support among stakeholders for the need to clarity what constitutes publicly available personal information. However, they had different views on how to define the concept.

The OPC supported defining the concept of publicly available personal information in the Act, but recommended that any such definition expressly provide that "publicly available personal information does not include information in respect of which an individual has a reasonable expectation of privacy." The OIC expressed concerns with the potential approach for defining publicly available personal information set out in the discussion paper. The OIC recommended that this definition be consistent with the jurisprudence that has interpreted the term, to achieve a proper balance between the protection of privacy and access to information. On the other hand, the CBA supported the definition set out in the discussion paper and agreed that any such definition should exclude information in respect of which individuals have a reasonable expectation of privacy. The CBA also held that such a definition should not differentiate between the information of individuals located in Canada and those outside of Canada. A number of federal public bodies, academic stakeholders, and non-governmental organizations also supported clarification of what constitutes publicly available personal information. One government institution expressed the view that any such definition should be broad enough so as not to impede law enforcement activities, which can sometimes involve the collection, use and disclosure of personal information that is publicly available on the Internet, for example.

Introducing Personal Information Principles into the *Privacy Act*

The idea of introducing personal information principles inspired by those in the *Personal Information and Protection of Electronic Documents Act* (PIPEDA) into the *Privacy Act* garnered substantial support from most stakeholders. Many viewed the introduction of principles as an important tool for aligning the Act with PIPEDA and with internationally recognized standards. Further, such principles are widely seen as part of a contextually sensitive, adaptable and flexible approach to regulating activities involving personal information, in addition to supporting interoperability of the Act with other personal information protection frameworks.

The OPC supported the idea of introducing principles in the Act and noted that doing so had the potential to significantly improve the Act's ability to "effectively address the modern, data-centric needs of Canadians." Some federal public bodies also supported the introduction of principles, with appropriate adaptations and considerations for the unique nature of activities involving personal information in the public sector (e.g. law enforcement). Other stakeholders also pointed to the GDPR as a good reference point for relevant principles.

Some submissions included more detailed input, such as the proposal that the Act should include an overarching principle of necessity and proportionality that would apply to all federal public bodies' activities involving personal information. One academic stakeholder even suggested that those activities be further subject to a "minimal intrusiveness" principle.

On the other hand, a few Canadians expressed concerns with what they considered the "vagueness" and insufficiency of a principles-based approach. They also noted that it might be "too open to interpretation" and risk allowing misuse of personal information.

Updating the Rules on the Collection, Use, Disclosure, Retention and Disposal of Personal Information

Updating the Act's rules on the collection, use, disclosure, retention and disposal of personal information goes hand in hand with the introduction of new principles. Many stakeholders commented on what these requirements might look like in a modernized Act – especially those pertaining to the collection, use and disclosure of personal information.

Updating When Personal Information Can Be Collected

The proposal to update the rule for when federal public bodies can collect personal information (the "collection threshold") received significant interest from stakeholders. This issue is of particular importance, since it is central to determining whether federal public bodies can collect personal information and how much. The Act currently allows the collection of personal information by a government institution "where it relates directly to an operating program or activity of the institution." As outlined in the discussion paper, a modernized collection threshold would limit collection of personal information to what is "reasonably required" for the federal public body's functions or activities or what it is otherwise expressly authorized by another act of Parliament. The Act would also include a list of key considerations that federal public bodies would have to take into account in determining whether a collection is reasonably required.

Federal public bodies appeared comfortable with this newly proposed collection threshold. The OPC signaled that the threshold would be workable if the goal is to clarify the Act while protecting privacy through well-established principles of necessity and proportionality. However, the OPC recommended that any list of specified criteria for determining what might be reasonably required in any given context should, among other things, help to adequately frame the purposes for collection and clarify that the intrusiveness of the collection must be proportionate to the public interests involved. The OPC also held that potentially higher costs for federal public bodies is only one of many factors that should be considered in evaluating whether there are less intrusive means to achieve a particular purpose.

On the other hand, the CBA reiterated their ongoing concerns that a "reasonably required" collection threshold would be inappropriate for the public sector context, and questioned the rationale for a difference between the proposed collection threshold and the necessity standard that would apply under Canada's proposed federal private sector personal

information protection legislation (Bill C-11, the *Consumer Privacy Protection Act*). Many other stakeholders supported the introduction of a "necessity" threshold in the Act. One academic stakeholder argued that the Act's current collection threshold is "very weak," that the proposed threshold does not properly reflect the "constitutional dimensions of data collection," and that the collection threshold should more clearly reflect the government's obligations under the *Canadian Charter of Rights and Freedoms*. Another stakeholder suggested that the collection of personal information should be limited to what is absolutely necessary.

Providing Appropriate Use and Disclosure Authorities

Many stakeholders provided views on potential changes to authorities for using or disclosing personal information for purposes other than those for which it was initially collected. In particular, the OPC and the OIC welcomed the idea of making improvements to the "public interest" disclosure authority under the Act. The OPC also provided views on what protections could support new authorities in the Act to disclose personal information for data-integration purposes and for emergencies or serious threats to public or individual safety. The OPC further recommended adjusting the scope of federal public bodies' ability to disclose personal information to "investigative bodies," by narrowly defining this concept and adding greater accountability mechanisms. The OPC did not favour including a specific provision in the Act that would permit disclosures of personal information to Statistics Canada for "statistical and research purposes," given the absence of specific limitations and the need to frame the scope of such a disclosure, among other things. The OPC, the CBA and an academic stakeholder all supported some form of additional requirements (e.g. written agreements) for cross-border disclosures, including those to foreign governments. Some stakeholders, such as the OIC and some federal public bodies, proposed introducing new disclosure authorities in the Act, namely for compassionate reasons, under emergency situations, as well as to victims of crime.

Leveraging Artificial Intelligence…While Protecting Personal Information

Recognizing the Privacy Risks

Many stakeholders noted the potential advantages of artificial intelligence (AI) enabled processes and automated decision making. They also recognized the importance of using such technologies to enable federal public bodies to innovate and to create efficiencies in the public interest. However, the comments received reveal that the Act, in its current state, lacks certain protections for individuals' personal information where AI and automated decision-making technologies are involved. Stakeholders were nearly unanimous in flagging wide-ranging concerns about the use of such systems. These included: (i) the potential for introducing biases and discrimination in decision-making processes; (ii) the lack of definitions of key concepts in this area; (iii) the ways automated decision-making systems actually

process personal information; (iv) the perceived lack of involvement of human officials where such systems operate; and (v) the need to ensure proper accountability and transparency around the development and use of these systems.

Charting a Path Forward

Many stakeholders provided views on how to mitigate such concerns and help modernize the Act in a manner that is sensitive to privacy but would also provide adequate support for using AI and automated decision making in the public interest. For instance, the OPC and another stakeholder mentioned the need for the Act to expressly define "automated decision making." However, one government institution cautioned that the Act should not define the term too broadly and that related requirements should be kept general and high-level enough to accommodate rapid changes in this area. The OPC also recommended that the Act include a right to "meaningful explanation" and to human intervention when automated decision-making systems are used, as well as an obligation for federal public bodies to log and trace their use of personal information in this context. Many other stakeholders supported the introduction of clear transparency requirements in the Act that would both support individual understanding of these processes and foster trust in their use. One stakeholder group also raised the potential for individuals to be able to opt out of the use of such systems. Finally, many stakeholders agreed that the existing *Directive on Automated Decision-Making* provided a useful framework for the Act to draw from in creating new legal rules.

Dealing with De-identified Personal Information

Stakeholder input revealed divided opinions on whether the *Privacy Act* should define "de-identified" personal information and include specific rules for the collection, use, disclosure, and retention of such information.

Defining De-identified Personal Information

A number of stakeholders discussed de-identified personal information, including whether the Act should define this concept. Many, including the OPC, some private sector organizations, academics, federal public bodies, Indigenous partners and private individuals, expressed support for defining de-identified personal information. These stakeholders felt that the concept needed greater clarification and suggested that any such definition should align with the definition being proposed for updating Canada's federal private sector personal information protection legislation or the European Union's GDPR.

While most stakeholders who provided input on this issue supported the idea that the Act should explicitly define de-identified personal information, a number of others disagreed, including the OIC, the CBA, some private sector organizations, and certain academics. These stakeholders argued that the *Privacy Act* should not apply to personal information once it is

de-identified. The CBA also expressed concerns that significant terminological and analytic confusion could be caused by introducing the concept of "de-identified personal information," which differs from the concept of "pseudonymised data" contained in the European Union's GDPR.

