Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the *Digital Charter Implementation Act, 2022*

April 2023

Table of contents

I. OPC's 15 key recommendations on Bill C-27

Recommendation #1: Recognize privacy as a fundamental right.

Recommendation #2: Protect children's privacy and the best interests of the child.

Recommendation #3: Limit organizations' collection, use and disclosure of personal information to specific and explicit purposes that take into account the relevant context.

Recommendation #4: Expand the list of violations qualifying for financial penalties to include, at a minimum, appropriate purposes violations.

Recommendation #5: Provide a right to disposal of personal information even when a retention policy is in place.

Recommendation #6: Create a culture of privacy by requiring organizations to build privacy into the design of products and services and to conduct privacy impact assessments for high-risk initiatives.

Recommendation #7: Strengthen the framework for de-identified and anonymized information.

Recommendation #8: Require organizations to explain, on request, all predictions, recommendations, decisions and profiling made using automated decision systems.

Recommendation #9: Limit the government's ability to make exceptions to the law by way of regulations.

Recommendation #10: Provide that the exception for disclosure of personal information without consent for research purposes only applies to scholarly research.

Recommendation #11: Allow individuals to use authorized representatives to help advance their privacy rights.

Recommendation #12: Provide greater flexibility in the use of voluntary compliance agreements to help resolve matters without the need for more adversarial processes.

Recommendation #13: Make the complaints process more expeditious and economical by streamlining the review of the Commissioner's decisions.

Recommendation #14: Amend timelines to ensure that the privacy protection regime is accessible and effective.

Recommendation #15: Expand the Commissioner's ability to collaborate with domestic organizations in order to ensure greater coordination and efficiencies in dealing with matters raising privacy issues.

II. Introduction

The Office of the Privacy Commissioner of Canada (OPC) welcomes the opportunity to provide this submission to Parliament on Bill C-27, the *Digital Charter Implementation Act, 2022*.

Bill C-27 was tabled on June 16, 2022, and would repeal Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and enact the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* (PIDPTA) and the *Artificial Intelligence and Data Act* (AIDA). The Bill follows the former Bill C-11, *The Digital Charter Implementation Act, 2020,* which also proposed amendments to PIPEDA and died on the Order Paper when Parliament was dissolved on August 15, 2021 in advance of the 2021 federal election.

The OPC is encouraged by the introduction of Bill C-27 which is a recognition by the Government that Canadians need and expect modernized privacy laws that support innovation and enable Canadians to enjoy the many benefits of technology with the reassurance that their personal information will be protected. Canadians should not have to choose between their participation in the digital economy and their fundamental rights.

Bill C-27 is an important step toward meeting this challenge, establishing stronger privacy protections for individuals and creating incentives for organizations to comply while allowing greater flexibility to innovate. It is, in many ways, an improvement over both the PIPEDA and the former Bill C-11. The Bill addresses several concerns and recommendations raised by this Office and others. Some of the positive developments include:

- The addition of a preamble to offer guidance on the law's broader objectives;
- New provisions to help protect the privacy of minors;
- An expansion of personal information that individuals can request be disposed of;
- Amendments to require that information to obtain valid consent be presented in understandable language;
- Amendments that grant increased discretion to the OPC, for example in relation to complaints and investigations;
- An expanded requirement to ensure that the manner in which personal information is collected, used and disclosed is appropriate;
- An amendment to accountability measures requiring organizations to maintain privacy management programs;
- A new requirement to authenticate identity as part of security safeguarding requirements;
- A reversal of problematic modifications to the definition of "commercial activity" introduced in the former Bill C-11;

- An enhanced requirement for members of the proposed Personal Information and Data Protection Tribunal to have privacy experience;
- An expanded list of contraventions to which administrative monetary penalties (AMPs) may apply; and
- Measures to regulate artificial intelligence (AI) with the introduction of the *Artificial Intelligence and Data Act* (AIDA).

With these changes, we believe that Bill C-27 is a step in the right direction. Encouraging innovation in a privacy protective manner will help increase individuals' privacy and control over their personal information, as well as their trust and ability to realize the benefits of the online economy.

However, despite the positive aspects of the Bill, the OPC believes that it can and must be further improved. There are a number of important changes that we believe are necessary to ensure that Canadians' privacy rights are better protected in the digital environment, to serve innovation and to avoid leaving too much to be determined through regulation.

The Privacy Commissioner of Canada, Philippe Dufresne, has shared his intent to promote and implement a vision of privacy that recognizes:

1. Privacy as a fundamental right;
2. Privacy in support of the public interest and Canada's innovation and competitiveness; and
3. Privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens.

The OPC has reviewed and assessed Bill C-27 through this lens. In addition, we have heard from civil society groups and representatives from the private sector which has helped to inform our recommendations on how the Bill can be improved.

Privacy law reform is overdue and must be achieved. With this in mind, the OPC makes 15 key recommendations that are necessary to further protect the privacy of Canadians while supporting the digital economy.

With the key concerns raised in this submission addressed, the OPC has both confidence and optimism that a stronger legislative framework will emerge that will further individuals' fundamental right to privacy, allow Canadians to participate fully in the digital economy, support innovation, and help position Canada as a leader in this important and evolving area.

Should Parliament wish to consider additional ways to further enhance the Bill, it may refer to suggestions made by the OPC in response to the former Bill C-11 which remain relevant under Bill C-27. These are listed in Appendix A to this Submission.