Special Rules for De-identified Personal Information

The majority of stakeholders suggested that specific rules are necessary for the collection, use and disclosure of personal information that has been de-identified. Some argued that de-identified personal information and "regular" personal information should be generally be subject to the same rules, with a few nuanced exceptions. Other stakeholders suggested that de-identifying personal information should result in more relaxed rules, allowing federal public bodies greater flexibility in using this information for innovative purposes. A number of stakeholders took the position that de-identified personal information should not be covered by the Act at all. Still others simply suggested that greater clarity surrounding this issue is required, and that further study and consultation might be warranted.

Identifying the Risks

Many stakeholders pointed out that privacy risks can sometimes persist even when personal information is de-identified. Such risks increase where personal knowledge, "publicly available" information, individual notoriety, or multiple pieces of information are involved, and especially where the de-identified personal information is made public. Given the context-specific risks to re-identification, many stakeholders argued that the focus should be on the privacy safeguards for information generally, not on whether the personal information is de-identified. For these stakeholders, a better focus would be on the algorithms, cybersecurity and contractual protections, access limits, and secure computing environments that apply when using such information.

There was divided opinion on the issues of whether trying to re-identify de-identified personal information without authorization should be an offense punishable by a sanction in the Act (e.g. a fine), and whether an individual's consent should be required before their de-identified personal information can be used or disclosed.

Other Concerns and Considerations

Some stakeholders raised concerns regarding the logistics of using de-identified personal information, suggesting that the costs associated with the proper storage of de-identified personal information could dis-incentivize federal public bodies from using this privacy protection method. Other stakeholders suggested that special attention should be paid to the use of de-identified information in an Indigenous and smaller community context, given the increased risks and impacts of re-identification. Finally, one stakeholder raised the point that

there may be a collective interest in the protection of personal information, even when it can no longer be associated with an identifiable individual. For instance, decision making that relies on de-identified data to track demographic level trends still raises concerns related to accuracy, bias, and potentially discriminatory impacts, which might affect groups as well as individuals.

Enhancing Transparency

Most stakeholders supported greater transparency measures around federal public bodies' activities that involve personal information. Stakeholders expressed support for replacing the existing Personal Information Bank regime with a more accessible online and searchable registry. The OPC expressed its support for Justice Canada's proposals to improve transparency, but recommended additional measures. These included limiting the exceptions to an individuals' right of direct notification about collection; requiring that such notices include specific details on the circumstances of the collection; and exploring ways to enhance individuals' direct access to the personal information that federal public bodies collect, use and disclose about them. One stakeholder suggested that information-sharing agreements (ISAs) should also be subject to enhanced requirements, including that they be in writing and accessible for evaluation by independent oversight bodies, and that written records on the nature and scope of information sharing itself should be created. Several stakeholders recommended that the Act require federal public bodies to publish information about their ISAs as well as their privacy management programs (PMPs) and privacy impact assessments (PIAs). One stakeholder noted the importance of greater transparency around policies and programs developed with the personal information of Indigenous individuals, and emphasized that this would help build confidence in federal public bodies. Finally, several federal public bodies called for new transparency measures in the Act to account for sensitive government functions, such as law enforcement, and for the unique nature of institutions with commercial mandates.

Increasing Accountability

The overwhelming majority of stakeholders stressed the importance of, and need for, increased accountability around federal public bodies' activities that involve personal information. The OPC agreed with the proposal to introduce a new accountability principle in the Act, one which would be supported by new requirements such as obligations to design programs and activities with the protection of personal information in mind and to undertake PIAs and put PMPs in place. Along the same lines, the CBA and a number of other stakeholders expressed support for a legislated obligation for federal public bodies to undertake PIAs.

Requirements to establish PMPs and privacy by design also received support, including from academic stakeholders. One stakeholder proposed that the accountability obligations currently set by policy instruments be "formalized" and brought under the Act itself, and that they be subject to review by the Privacy Commissioner. Another emphasized the importance of close alignment between the accountability requirements under the Act and those in the federal private sector, in order to ensure continuity in the application of relevant rules where personal data may be shared between public and private sector entities. Finally, one government institution called attention to the need to provide exemptions to any legislated obligation to publish PIAs or their summaries, so as to avoid the public disclosure of sensitive information, such as operational details that could raise national security concerns.

Strengthening Oversight and Enforcement

Many stakeholders expressed support for enhancing the compliance and enforcement framework under the Act. The OPC in particular welcomed measures to provide oversight and quick and effective remedies for individuals, including a more active guidance role for the OPC and an overall enhanced compliance framework. The OPC also expressed support for expanded proactive audit powers, while noting the need for increased discretion to focus its limited resources on the most pressing issues, along with much-needed remedies in the form of order-making powers and expanded rights of recourse to Federal Court.

Clarifying the Role of the Privacy Commissioner

The OPC noted that the proposed enhancements to the Act's oversight framework lagged behind the domestic and international frameworks that applied to other privacy regulators. The OPC argued that its ability to issue orders under the Act should extend to matters involving the collection, use and disclosure of personal information by federal public bodies, and not be limited to the denial of access to personal information. Most stakeholders expressed general support for increased powers for the OPC, including general order-making powers, and many specifically called for such powers to be broader than what was envisioned in the discussion paper. Some stakeholders also specifically expressed support for providing the OPC with the power to enter into binding compliance agreements.

The CBA signaled support for an enhanced oversight and enforcement framework under the Act, subject to some limits. For instance, the CBA supported the use of compliance agreements as a remedial and enforcement mechanism, but noted that these might be more appropriate for some federal public bodies, such as Crown corporations, rather than federal public bodies with important policy development functions. The CBA supported providing the OPC with a limited power to issue binding orders, similar to that provided to the OIC in 2019. The CBA also expressed concerns with the organizational structure of the OPC. It specifically

noted the importance of establishing strong procedural safeguards and a proper separation of the OPC's investigative and audit functions from any adjudicative ones.

Finally, stakeholders were supportive overall of introducing penalties and fines for violations of the Act. One stakeholder cautioned that the power to issue fines in the public sector context would amount to a "redistribution of public funds," and that giving the OPC power to issue orders in relation to activities involving personal information would likely be more effective.

Empowering Individuals

The OPC expressed the view that an individual's right to seek recourse before the Federal Court should not be limited to those matters that remain unresolved following an investigation under the Act. It recommended that this right be made available in three circumstances: (1) where a complainant has received the results of the OPC's investigation; (2) where this complainant has been informed of the OPC's decision to refuse or cease to investigate the complaint; (3) or where the complainant has not been informed of the result of the investigation or of a decision within six months of filing his or her complaint. The CBA, as well as several other stakeholders, also expressed support for a private right of action for individuals under the Act so they could bring matters directly before the Court themselves.

Considering Resource Implications

The OPC proposed that any new oversight measures in the Act should provide the OPC with sufficient discretion to support the proper allocation of its limited regulatory resources. One government institution raised similar concerns and noted that increased powers for the OPC would likely entail corresponding increases in compliance costs, which could strain government operations. This institution further suggested that the Act could provide federal public bodies with a period to assess and update their practices to comply with modernized legislation, once legislative amendments come into force.

Revisiting the Regulation of "Publicly Available" Personal Information

One stakeholder group suggested that individuals' degree of comfort with federal public bodies' collection, use and disclosure of "publicly available" personal information would vary depending on their existing level of confidence in the Government of Canada. This group also shared differing views on personal levels of comfort with activities involving publicly available information and regarded the issue as being complex and quite polarizing. However, there was a general consensus among stakeholders on the importance of subjecting publicly available personal information to the principles and requirements in the Act.

Applying all the Privacy Act's Rules to "Publicly Available" Personal Information

The OPC strongly supported the addition of specialized rules that would ensure the alignment of federal public bodies' activities involving publicly available personal information with individuals' reasonable expectations of privacy. The CBA shared similar views, but emphasized that federal public bodies should consider whether it is appropriate to collect personal information from publicly available sources in light of the nature of their mandates and programs. The CBA also provided a list of considerations for federal public bodies to assess in the context of handling publicly available personal information. These include, among other things, criteria for determining what constitutes publicly available and for determining appropriate retention periods, as well as for ensuring the conduct of PIAs in relation to the use and disclosure of publicly available information. The CBA went further, recommending that all collection of such information should be necessary to achieving a federal public body's mandate. Other stakeholders agreed that the Act's requirements should fully apply to publicly available personal information, and that guidance for federal public bodies would be beneficial. Some expressed concerns with including potential exceptions in the Act for law enforcement, national security, and intelligence activities that involve publicly available personal information.

Accessing One's Personal Information under the *Privacy Act*

A number of stakeholders provided their views both on the scope of the right to access personal information and on processing personal information requests.