III. Privacy as a fundamental right

Privacy is both a fundamental right in itself, and is instrumental to the exercise of other rights. In this submission, the OPC makes recommendations and proposes amendments in the following five areas to advance this broader theme:

- Privacy as a fundamental right;
- Children's privacy and the rights of the child;
- Appropriate purposes;
- Administrative monetary penalties; and
- Disposal.

Privacy as a fundamental right

Recommendation #1: Recognize privacy as a fundamental right.

There is no question that the addition of a preamble in Bill C-27 is a positive development that will offer much needed guidance to the courts about the law's objectives and constitutional basis. That said, the preamble does not go far enough in recognizing the fundamental right to privacy and could create a challenge for the courts when assessing economic interests and privacy. We heard from stakeholders in civil society who echoed this sentiment and shared the view that Bill C-27 should go further in recognizing privacy as a fundamental right.

The new English version of the preamble recognizes that the protection of privacy "interests" is "essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada." In contrast, the French version of the preamble uses the phrase "droit à la vie privée des individus" (privacy rights of individuals). The preamble ought to use terminology that highlights the fact that we are dealing with "rights", rather than "interests", in both official languages.

A stronger recognition in the law of the importance of the fundamental right to privacy is necessary to foster greater consumer confidence in the digital economy and encourage responsible use of personal information by organizations in a way that supports innovation and economic growth. The OPC believes that the law can achieve both commercial objectives and privacy protection in the pursuit of responsible innovation. However, in those rare circumstances where the two are in an unavoidable conflict, privacy rights should prevail.

The English version of the purpose clause already refers to the "right of privacy"; the French version uses the phrase "droit à la vie privée". Explicitly referring to the "fundamental right to privacy of individuals" in the English version of the preamble of C-27 and the purpose clause of the CPPA would strengthen this recognition. The same

would be true of adding the qualifier "fondamental" within the phrase "droit à la vie privée" in the French versions of C-27's preamble and the purpose clause of the CPPA. It would not, in the OPC's view, affect the constitutional validity of the Act and would create more congruence between these two parts. Characterising privacy as a fundamental right would also be consistent with international human rights instruments that recognize the right to privacy and with the Supreme Court of Canada's jurisprudence.[1] The Supreme Court of Canada has confirmed time and time again that legislation aiming to protect the control of personal information should be characterized as "quasi-constitutional" because of privacy's fundamental role in preserving a free and democratic society.[2]

We note that this was recently recommended by the Standing Committee on Access to Information, Privacy and Ethics (ETHI) in its November 2022 report on Device Investigative tools used by the RCMP.[3]

The OPC further notes that as drafted, the preamble appears only in the introductory text of Bill C-27 itself and not at the beginning of the CPPA, PIDPTA or AIDA. In other words, it appears that, once enacted, these Acts would not have preambles. While the OPC supports the addition of the preamble in Bill C-27, it should be embedded in Parts 1 through 3 inclusively of the *Digital Charter Implementation Act, 2022,* to ensure that it is not overlooked in the future.

Proposed amendments

- Amend the English version of the preamble as follows:
  - Paragraph 2: Whereas the protection of the fundamental right to privacy ~~interests~~ of individuals with respect to their personal information is essential…
  - Paragraph 3: Whereas Parliament recognizes the importance of the privacy and data protection principles contained in various international instruments including international human rights instruments that recognize privacy as a fundamental right;

[1] See *Douez v. Facebook, Inc*., 2017 SCC 33 at para. 105, per Abella J., concurring. Without using the language of "fundamental right" the Supreme Court has also referred to privacy of being a fundamental value or of being of paramount importance: *R. v. Jarvis*, 2019 SCC 10 at para. 66; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para. 19. See also *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2001 FCA 56 at para 20; reversed but not on this point in *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at para 10.
[2] *Ibid*.
[3] Recommendation 4, Device Investigative Tools Used by the Royal Canadian Mounted Policy and Related Issues, Report of the Standing Committee on Access to Information, Privacy and Ethics, November 2022.

- Amend the French version of the preamble as follows:
  - Paragraph 2: que la protection du droit fondamental à la vie privée des individus en ce qui a trait à leurs renseignements personnels est essentielle…
  - Paragraph 3 : que le Parlement reconnaît l'importance des principes de protection de la vie privée et des données qui sont exprimés dans divers instruments internationaux, y compris les instruments internationaux en matière de droits de la personne qui reconnaissent le droit à la vie privée comme un droit fondamental;

- Amend s. 5 of the CPPA as follows:
  - The purpose of this Act is to establish – in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information – rules to govern the protection of personal information in a manner that recognizes the fundamental right to ~~of~~ privacy of individuals…

- Embed the text of the preamble in Parts 1 through 3 inclusively of the *Digital Charter Implementation Act, 2022*.

Children's privacy and the rights of the child

Recommendation #2: Protect children's privacy and the best interests of the child.

The preamble should also reflect the importance of protecting children and minors. Jurisdictions around the world have recognized that children and minors may be impacted by technologies differently than adults, be at greater risk of being affected by privacy-related issues, and therefore require special protections. One of the CPPA's improvements over the former Bill C-11 relates to new measures specific to minors; this key element should also be reflected in the preamble.

The OPC supports these new measures, including the CPPA's clarification that minors' information is sensitive, as this is consistent with its past positions and expectations as expressed in guidance. However, in the OPC's view, these measures do not offer sufficient protection as they would not necessarily prohibit uses that could be harmful, such as using information to nudge children to turn off privacy controls or for behavioural or targeted advertising.

In the absence of specific prohibitions or "no-go" zones related to minors' data, the OPC recommends that the preamble recognize that the processing of personal data should respect children's privacy and the best interests of the child.

Updating the preamble in such a manner would encourage organizations to build privacy for children into products and services, from the start and by design. Since Canada's privacy laws were designed to be technology neutral, this would help ensure that the best interests of children will be considered for new and emerging technologies, and for future uses of data. It would also act as a further interpretive tool in cases dealing with requests by children to dispose of their personal information online and when considering new or emerging technologies such as sophisticated nudging techniques that encourage children to engage in potential harmful activities such as volunteering more data or turning off privacy controls, or for behavioural or targeted advertising. As UNICEF notes in its Policy guidance on AI for children, children are biologically and psychologically distinct from adults and are impacted by these technologies to a greater extent than adults.[4] Protecting children in the digital world means allowing them to be children in that world, with appropriate protections for their safety and reputations.

As the preamble would apply to all the Acts comprised in Bill C-27, including the CPPA and AIDA, adding the proposed language to the section that frames the legislation's intent would help ensure that the best interests of children and minors are prioritized and consistently considered across all the related Acts. The law should recognize the rights of the child, and the right to be a child. That means interpreting the privacy provisions in the legislation in a way that is consistent with the best interests of the child.

Proposed amendments

- Amend both the English and French versions of the preamble to add:
  - Whereas the processing of personal data should respect children's privacy and the best interests of the child.

Appropriate purposes

Recommendation #3: Limit organizations' collection, use and disclosure of personal information to specific and explicit purposes that take into account the relevant context.

Section 12 of the CPPA sets out a normative framework for organizations to determine what is, and what is not, a reasonable collection, use or disclosure of personal information.

[4] UNICEF, Policy guidance on AI for children, November 2021.

Section 12 sets out factors that must be considered when determining the appropriateness of the purpose. The challenge with this approach is that the assessment of appropriateness may vary by context. PIPEDA does not enumerate or require a list of factors to be satisfied. Rather, the factors have developed over time, experience and through case law. The OPC frequently considers some, but not necessarily all, of the factors listed and there may be occasions where additional factors are relevant. A list of factors is useful, but it should be non-exhaustive as there may be other relevant contextual factors that should be considered. The statute should allow for this flexibility by allowing the OPC and courts to consider any other relevant factor. This type of flexible approach is taken by many courts in Canada and by a number of provinces with substantially similar privacy laws so adopting it in the CPPA would also facilitate the OPC's collaboration with other regulators.

The CPPA, like PIPEDA, also sets boundaries for how an organization can collect, use or disclose personal information. However, under PIPEDA, organizations' purposes for handling personal information need to be "explicitly specified." This important requirement, that purposes be both explicit and specific, is missing from section 13 of the CPPA. Without it, the door is open to organizations identifying overly broad and ambiguous purposes, such as "improving customer experience."

Proposed amendments

- Amend ss. 12(2) of the CPPA as follows:
    - The ~~following~~ factors ~~must~~ to be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate include:
      …
      (f) any other relevant factors

- Amend s. 13 of the CPPA to require that organizations only collect, use and disclose personal information for purposes that are *specific* and *explicit*.

Administrative monetary penalties

Recommendation #4: Expand the list of violations qualifying for financial penalties to include, at a minimum, appropriate purposes violations.

Administrative monetary penalties (AMPs) are tangible and effective tools to encourage compliance and to respond to violations of the law in appropriate circumstances. PIPEDA does not currently provide for the imposition of AMPs, which limits organizations' incentive to comply with federal privacy law. Bill C-27 would allow the OPC to recommend that AMPs be imposed by the Personal Information and Data

Protection Tribunal, when warranted, strengthening the set of tools available for encouraging compliance.

Subsection 94(1) of the CPPA significantly expands the list of violations qualifying for AMPs from those proposed in the former Bill C-11. This is a positive development. However, the list remains limited, meaning that violations of many provisions of the CPPA would still not qualify for AMPs, including the appropriate purposes provisions, which are a cornerstone of the legislation.

The appropriate purposes provisions require organizations to only collect, use and disclose personal information in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, regardless of whether there is consent. When making this determination, there are various factors that must be taken into account including, for example, the sensitivity of the information and whether the loss of privacy would be proportionate to the benefit gained.

These foundational provisions should not be excluded from those that would qualify for AMPs. Under the CPPA, as drafted, there could be serious violations in terms of the appropriateness and reasonableness of organizations' treatment of personal information that would not face the same potential consequences as other types of violations.

Proposed amendments

- Further expand the list of violations qualifying for an AMP under ss. 94(1) of the CPPA to include, at a minimum, ss. 12(1) and 12(2).

Disposal

Recommendation #5: Provide a right to disposal of personal information even when a retention policy is in place.

The CPPA requires organizations to dispose of an individual's personal information, on their written request, under certain conditions. It also identifies scenarios where an organization can refuse this kind of request.

Among these scenarios is a provision in paragraph 55(2)(f) that would allow an organization to refuse to dispose of an individual's personal information if it is scheduled to be disposed of in accordance with a retention policy and if the individual is informed about the remaining period for which the information will be retained. This means that an organization with a lengthy retention policy could simply deny an individual's disposal request by notifying them of the remaining retention period for that

data. This could be problematic as personal information held by the organization can run the risk of being subject to a data breach.

OPC investigations have revealed cases of organizations with overly lengthy retention periods or with too-casual approaches to disposing of personal information at the end of its life cycle. For example, one organization that experienced a data breach held millions of documents in inactive accounts with only ambiguous guiding principles for retention.[5]

This approach to refusing disposal would limit individuals' ability to have their personal information disposed of in a timely way, undermine their right to disposal and generally diminish their control over their personal information.