Broadening the Scope of the Right to Request Access to Personal Information

Many stakeholders, including the CBA, academic and international stakeholders, as well as some private individuals, expressed support for broadening the scope of the right to request access to personal information to non-Canadians not physically located in Canada. The CBA noted that there was no principled basis to limit the scope of this right, and suggested that a pilot project could test the impact that broadening this right might have on public resources and on the ATIP system. There was a split among federal public bodies on this question – some supported the approach, while most expressed concerns about potential resource, volume and authentication issues, and some noted that the current volume of requests makes compliance with legislated timelines very challenging.

Dealing with Vexatious, Bad Faith or Abusive Requests

Most stakeholders supported introducing a mechanism in the Act that would allow federal public bodies to decline to respond to requests for personal information that are vexatious, made in bad faith, or otherwise an abuse of the right to make such a request. The OPC suggested that federal public bodies themselves should approve whether they would decline such requests, but that such decisions should be subject to the OPC's review powers, either

through complaints from individuals or under the OPC's discretionary investigative and audit powers.

Safeguarding Personal Information

All stakeholders who provided input on this issue spoke in support of the Act requiring federal public bodies to put in place robust technical, physical, administrative and legal safeguards for the protection of personal information. Stakeholders suggested that there should be set standards which take into consideration industry best practices and technologies for safeguarding personal information, such as clear encryption and storage requirements.

Many stakeholders, including the OPC, supported the proposal to introduce an express safeguarding principle in the Act. One stakeholder suggested that the Act should explicitly prohibit federal public bodies from actively undermining security protocols and tools and also require them to systematically consider cybersecurity best practices.

Most stakeholders called for a flexible, risk-based approach to safeguarding personal information. For example, many stakeholders held that safeguards should reflect the sensitivity of the personal information being protected. Opinion was divided on whether the Act should require sensitive personal information to be stored in Canada or whether it could be stored in another jurisdiction. Some stakeholders suggested that other means (such as ISAs) could be used to provide appropriate safeguards for personal information where it is being stored outside of Canada.

The OPC and some other stakeholders also supported the introduction of requirements to report legal breaches, including requirements for federal public bodies to keep records of any privacy breaches and to report them to both the OPC and any affected individual where there is a risk of significant harm.

Addressing the Needs and Expectations of Indigenous Peoples

Some Indigenous partners and non-Indigenous stakeholders provided submissions in the context of the online public consultation that discussed the unique impacts that potential changes to the *Privacy Act* could have for Indigenous Peoples in Canada. The use of the term Indigenous Peoples in this section reflects that the majority of the partners and stakeholders that provided comments on this topic did not specifically distinguish between First Nations, Metis, and Inuit in their comments.

Guiding Principles

Most of these partners and stakeholders emphasized the importance of Indigenous data sovereignty – that First Nations, Metis, and Inuit should have control over their personal

information and information relating to their communities (including de-identified and statistical demographic data).

Specific proposals for amending the *Privacy Act* included explicitly recognizing the Government of Canada's commitment to reconciliation, the OCAP® principles[2] and the *United Nations Declaration on the Rights of Indigenous Peoples* in the legislation's preamble. Some partners and stakeholders suggested that Justice Canada should further engage with Indigenous groups to determine whether there are specific concepts that may require additional and explicit protection within the *Privacy Act* (such as defining the concept of communal data or to address collective privacy rights).

Governance Mechanisms and Information-Sharing Agreements

Some partners and stakeholders suggested that the *Privacy Act* should allow for new governance mechanisms, which would allow Indigenous governing bodies to enter into ISAs with the Government of Canada. While they were of the view that governance mechanisms should be developed in consultation with national and regional Indigenous groups, these governance mechanisms could include a formal role for community input or third-party data stewards (such as the First Nations Indigenous Governance Centre). As well, information sharing agreements would need to balance Indigenous governments' rights of access to their members' information with appropriate protections for Indigenous individuals' personal information. These protections could include notice requirements, the opportunity for an individual to opt-out of this information disclosure, and specific offences for any privacy breaches.

Government of Canada's Use of Indigenous Individuals' Personal Information

Partners emphasized the need for greater transparency in how federal departments such as Indigenous Services Canada and Crown-Indigenous Relations and Northern Affairs Canada use Indigenous individuals' personal information. Partners and stakeholders suggested that the Government of Canada could further support Indigenous data governance by providing funding to Indigenous communities seeking to exercise control over their information and by providing training to government employees on Indigenous data governance.

Unique Risks

Some partners and stakeholders suggested that Indigenous individuals, and Indigenous women in particular, may face unique vulnerabilities when their personal information is shared in a law enforcement context. Some also raised the point that the risks of using de-

[2] OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC). See www.FNIGC.ca/OCAP-training/ for details.

identified personal information may be greater where it relates to Indigenous Peoples, as data from smaller communities may lead to increased risks of re-identification. One Indigenous partner suggested that the Privacy Commissioner's mandate be amended to include a duty to undertake an investigation where complaints relate to the disclosure of personal information "that may adversely affect individual or collective Indigenous rights or that create the risk of physical, psychological, social or political harm to an Indigenous person, with particular attention to the risk of violence toward Indigenous women and girls".

Survey Results

In all, 1,121 respondents, from all provinces and territories, participated in the online survey.[3] The highest proportions of respondents were from Ontario (39%), British Columbia (16%) and Quebec (13%). Almost three quarters (73%) of respondents had some level of familiarity with the *Privacy Act*, and over half (58%) had "some trust" or "a little trust" that the federal government is doing a good job protecting personal information.

Just under three quarters of respondents (72%) "strongly" or "somewhat" agreed that the private sector and federal government should be subject to the same rules when it comes to protecting personal information.

Respondents' comfort levels with their personal information being shared between government departments and agencies without consent differed depending on the reason for the information sharing. A majority of respondents were "somewhat comfortable" or "extremely comfortable" with personal information being shared to provide a service or benefit that they had requested (68%), to fulfil the purpose for which it was originally collected (57%), or to protect the integrity of a program by minimizing fraud or abuse (56%). Respondents were less comfortable ("totally uncomfortable" or "somewhat uncomfortable") with their information being shared to propose new or additional services (53%) or to carry out research in the public interest (51%).

Respondents expressed high levels of discomfort with their personal information being shared with foreign governments or with private sector for-profit businesses. This discomfort was evident whether the information would be used for the purpose it was originally collected for or for a different purpose. A majority were not supportive of their information being shared with a foreign government or a private sector for-profit business (92% "totally uncomfortable" or "somewhat uncomfortable"), even for the purpose for which it was originally collected. This was still higher for information used for a different purpose than it was collected for, with 96% of respondents "totally uncomfortable" or "somewhat

[3] A detailed analysis of survey results is available in Appendix A.

uncomfortable" with their information being shared with a foreign government, and the same proportion for a private sector for-profit business.

Most respondents felt that being able to access their personal data was an important aspect of protecting their privacy, with 87% "strongly" or "somewhat" agreeing. Respondents also agreed that federal public bodies should inform people when artificial intelligence is used to make decisions that affect them, with 86% "strongly" or "somewhat" agreeing. Respondents were not supportive of government using publicly available personal information such as that found on social media, with nearly two thirds of respondents (64%) "strongly" or "somewhat" disagreeing with this practice.

There was considerable support for proposed options to strengthen the powers of the Privacy Commissioner of Canada, mostly for the power to provide recommendations to federal departments and agencies on how to address potential privacy risks (91% "strongly" or "somewhat" agreed) and to assist them in assessing privacy risks when designing new programs or activities (90% "strongly" or "somewhat" agreed).

There was also very solid support for enhanced accountability and transparency measures. Almost all respondents felt that an accessible, easy-to-find privacy policy was important for their understanding of why and how government departments and agencies collect and use personal information (96% rating this as "moderately important" or "very important").As well, proper safeguarding of their information and knowing what personal information federal departments and agencies have and how they can use and share it were rated as "very important" or "moderately important" by 99% and 96% of respondents respectively.

KEY OPPORTUNITIES AND CHALLENGES GOING FORWARD

Securing Canadians' Trust

The online public consultation showed that, in the eyes of the Canadian public and most stakeholders, the *Privacy Act* lags substantially behind comparable personal information protection instruments elsewhere in Canada and internationally. The Act's definitions; its rules on the collection, use and disclosure of personal information; its treatment of "publicly available" personal information; the scope of its rules on who can request access to their personal information; its accountability and transparency frameworks, as well as its oversight regime – all these are widely seen as unlikely to meet the challenges of a modern, digital Canadian society. An overhaul of such elements, as proposed in Justice Canada's discussion paper, would help restore and secure Canadians' trust in their federal government's activities involving personal information.

Aligning Public and Private Sector Frameworks

Canada's federal private sector personal information protection framework is seen by key stakeholders as providing useful points of reference for modernizing the Act. For instance, its principles-based approach to the regulation of personal information, as well as its more modern oversight and enforcement framework could inspire amendments to the Act. Further, Canadians and other stakeholders have consistently signaled their support for a much closer alignment between the federal public and private frameworks for the protection of personal information.

Harnessing Innovation in the Public Interest

Canadians and other stakeholders showed support for various approaches to addressing the widespread view that technological innovation can also give rise to increased privacy risks. Justice Canada heard that federal public bodies' activities involving either de-identified or "publicly available" personal information collected digitally, as well as their increasing reliance on automated decision-making tools, were top-of-mind for most stakeholders. On one hand, Canadians and other stakeholders recognize, and even welcome, the benefits of advanced technology for carrying out government activities in the public interest. On the other hand, they insist that those benefits should not come at the cost of protecting Canadians' privacy. Including improved transparency requirements as well as stronger oversight mechanisms in a modernized Act would help to address these concerns.

CONCLUSION

The online public consultation provided Justice Canada with a deeper understanding of the perspectives of the federal Privacy and Information Commissioners, federal public bodies, private sector stakeholders, academics, Indigenous partners and the Canadian public on a set of core issues. These views will be instrumental in helping the Government develop proposals for amending the *Privacy Act* so that it meets the privacy challenges Canada faces today, and into the future.

Appendix A – Analysis of Survey Results

As part of the Government of Canada's consultation on the federal *Privacy Act,* Canadians were invited to participate in an online survey to share their views on key issues related to privacy. The survey was open to the public from November 16, 2020, to February 14, 2021, and received 1,121 responses. An overwhelming majority of the respondents – 1,029 – chose to participate in English (92%). Only 92 respondents participated in French (8%). Survey results are presented below, starting with voluntary demographic questions and then following the order questions appeared in the survey. Throughout the report, percentages may not add up to 100% due to rounding.

Demographics

Survey respondents were asked what province/territory they reside in. Table 1 shows that the highest proportion of respondents were from Ontario (39%), followed by British Columbia (16%), Quebec (13%), and Alberta (11%). Respondents were also asked whether they lived in an urban or rural area. Almost three quarters of respondents (73%) indicated that they lived in an urban area, while 15% said they lived in a rural area. The remaining 12% did not provide a response.

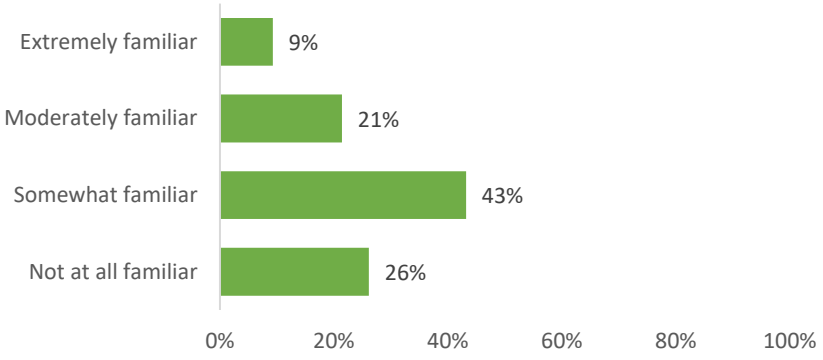
Table 1 – Respondents' province/territory of residence

	n (%)
Newfoundland and Labrador	7 (1)
Nova Scotia	39 (4)
New Brunswick	14 (1)
Prince Edward Island	4 (0)
Quebec	144 (13)
Ontario	439 (39)
Manitoba	40 (4)
Saskatchewan	33 (3)
Alberta	125 (11)
British Columbia	176 (16)
Territories	6 (1)
Prefer not to say/Not sure/skipped	94 (8)
TOTAL	1,121 (100)

Familiarity with the *Privacy Act*

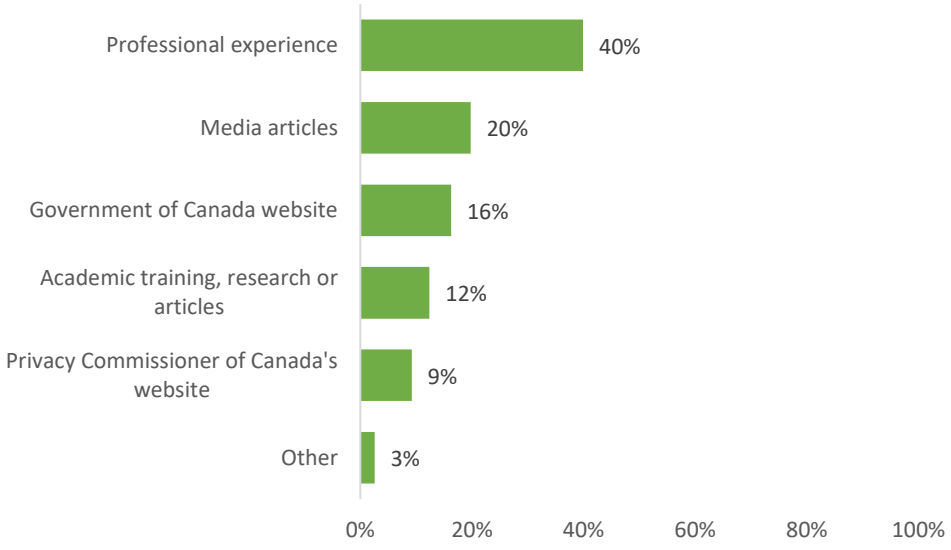
Respondents were asked to rate their level of familiarity with the *Privacy Act* on a four-point scale. Chart 1 shows that almost three quarters (73%) of respondents had some level of familiarity (extremely, moderately or somewhat familiar) with the Act. Less than half (43%) considered themselves "somewhat familiar," while 21% felt they were "moderately familiar" with the Act, and 9% felt they were "extremely familiar."

Chart 1 – Respondents' familiarity with the *Privacy Act*
n=1,121



Respondents who said they had some familiarity (extremely, moderately or somewhat familiar) (n=824) were asked about their main source of knowledge of the *Privacy Act*. Chart 2 shows that 40% of these respondents considered professional experience to be their main source of knowledge, followed by 20% of respondents who indicated that their main source was media articles and 16% who said it was a Government of Canada website.

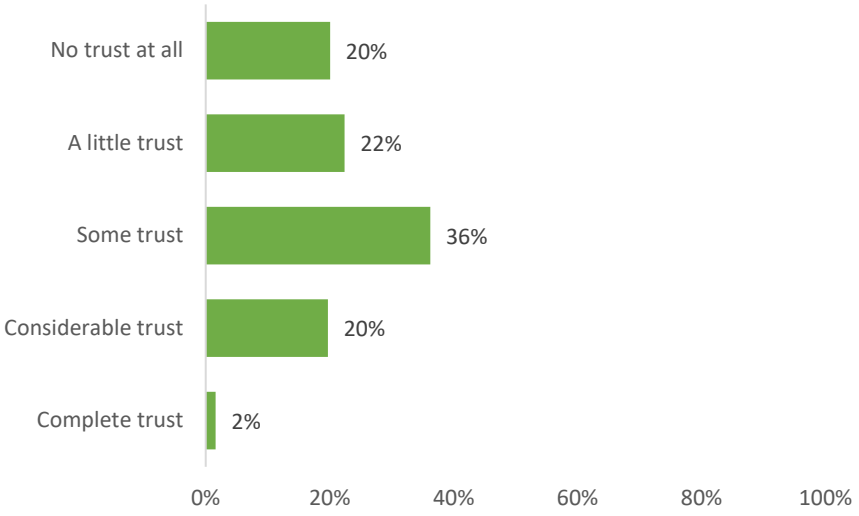
Chart 2 - Respondents' main sources of knowledge of the *Privacy Act*
n=824



Respondents were next asked, "To what extent do you trust that the federal government is doing a good job protecting your personal information?" Most respondents fell in the mid-range, with 58% having "some trust" (36%) or "a little trust" (22%) that the federal

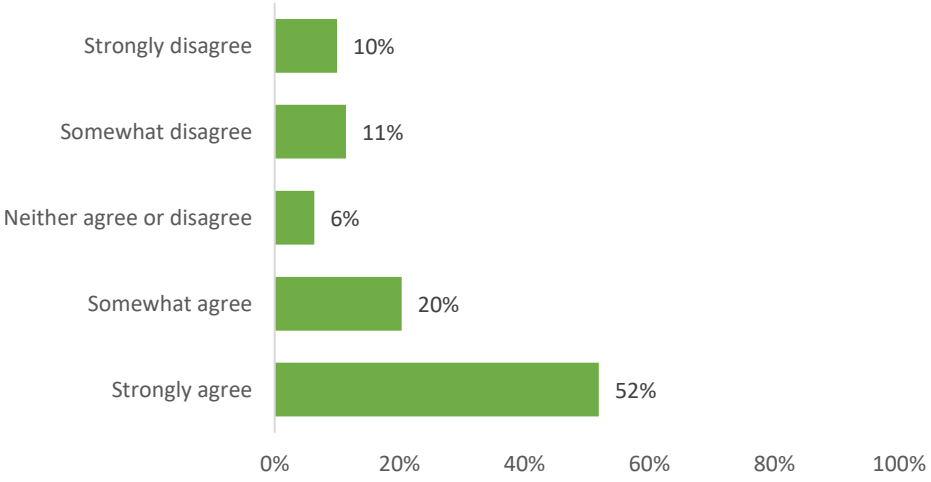
government is doing a good job (Chart 3). Less than a quarter of respondents (20%) said they had “no trust at all” in the government’s handling of personal information.