Proposed amendments

- Remove paragraph 55(2)(f) from the CPPA.

IV. Privacy in support of the public interest and Canada's innovation and competitiveness

Privacy is not a barrier to innovation; privacy and innovation are complementary as they build on and strengthen each other. Canadians should not have to choose between protecting their personal information and participating in the digital economy. Considering privacy impacts at the front end allows data to be leveraged in a privacy-protective manner and encourages responsible innovation. The OPC makes recommendations and proposes amendments in the following five areas to advance the broader theme:

- Privacy by design and privacy impact assessments;
- De-identification and anonymization;
- Automated decision-making;
- Business activities; and
- Exceptions to consent for research.

[5] See Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019.

Privacy by design and privacy impact assessments

Recommendation #6: Create a culture of privacy by requiring organizations to build privacy into the design of products and services and to conduct privacy impact assessments for high-risk initiatives.

Implementing privacy by design and conducting privacy impact assessments (PIAs) can help organizations demonstrate that they are accountable for personal information under their control, ensure that they are in compliance with the law and limit the risk of privacy breaches.

Privacy by design refers to proactively integrating privacy-protective measures into the very design of a product, service, or initiative from the initial phases of development. In a 2018 report, and more recently in its May 2022 report on the collection and use of mobility data, ETHI recommended that privacy by design be included as a central principle in federal privacy legislation.[6] The OPC agrees with ETHI's recommendations and believes that the accountability provisions of the CPPA should explicitly include a requirement that organizations apply privacy by design.

A PIA is a risk management process which should be undertaken at the beginning of a new or modified initiative involving personal information. It can help organizations proactively comply with privacy law, identify the impacts on personal information, and mitigate privacy risks. The CPPA's accountability provisions should explicitly include a requirement that, where an organization is engaged in higher risk activities, such as those involving sensitive information or high-impact AI systems, PIAs be prepared.

In the OPC's view, requiring PIAs for all activities could pose an excessive burden, especially on small- and medium-sized enterprises. However, a PIA requirement for higher risk activities ensures that privacy risks are being assessed and addressed in appropriate cases. These could include things like AI systems making impactful decisions about individuals, including whether they get a job offer, qualify for a loan, pay a higher insurance premium, or are suspected of suspicious or unlawful behaviour. In addition, clarity on what a PIA report must entail should be either prescribed through regulation or specified in OPC guidance.

While AIDA requires those responsible for AI systems to assess and mitigate the risks of harm of high impact AI systems, the definition of harm is limited and would exclude privacy from being considered in the risk assessment process. Adding a PIA requirement in the CPPA for high-risk activities would address this problem.

[6] Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018; Recommendation 19, Collection and Use of Mobility Data by the Government of Canada and Related Issues, Report of the Standing Committee on Access to Information, Privacy and Ethics, May 2022.

Proposed amendments

- Add provisions in the CPPA to require organizations to practice privacy by design and to conduct PIAs for high-risk activities.

De-identification and anonymization

Recommendation #7: Strengthen the framework for de-identified and anonymized information.

The OPC supports the introduction of a new framework for de-identification and anonymization in Bill C-27. The framework has some positive elements, for example, it provides flexibility to organizations using de-identified information, and adds some needed clarity as to how and in what circumstances de-identified personal information can be used and disclosed. That said, as currently drafted, it provides too little protection for de-identified and anonymized data.

Bill C-27 does not explicitly require organizations to apply de-identification measures that are proportionate to the risk of the information being re-identified. Given the broad definition for what is considered to be de-identified information under subsection 2(1), organizations could, in some circumstances, use and disclose a potentially wide range of personal information, that might be relatively easy to re-identify, without an individual's knowledge or consent. Further, under subsection 2(3) individuals may also lose the ability to exercise certain rights with respect to de-identified information, including the right to have inaccuracies corrected and to have information disposed of upon request. In light of these restrictions on individuals' control over their personal information, it is important that organizations reduce the potential impacts, including the risk of the information being re-identified. Organizations should be explicitly required to account for the risk of re-identification when applying de-identification measures.

As well, subsection 2(3) appears to state that de-identified information must be treated as personal information, except in certain circumstances. While we understand and agree that certain privacy requirements may not need to apply to de-identified information, this information remains and should always be considered personal information. To avoid ambiguity, we recommend that this subsection be amended to clarify that all de-identified personal information remains personal information.

There appears to be a discrepancy between the French and English versions of the definition of "de-identify" under section 2 of the CPPA. The English version clearly states that de-identified information means that one cannot directly identify an individual from such information, but there is nevertheless a risk that re-identification could occur. In

the French version, the wording appears to focus on lessening the risk of re-identification rather than clearly stating that the individual should not be directly identifiable despite the fact that such a risk cannot be completely eliminated. To avoid potential interpretive discrepancies, the French version of this definition should be modified to reflect the more rigorous meaning in the English version.

A final point relates to the new definition proposed for anonymized information. As currently drafted, organizations could anonymize personal information using "generally accepted best practices". However, there is no explanation of what these practices are or what would be considered "generally accepted." Including this language opens the door to the possibility that some organizations might rely on anonymization techniques promoted by certain experts or groups that are insufficient for a given dataset.

Given that anonymized information would fall outside the scope of the CPPA – and may therefore not be subject to any privacy protections at all – it is important to ensure that the threshold for anonymizing personal information is high and leaves no space for insufficient practices. While this may be a challenge for businesses that wish to anonymize personal information, the CPPA includes a number of mechanisms for the OPC to assist organizations in meeting their obligations, including providing guidance on privacy management programs, developing guidance materials, and reviewing and approving codes of practice.