Chart 3 - Respondents' trust that the federal government is doing a good job protecting their personal information
n=1,121



When asked about the rules governing the private sector versus the public sector in protecting personal information, almost three quarters of respondents “strongly” (52%) or “somewhat” agreed (20%) that the private sector and federal government should be subject to the same rules (Chart 4).

Chart 4 - Respondents' level of agreement that the private sector and federal government should be subject to the same rules for protection of personal information
n=1,121



Sharing of personal information between federal government departments and agencies

Survey respondents provided their views on the sharing of personal information between federal government departments and agencies without permission. Table 2 shows respondents' views on personal information being shared between departments and agencies under nine different scenarios. Over two thirds of respondents (68%) were "somewhat comfortable" or "extremely comfortable" with their information being shared without permission when it is to provide a service or benefit that was requested. Fifty-seven percent (57%) of respondents were "somewhat comfortable" or "extremely comfortable" with their information being shared to fulfil the purpose for which it was originally collected or to protect the integrity of a program by minimizing fraud or abuse (56%).

Around half of respondents were "totally uncomfortable" or "somewhat uncomfortable" with their information being shared to propose new or additional services (54%) or to carry out research in the public interest (51%).

TABLE 2 – RESPONDENTS' VIEWS ON FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES SHARING THEIR PERSONAL INFORMATION WITH EACH OTHER, WITHOUT PERMISSION (N=1,121)

	Totally uncomfortable N (%)	Somewhat uncomfortable N (%)	Neutral N (%)	Somewhat comfortable N (%)	Extremely comfortable N (%)
TO FULFIL THE PURPOSE FOR WHICH THE INFORMATION WAS ORIGINALLY COLLECTED.	235 (21)	155 (14)	95 (9)	333 (30)	303 (27)
TO PROVIDE ME WITH A SERVICE OR BENEFIT THAT I HAVE REQUESTED.	153 (14)	112 (10)	104 (10)	378 (34)	374 (34)
TO ELIMINATE THE NEED FOR ME TO PROVIDE THE SAME INFORMATION AGAIN.	209 (19)	174 (16)	145 (13)	362 (32)	231 (21)
TO PROPOSE NEW OR ADDITIONAL SERVICES I MAY BE INTERESTED IN.	346 (31)	252 (23)	200 (18)	243 (22)	80 (7)
TO SUGGEST OTHER BENEFITS TO WHICH I MAY BE ENTITLED BUT AM NOT AWARE OF.	196 (18)	173 (15)	160 (14)	391 (35)	201 (18)
TO PROTECT THE INTEGRITY OF A PROGRAM BY MINIMIZING FRAUD OR ABUSE.	175 (16)	144 (13)	170 (15)	360 (32)	272 (24)
TO ANALYZE THE OPERATION OF A PROGRAM OR BENEFIT PROGRAM.	258 (23)	230 (21)	234 (21)	275 (25)	124 (11)
TO CARRY OUT RESEARCH IN THE PUBLIC INTEREST.	340 (30)	230 (21)	171 (15)	260 (23)	120 (11)
TO USE IT FOR ANY PURPOSE, BUT ONLY WHERE THE PERSONAL INFORMATION WAS DE-IDENTIFIED.	270 (24)	197 (18)	153 (14)	318 (28)	183 (16)

There was notable support for the use of formal written agreements for sharing personal information. Over three quarters of respondents indicated they “strongly” (51%) or “somewhat” agreed (27%) that federal government departments and agencies should enter into formal written agreements to share personal information with each other (Chart 5a).

Chart 5a - Respondents' level of agreement that federal government departments and agencies should enter into formal written agreements to share personal information with each other

n=1,121

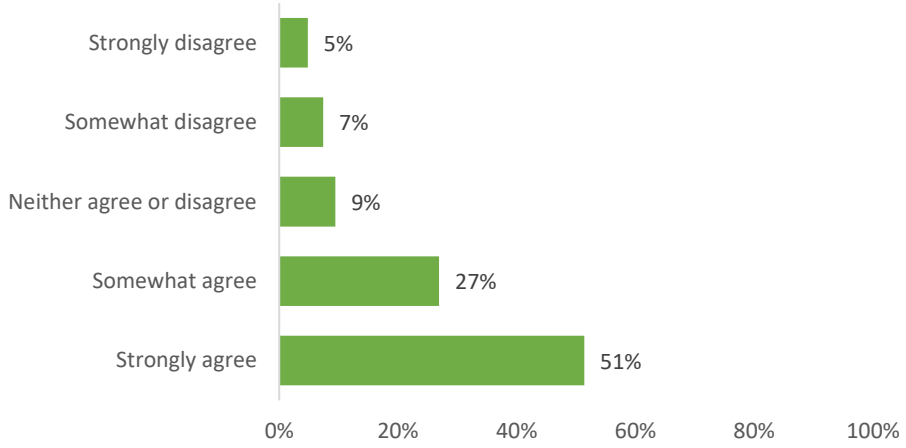


Chart 5b shows respondents’ willingness to change their answer to the question about written agreements under certain scenarios. Overall, a low proportion of respondents indicated they would change their answer to this question in all four scenarios presented. The scenario where respondents were most willing to change their view on the need for formal written agreements was when the reason for sharing the information was for the purpose for which it was originally intended (31%).

Chart 5b - Respondents' willingness to change their view on the need for formal written agreements for information sharing under certain scenarios
n=1,121

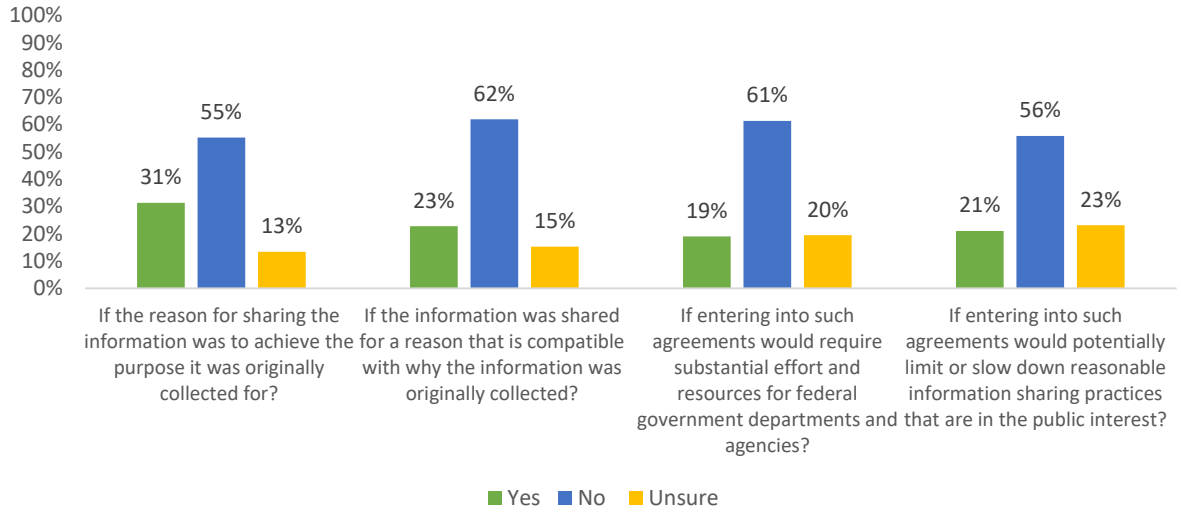
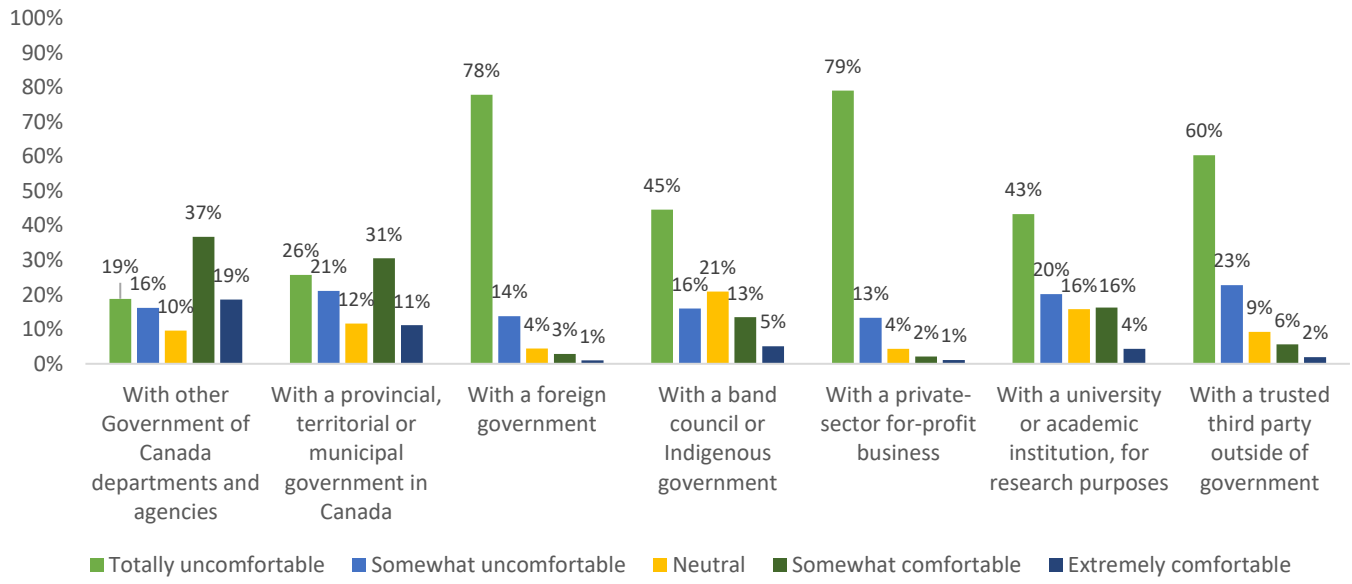


Chart 6 shows respondents' views on federal departments and agencies sharing their personal information with different entities when the information is to be used to carry out the purpose for which it was originally collected. The highest proportion of respondents were comfortable with their information being shared with other Government of Canada departments or agencies. Over half (56%) of respondents were "somewhat comfortable" or "extremely comfortable" with this type of information sharing. Information sharing with provincial, territorial or municipal governments was also viewed favourably to some degree, with 42% being "somewhat comfortable" or "extremely comfortable." More than nine in ten respondents were not supportive of their information being shared with a foreign government (92% "totally uncomfortable" or "somewhat uncomfortable") or with a private sector for-profit business (92% "totally uncomfortable" or "somewhat uncomfortable").

Chart 6 – Respondents' views on federal departments/agencies sharing their personal information with different entities to carry out the purpose the information was originally collected for (n=1,121)



When looking at personal information being shared with other entities for reasons that are different from those for which it was originally collected, respondents were generally uncomfortable. Chart 7 shows that more than nine in ten respondents (96%) were "totally uncomfortable" or "somewhat uncomfortable" with their information being shared with a foreign government to carry out a purpose different from the original one. The same proportion (96%) were "totally uncomfortable" or "somewhat uncomfortable" with their information being shared with a private sector for-profit business.

Respondents were slightly less concerned about this type of information sharing when it involved other Government of Canada departments and agencies (72% were "totally uncomfortable" or "somewhat uncomfortable") or with provincial, territorial or municipal governments (75% were "totally uncomfortable" or "somewhat uncomfortable").

Chart 7 - Respondents' views on federal departments/agencies sharing their personal information with different entities to carry out a purpose different from what the information was originally collected for (n=1,121)

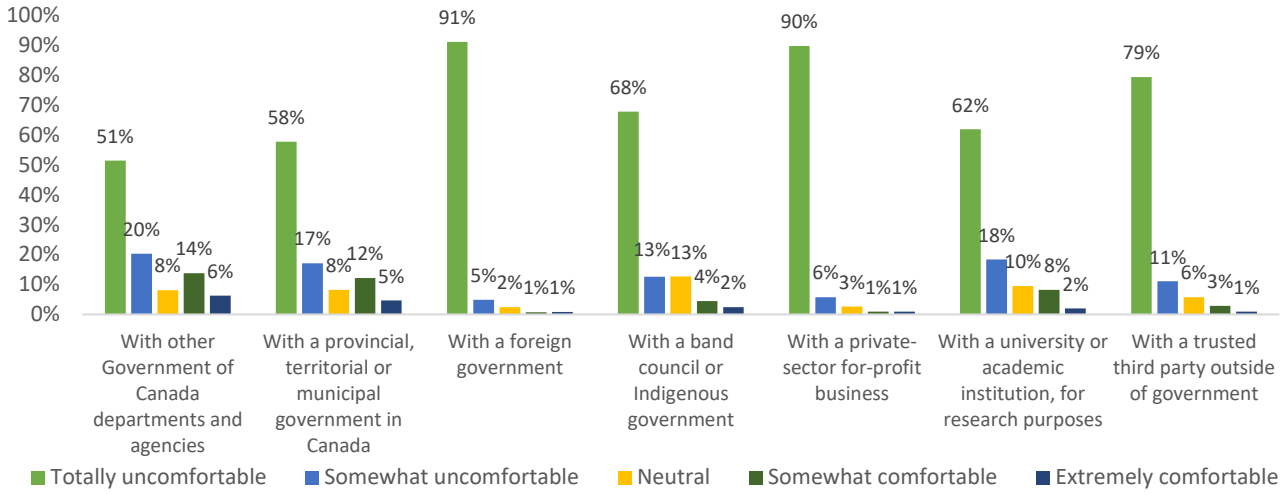
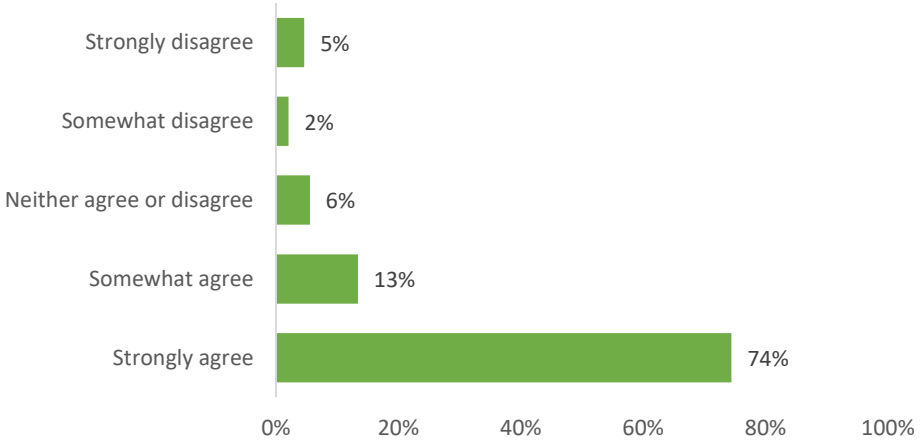


Chart 8 outlines respondents' views on whether being able to request access to their personal information from a federal government department or agency is an important aspect of privacy protection. Just under nine in ten respondents (87%) either "strongly" or "somewhat" agreed that being able to access their personal data is an important aspect of protecting privacy.

Chart 8 - Respondents' level of agreement that being able to request access to their personal information from a federal government department or agency is an important aspect of protecting privacy
n=1,121

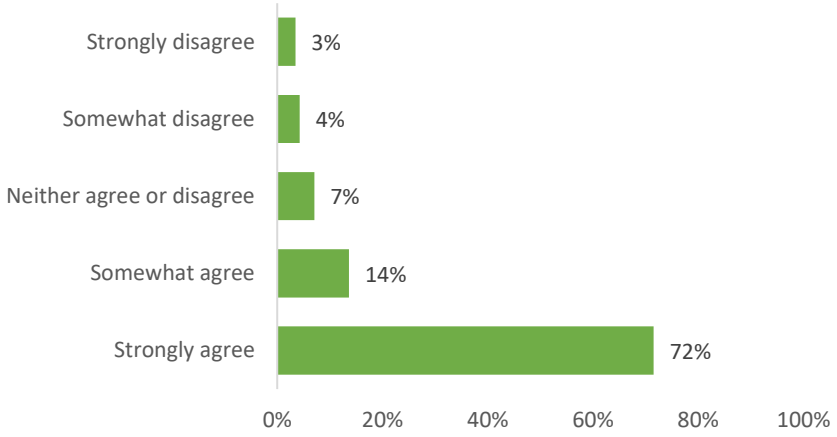


Use of automated decision making and publicly available personal information

Respondents indicated that they would want to be informed when artificial intelligence is used to make decisions about them. When asked about the use of automated decision making and artificial intelligence, 86% of respondents indicated they "strongly" or "somewhat" agreed that federal departments and agencies should inform people when artificial intelligence is used to make decisions that affect them (Chart 9).