Proposed amendments

- Amend the CPPA as follows:
  - S. 74: An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified, ~~and~~ the sensitivity of the personal information, and the risk of re-identification.
  - Ss. 2(3): For the purposes of this Act~~, other than sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116,~~ personal information that has been de-identified is considered to be personal information.
    - Should Parliament wish to exempt de-identified personal information from specific sections or subsections of the Act (as above), it should do so by prefacing the clause with: The following sections do not apply in respect to personal information that has been de-identified […]
  - Ss. 2(1): ***anonymize*** means to irreversibly and permanently modify personal information~~, in accordance with generally accepted best practices,~~ to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.

- Amend the definition of "de-identify" in the French version of the CPPA as follows, to better reflect the definition contained in the English version:
    - Paragraphe 2(1) : ***dépersonnaliser*** : Modifier des renseignements personnels ~~afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement~~ de sorte qu'un individu ne puisse être identifié directement sans pour autant en éliminer le risque.

Automated decision-making

Recommendation #8: Require organizations to explain, on request, all predictions, recommendations, decisions and profiling made using automated decision systems. The CPPA imposes two new obligations on organizations using automated decision-making (ADM) systems. While the OPC is generally supportive of these new obligations, as drafted, their scope is too limited in areas where there should be increased transparency.

Firstly, the CPPA requires organizations to provide a general account of the use of any ADM system that makes predictions, recommendations or decisions that could have a "significant impact" on individuals. It also requires organizations to explain predictions, recommendations or decisions that could have a "significant impact" to individuals upon request.

Limiting the general account requirement to activities with a "significant impact" would likely strike a reasonable balance between providing transparency for individuals and compliance effort for organizations. However, its addition to the explanation requirement is a problematic change from the former Bill C-11, as it narrows the scope of the requirement and would likely exclude decisions for matters such as online advertising, personalized news feeds and digital environments. As a result, narrowing this requirement to only those with significant impacts would not be in the interest of achieving algorithmic transparency.

There is also a key element missing from the CPPA in relation to ADM. Unlike the EU's General Data Protection Regulation (GDPR), and other modern privacy laws in California and Québec, the obligations do not explicitly apply to profiling. As drafted, the obligations would only apply to ADM systems that make decisions, recommendations, or predictions.

While profiling may be implicitly included in recommendations or predictions, not including it explicitly in the CPPA could create unnecessary ambiguity resulting in a significant gap. It could mean that often-opaque activities such as data brokering – selling or otherwise making available datasets about individuals which they will typically be unaware of – may not have the same needed transparency. It is also unclear if the

obligations would apply to personalized digital environments, which is an important consideration given developments in the metaverse and other immersive technologies.

Proposed amendments

- Remove the qualifier of "significant impacts" for the explanation requirement under ss. 63(3) of the CPPA for automated decision-making systems.
- Ensure that profiling is explicitly included in the provisions related to automated decision-making systems (paragraph 62(2)(c) and ss. 63(3)), in addition to predictions, recommendations and decisions, and that the term is defined similarly to Article 4(4) of the GDPR.

Business activities

Recommendation #9: Limit the government's ability to make exceptions to the law by way of regulations.

The CPPA permits the collection and use of personal information without the knowledge or consent of the individual for defined business activities, where a reasonable person would expect the collection or use for the activity, provided that it is not for influencing an individual's behaviour or decisions. There is also a provision allowing the Governor in Council to add any other activity to the list of business activities through regulation.

The business activities currently listed in subsection 18(2) of the CPPA must all be "necessary" to achieve a given purpose, which will help ensure that the consent exception is sufficiently narrow. The CPPA is, however, missing a requirement that all other prescribed business activities also be necessary to achieve a specific purpose. This could lead to activities being added by regulation that are overly broad, for example to "improve our services", and that would not have to meet a necessity threshold.

Subsection 122(1) of the CPPA, as drafted, would also grant the Governor in Council authority to make regulations specifying activities that would be completely excluded from the application of the Act.

This is of serious concern, as even when a collection or use is exempt from certain consent requirements, an organization should remain subject to the other requirements of the Act, ensuring that personal information remains protected and that the OPC has oversight.

Proposed amendments

- Amend the CPPA to require that all prescribed business activities for the purposes of ss. 18(2) are activities that are **necessary** to achieve a specific purpose.

- Amend ss. 122(1) of the CPPA as follows: The Governor in Council may make regulations for carrying out the purposes and provisions of this Act, including regulations

  (a) Respecting the scope of any of the activities set out in paragraphs 18(2)(a) to (c), including specifying activities that are excluded from the ~~application of this Act~~ activities set out in those paragraphs.

Exceptions to consent for research

Recommendation #10: Provide that the exception for disclosure of personal information without consent for research purposes only applies to scholarly research.

Encouraging responsible innovation involves giving organizations some flexibility to use and disclose personal information, both internally and externally, without consent. The CPPA includes such provisions, but the parameters to protect privacy are not always stringent enough to strike the right balance.

When it comes to internal research, analysis and development, the CPPA allows organizations, under section 21, to use personal information for these purposes without knowledge or consent provided that the information is de-identified before it is used.

In addition, section 35 of the CPPA facilitates the disclosure of personal information outside an organization without knowledge or consent, in certain circumstances, when the disclosure is for statistics, study or research purposes.

The former Bill C-11 had previously used the term “scholarly study” for this exception to consent, which was consistent with PIPEDA. The word “scholarly” has since been removed from Bill C-27.

The OPC believes that the removal of the “scholarly” qualifier turns what should have been a narrow exception to consent into an expansive one, with few safeguards. Without more specificity for the type of study or research that would fall under this exception, or the organizations that can receive personal data under this provision, “study” could be interpreted to include a broad range of commercial study or research, rather than work done by organizations working in the public interest and governed by ethics standards and safeguard requirements, such as universities.

As drafted, the provision could also permit the sharing of personal information with government institutions, bypassing section 39 of the CPPA, which limits disclosures to government to prescribed "socially beneficial purposes", rather than for broader "research" or "study" purposes.

Other domestic laws also include provisions permitting disclosure for research. For example, Québec's *Act respecting the protection of personal information in the private sector* permits disclosure for research without consent, but also provides additional safeguards to ensure that privacy remains protected, by requiring that a PIA be completed before the disclosure.[7] The PIA must reach a number of conclusions, including that the public interest in the study or research outweighs the impact that the disclosure may have on the individual, and that the personal information will be used in a manner that ensures confidentiality. The CPPA lacks such safeguards.

Re-inserting the term "scholarly" in section 35 would ensure that the exception to consent for research remains appropriately narrow.

Proposed amendments

- Amend s. 35 of the CPPA as follows:
    - An organization may disclose an individual's personal information without their knowledge or consent if
      (a) the disclosure is made for statistical purposes or for scholarly study or research purposes and those purposes cannot be achieved without disclosing the information

V. Privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens

Greater trust and participation in the digital economy can be fostered by protecting privacy and ensuring that individuals can exercise their rights. Strong private sector privacy laws include effective enforcement mechanisms that help instill confidence in the data-driven economy. The OPC makes recommendations and proposes amendments in the following five areas to advance this broader theme:

- Authorized representatives;
- Compliance agreements;

[7] *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 at ss.18(8) & 21.

- Review of the Commissioner's decisions;
- Timelines; and
- Domestic collaboration.

Authorized representatives

Recommendation #11: Allow individuals to use authorized representatives to help advance their privacy rights.

Like the former Bill C-11, Bill C-27 allows the rights and recourses provided under the CPPA to be exercised by others, explicitly stating in section 4 who can act as an authorized representative and under what circumstances. However, subsection 4(c) of the former Bill C-11, which would have allowed individuals to authorize any other person in writing to be their representative, has been removed. We have heard from private sector stakeholders that this provision raised concerns for potential abuse or fraud. However, as a result of the removal, it is now unclear if individuals will still be able to get help from a third party of their choosing.

For instance, it may now be uncertain if individuals still have the ability to file complaints with the OPC through their chosen representative. Currently, PIPEDA only addresses this issue in a limited fashion. For instance, the law does not currently specify whether someone can submit a complaint on behalf of someone else. In practice, the OPC has accepted complaints from an individual's personal representative, with their written consent.

There may be any number of reasons why an individual may want or need to choose an authorized representative to advance their privacy rights, for example, because of disability, a language barrier or available time. Re-inserting the provision originally included in the former Bill C-11 would add clarity and ultimately ensure that there are no new barriers introduced in Bill C-27 that would reduce an individual's ability to exercise their privacy rights under the CPPA.

Some stakeholders may be concerned that reinserting this provision as written may increase the risk of fraud or other improper behaviour by individuals claiming to be an authorized representative. Therefore, if deemed appropriate, that provision could be modified to specifically address such risks.

Proposed amendment

- Amend s. 4 of the CPPA to state: The rights and recourses provided under this Act may be exercised… (d) on behalf of any other individual by any person authorized in writing to do so by the individual.

Compliance agreements

Recommendation #12: Provide greater flexibility in the use of voluntary compliance agreements to help resolve matters without the need for more adversarial processes.

Like PIPEDA, the CPPA allows the Commissioner to enter into a compliance agreement with an organization in certain circumstances, with the aim of ensuring compliance with the Act. The use of compliance agreements under section 87 of the CPPA is more restrictive than what is currently available under PIPEDA, limiting the use of what the OPC has found to be a very effective enforcement tool. The framework for using compliance agreements in the CPPA should avoid unnecessary delays and provide more certainty for organizations.

Unlike PIPEDA, the CPPA provides that compliance agreements can only be used "in the course of an investigation". This means that the window to use compliance agreements would be much shorter and less flexible in the CPPA than what is currently allowed under PIPEDA. For instance, compliance agreements could no longer be used during an inquiry or in response to an incident outside of investigation. Once an inquiry begins, the OPC would have to pursue the matter until an order is made and/or an administrative monetary penalty (AMP) is recommended, even if the parties involved would prefer to settle. This could lead to unnecessarily drawn-out and expensive proceedings with uncertain outcomes. Organizations would not be able to enter into compliance agreements with the OPC as an alternative to undergoing a resource-intensive inquiry. Maintaining PIPEDA's flexibility to enter into a compliance agreement at any time would help ensure the timely and effective resolution of matters in the interest of all the parties.

The CPPA also delays the enforcement of compliance agreements. Under PIPEDA, if the OPC believes that an organization is not complying with a compliance agreement, it can immediately apply to the court for an order requiring the organization to respect its commitments. Under the CPPA, the OPC would only be able to do this once it has conducted an inquiry into the non-adherence to an agreement, issued an order, and the organization has failed to comply with that order. Allowing the OPC to register compliance agreements with the court, so that they have the same effect as a court order, would avoid this unnecessary delay. This approach would be similar to what is available for consent agreements of the Commissioner of Competition or consent orders of the US Federal Trade Commission.