Chart 9 - Respondents' level of agreement that federal government departments and agencies should inform citizens when they use artificial intelligence to make a decision that affects them

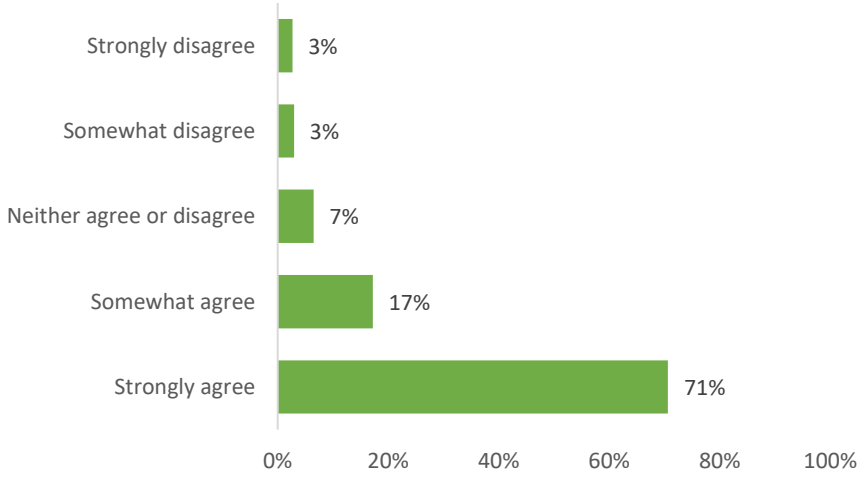
n=1,121



Respondents were asked about the extent to which they agreed with the statement "I should be able to request human involvement in a decision-making process about me that relies on computerized automated processes, such as artificial intelligence." Chart 10 shows that almost nine in ten respondents either "somewhat" (17%) or "strongly" (71%) agreed that they should be able to request human involvement in this type of decision making.

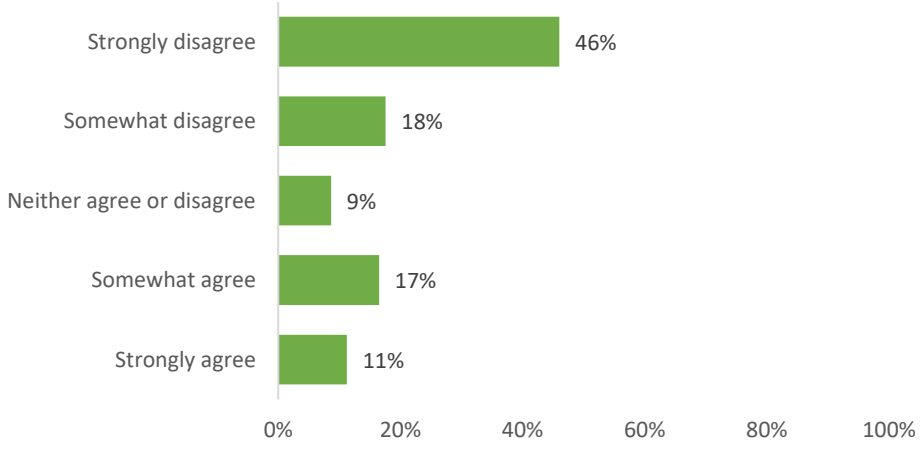
There was a follow-up question asking if the response about automated decision making would change if the decision would otherwise take longer to make or would entail higher costs. Most respondents indicated they would not change their view. Almost eight in ten respondents (78%) felt their response would not change even if it meant the decision would take longer (11% said their decision would change, and 12% were unsure). Seven in ten (70%) felt their response would not change even if it meant higher costs for them or the government of Canada (14% said their decision would change, and 16% were unsure).

Chart 10 - Respondents' level of agreement that people should be able to request human involvement in decision-making processes that rely on computerized automated processes
n=1,121



When asked about government use of publicly available personal information, such as that found on social media, there was less consensus among respondents. Almost two thirds (64%) either "strongly" or "somewhat" disagreed that federal government departments and agencies should be free to collect and use personal information that is publicly available, including information on social media (Chart 11).

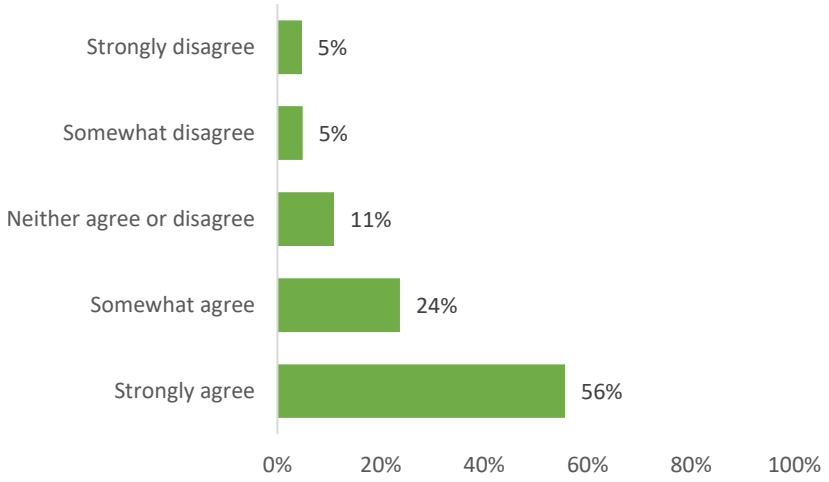
Chart 11 - Respondents' level of agreement that federal government departments/agencies should be free to collect, use and share personal information that is readily available to the public, including information from social media
n=1,121



Privacy Act Modernization

In the survey, respondents were informed that a chief privacy officer is responsible for supporting an organization's compliance with applicable privacy legislation and for helping develop internal privacy guidance and tools tailored to an organization. Chart 12 shows the extent to which respondents agreed that federal departments and agencies should have an internal chief privacy officer. Most respondents were supportive, with eight in ten either "strongly" (56%) or "somewhat" agreeing (24%) that federal departments and agencies should have an internal chief privacy officer.

Chart 12 - Respondents' level of agreement that each federal government department or agency should have an internal Chief Privacy Officer
n=1,121



Under the *Privacy Act*, the Privacy Commissioner is an officer of Parliament who investigates complaints and reports on their findings. Currently, the Privacy Commissioner can make recommendations to federal departments and agencies on their treatment of an individual's personal information. The Privacy Commissioner can also bring to the Federal Court matters relating to refusals by federal departments and agencies to provide access to personal information.

Respondents were asked whether they agreed or disagreed with various powers that could be granted to the Privacy Commissioner of Canada. Table 3 outlines respondents' views on this question. There was considerable support for all options, though the highest level of support was for the Privacy Commissioner having the power to provide recommendations to federal departments and agencies on how to address potential privacy risks (91% "strongly" or "somewhat" agreed). The second most frequently chosen option was the Privacy Commissioner having the power to assist federal departments and agencies in assessing

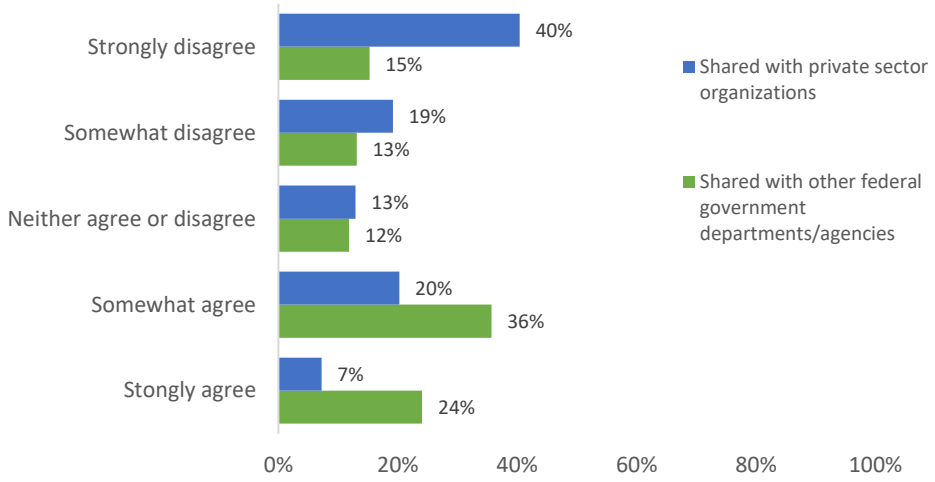
privacy risks when designing new programs or activities (90% “strongly” or “somewhat” agreed).