The CPPA should also clarify that compliance agreements can include the payment of AMPs as well as any other agreed-upon measures. While sections 86 and 87 of the CPPA may be interpreted to allow the inclusion of these terms, explicitly including them in the CPPA would provide parties with predictability and greater certainty. This would also be similar to the approach for consent agreements under the *Competition Act*.

Proposed amendments

- Amend s. 87 of the CPPA to:
  - Permit the use of compliance agreements where the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention;
  - Enable the registration of Compliance Agreements with the court, making them equivalent to an order of the court; and
  - Clarify that the payment of AMPs and all other negotiated measures are possible terms within Compliance Agreements.

Review of the Commissioner's decisions

Recommendation #13: Make the complaints process more expeditious and economical by streamlining the review of the Commissioner's decisions.

The review process established in the CPPA has the potential to be a long and expensive process for all parties involved. As drafted, a matter will go to the Personal Information and Data Protection Tribunal if the Privacy Commissioner recommends an administrative monetary penalty (AMP). Complainants and respondents can also appeal the Privacy Commissioner's findings, orders, decisions and interim orders to the Tribunal.

Pursuant to section 21 of the PIDPTA a decision of the Tribunal will be final and binding unless an individual or organization is not satisfied with the Tribunal's decision, and seeks judicial review of that decision with the Federal Court. If a litigant remains unsatisfied, they could then take the matter to the Federal Court of Appeal and eventually, with leave, to the Supreme Court of Canada. The creation of the Tribunal therefore adds one more level of review in the process, resulting in additional delays and costs.

In order to support more timely and cost-effective outcomes, Tribunal decisions should be reviewed directly by the Federal Court of Appeal rather than by the Federal Court. By removing the Federal Court step, Tribunal decisions would still be subject to court review, however the process would be expedited, bringing finality to matters more quickly. In the alternative, the Privacy Commissioner could be given the authority to issue AMPs and reviews of the Privacy Commissioner's decisions could be done by the Federal Court instead of the Tribunal.

These changes may also address concerns about differing levels of review in certain provinces and federally. Provincial counterparts with substantially similar private sector privacy legislation do not have this type of administrative tribunal acting as a review body. Instead, such matters go directly to a provincial court or superior court depending on the jurisdiction, and some have fewer levels of review overall of their decisions.

Proposed amendments

- Make *Personal Information and Data Protection Tribunal* decisions judicially reviewable directly by the Federal Court of Appeal instead of the Federal Court. In the alternative, the Privacy Commissioner could be given the authority to issue AMPs and reviews of the Privacy Commissioner's decisions could be done by the Federal Court instead of the Tribunal.

Timelines

Recommendation #14: Amend timelines to ensure that the privacy protection regime is accessible and effective.

This submission groups three issues regarding timelines in the CPPA:

Breach Reporting:
The first issue relates to timelines for reporting breaches to the OPC. Like PIPEDA, the CPPA requires organizations to report to the OPC breaches of security safeguards involving personal information that create a real risk of significant harm. Maintaining the language of PIPEDA, the CPPA requires reports to be made "as soon as feasible after the organization determines that the breach has occurred."

The OPC's experience under PIPEDA has shown that this type of language leaves too much room for interpretation. Currently, 40% of breach reports under PIPEDA are received more than three months after the breach occurred. This delay impacts the OPC's ability to fulfill its oversight role and to offer organizations timely advice on mitigating measures. It also prevents individuals from protecting themselves when a breach occurs, leaving them exposed for an unnecessarily extended period of time.

Another matter relates to who should report breaches to the OPC. As drafted, the CPPA requires breaches to be reported to the OPC by organizations with personal information under their control. However, service providers experiencing a breach are only required to report breaches to organizations that they are providing services to. It is that organization which in turn is responsible for reporting the incident to the OPC. Since service providers tend to have key information about how a breach occurred and was mitigated, both parties should be required to report the breach to the OPC.

Return of Records:
The second timelines-related issue is the requirement for the OPC to return any record or thing that an organization produces as part of an investigation, inquiry or audit within a strict timeframe -- 10 days upon request. This timeline could be problematic, as the OPC makes use of digital forensic techniques to extract evidence which can take well over 10 days to complete. If such techniques and processes are interrupted, they must be restarted anew to maintain the integrity of the evidence involved. A 10-day time limit could prevent the use of these techniques entirely. The OPC should have the flexibility to return records and other things after it completes the investigation, inquiry or audit and any related proceedings have concluded.

Prosecution of Summary Offences:
The third timelines-related issue relates to section 128, a hybrid offence punishable either as a summary conviction offence or as an indictable offence. For indictable offences, there is no limitation period, however, in the case of summary conviction offences, the *Criminal Code* imposes a 12-month limitation period unless the prosecutor and defendant agree to an extension, or a law provides otherwise. Because prosecutions would most likely take place either well into or after regulatory investigations by the OPC, which can be complex and take longer than 12 months, a limitation period with no possibility of extension is problematic. Providing for the possibility of an extension of limitation periods would address this. This approach would be consistent with other jurisdictions, such as Québec and Ontario, and would help ensure that the Crown can proceed with prosecutions by summary conviction.