TABLE 3 – RESPONDENTS’ VIEWS ON AUTHORITIES THAT COULD BE GRANTED TO THE PRIVACY COMMISSIONER OF CANADA (N=1,121)

	Strongly disagree N (%)	Somewhat disagree N (%)	Neither agree or disagree N (%)	Somewhat agree N (%)	Strongly agree N (%)
Providing guidance on how the *Privacy Act* should be interpreted and applied.	46 (4)	54 (5)	100 (9)	348 (31)	573 (51)
Providing advance views on how the privacy commissioner might address an issue if someone were to complain about it.	44 (4)	50 (5)	135 (12)	385 (34)	507 (45)
Assisting federal government departments and agencies in assessing privacy risks when designing new programs or activities.	36 (3)	9 (1)	66 (6)	289 (26)	721 (64)
Providing recommendations to federal government departments and agencies on how to address potential privacy risks they face.	30 (3)	12 (1)	64 (6)	281 (25)	734 (66)
Entering into legally binding and enforceable compliance agreements with federal government departments and agencies regarding the handling of personal information.	48 (4)	59 (5)	120 (11)	295 (26)	599 (53)
Ordering government departments and agencies to provide access to personal information after investigating a complaint.	63 (6)	81 (7)	145 (13)	253 (23)	579 (52)
Ordering government departments and agencies to stop collecting, using or disclosing personal information after a complaint.	31 (3)	32 (3)	106 (9)	235 (21)	717 (64)

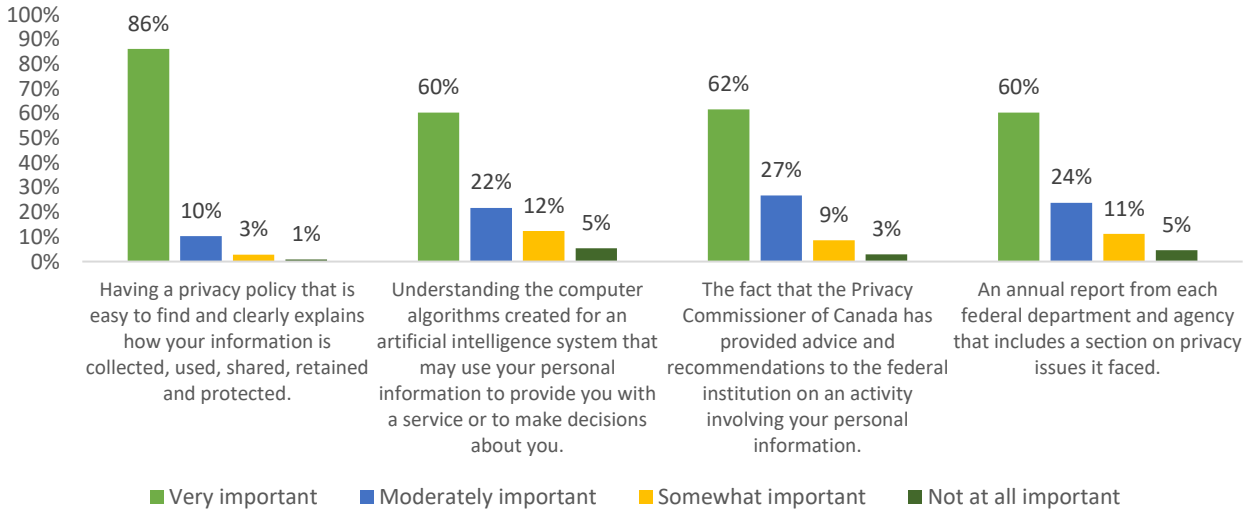
De-identified personal information is data from which personal identifying information has been removed so that the risk of identifying an individual is extremely low. Respondents were asked their views on federal government departments and agencies sharing de-identified personal information to encourage innovation in the public interest. Chart 13 shows that respondents’ views differed depending on where the data would be shared. There was a fairly high level of support (60% of respondents selected either “somewhat agree” or “strongly agree”) for de-identified personal information being shared with other federal government departments and agencies, while only 27% had the same level of agreement for sharing with private sector organizations.

Chart 13 - Respondents' views on federal government departments/agencies sharing de-identified data to encourage innovation in public interest
n=1,121



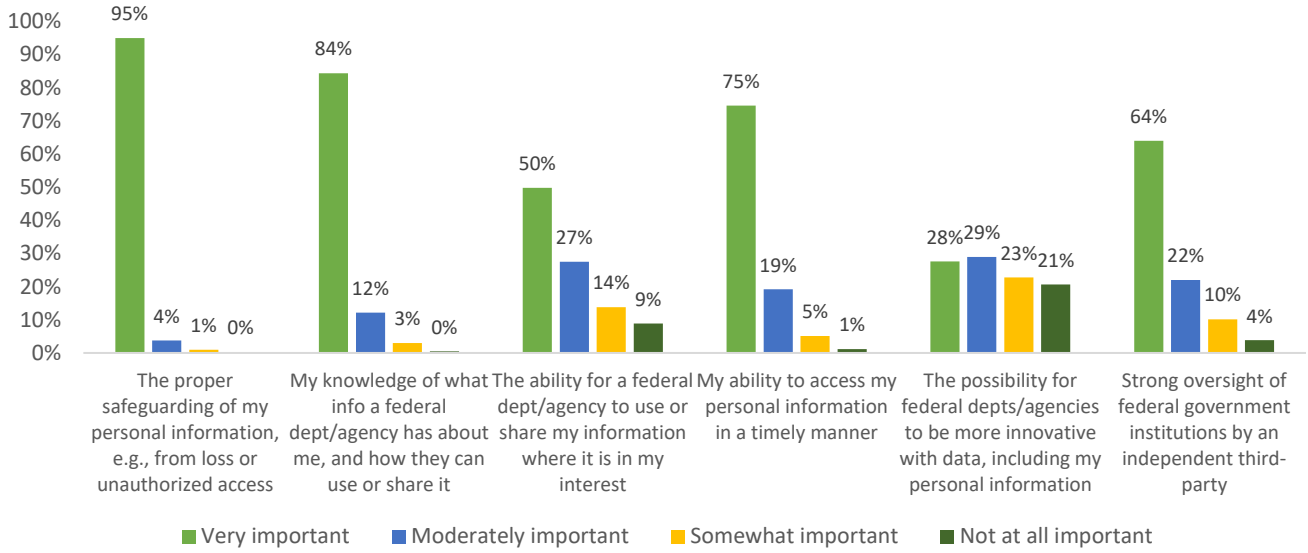
Respondents were asked to rate the level of importance of various areas to their understanding of why and how a federal government department or agency collects, uses or shares personal information. Respondents felt that having an accessible, easy-to-find privacy policy was most important, with 96% rating this as “moderately important” or “very important” (Chart 14). The next most important area was knowing that the Privacy Commissioner of Canada had provided advice and recommendations to the federal institution on an activity involving their personal information, with 89% rating this as “moderately important” or “very important.”

Chart 14 – Respondents’ views on the importance of the following areas to their understanding of why and how a federal government department or agency collects, uses or shares personal information (n=1,121)



When asked to rate the importance of various aspects of *Privacy Act* modernization, one area was overwhelmingly rated as important: 99% of respondents felt that proper safeguarding of personal information was pivotal to *Privacy Act* modernization, with 95% rating it as "very important" and 4% as "moderately important." The next most important area was knowing what personal information federal departments and agencies have and how they can use and share it, with 96% rating this as "very important" or "moderately important" (Chart 15).

Chart 15 – Respondents' views on importance of various aspects of *Privacy Act* modernization
(n=1,121)



The final survey question allowed respondents to share additional comments on elements not covered in the survey. There were 342 comments provided. Several themes emerged from a qualitative review of responses. The most common theme was the importance of including adequate powers and consequences for violations in a modernized *Privacy Act.* Comments also emphasized that Canadians should have access to their own data as well as the ability to have their data removed or deleted from government databases. Respondents were also concerned that true data de-identification may not be possible, so questions around sharing de-identified personal information should be viewed with this in mind. Finally, the European Union approach to privacy modernization was raised as a model for Canada to follow.