Proposed amendments

- Amend the CPPA to require that:
    - Breach reports be provided to the Privacy Commissioner without unreasonable delay, but no more than 7 calendar days after the organization becomes aware of the breach (ss. 58(2)), and that affected individuals, unless otherwise prohibited by law, be notified of a privacy breach without unreasonable delay after the organization determines that the breach has occurred (ss. 58(3)).
    - Service providers, if they determine that any breach of their security safeguards has occurred that involves personal information, report the breach within 7 days to the organization that controls the personal information, and report the breach to the Privacy Commissioner along with a list of data controllers notified of the breach (s. 61).

- Revise ss. 99(2) of the CPPA so that the Privacy Commissioner will have to return records or things after the investigation, inquiry, or audit is complete and after all related proceedings have been concluded.

- Provide for an extension of the limitation periods for summary convictions.

Domestic collaboration

Recommendation #15: Expand the Commissioner's ability to collaborate with domestic organizations in order to ensure greater coordination and efficiencies in dealing with matters raising privacy issues.

Internationally, the CPPA would offer the OPC flexibility to work with a variety of partners, which helps achieve impactful outcomes for Canadians. In contrast, the CPPA would limit the domestic authorities with whom the OPC can collaborate to only provincial and territorial information and privacy commissioners (IPCs), the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau. Collaboration with domestic regulators, in both privacy and other regulatory spheres like competition, consumer protection, and telecommunications, has become increasingly important to ensure impactful outcomes for individuals. OPC experience suggests that such partners could include additional regulators such as credit reporting regulators, the Office of the Superintendent of Financial Institutions, and human rights commissions. Looking forward, the OPC can also envisage the need to work with the proposed AI and Data Commissioner regarding conduct that potentially involves the misuse of personal information within an AI system.

The contrast between the OPC's ability to collaborate with international and domestic partners is also apparent in terms of what activities can be the subject of such collaborations. For instance, domestically, the CPPA does not specify, as it does with respect to collaboration with IPCs and international authorities, that the OPC can work with the CRTC and the Competition Bureau to address compliance-related matters and conduct joint investigations. As a result, joint investigations with the CRTC or the Competition Bureau could be subject to challenge, limiting the effectiveness of cooperation. The OPC seeks to avoid situations like that faced while investigating the adult dating website, Ashley Madison, where the Office was able to share information with the Federal Trade Commission (FTC) in the US, but not with Canada's own Competition Bureau.

Flexibility for the OPC to work with other regulators would be valuable where the conduct in question falls within the scope of multiple jurisdictions and would also be consistent with the OPC's current ability to cooperate with international partners. Among its many benefits, increased collaboration would help reduce costs and duplicative efforts for regulators and organizations alike. This collaboration would also help avoid conflicting or inconsistent outcomes, which can make compliance difficult for organizations, and means further risks for consumers.

Proposed amendments

- Amend ss. 118(1) of the CPPA as follows:
    - The Commissioner may enter into agreements or arrangements with the Canadian Radio-television and Telecommunications Commission, ~~or~~ the Commissioner of Competition, or the AI and Data Commissioner in order to

        (a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any investigations, inquiries, or other formal compliance matters in which they are mutually interested;

        (~~a~~b) undertake and publish research on issues of mutual interest; and

        (~~b~~c) develop procedures for disclosing information referred to in subsection (2).

- Amend ss. 119(1) of the CPPA to achieve parity with ss. 120(1) by permitting the Privacy Commissioner to collaborate and share information with any person or body who has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.

VI. Appendix: Previous OPC recommendations on the former Bill C-11

Should Parliament wish to consider additional ways to further enhance Bill C-27, the following are recommendations made by the OPC in response to the former Bill C-11 which remain relevant under Bill C-27. These recommendations were outlined in a submission shared with the House of Commons' Standing Committee on Access to Information, Privacy and Ethics in May 2021.[8]

1. Definition of Personal Information to Include Inferences (#7)

That the definition of personal information be amended to expressly include inferred information.

2. Definition of Sensitive Information (#8)

That a definition of sensitive information be included in the CPPA, that would establish a general principle for sensitivity followed by an open-ended list of examples

3. Political Parties (#10)

Subject federal political parties to the CPPA, for example by registering them in the schedule pursuant to subsection 6(3) and paragraph 119(2)(c) (122(2)(c)).

4. Socially Beneficial Purposes (#15)

That s. 39 of the CPPA be amended to require that:

- A written request be made prior to information being disclosed to ensure that the use is of societal benefit as defined in the CPPA;
- An information sharing agreement be entered into, which would prohibit the recipient from re-identifying the information as well as from using the information for secondary purposes which are not of a societal benefit; and
- The definition of "socially beneficial purposes" be amended to include a limit on regulatory power, for example by indicating that they must be "purposes that are beneficial to society and not simply of individual or commercial interest or profit."

5. Publicly Available Information (#16)

That s. 51 of the CPPA be amended to provide, in addition to the conditions already present, that the personal information is such that the individual would have no reasonable expectation of privacy.

[8] Section numbers identified in brackets correspond to the numbering in C-27.

6. Disclosure to Law Enforcement (#18, #19)

(Recommendation 18) That record-keeping and reporting requirements be established with respect to disclosures of personal information to government organizations, especially with respect to disclosures to law enforcement.

(Recommendation 19) That a definition clarifying the meaning of "lawful authority" for the purposes of section 44 be introduced.

7. Accountability – Objective Standard (#20), Record-keeping, Scalability (#21)

(Recommendation 20) That s. 9 of the CPPA be amended to prescribe an objective standard for accountability, as follows:

9(1) Every accountable organization must implement a privacy management program to ensure compliance with its obligations under the Act.

(2) A privacy management program includes the organization's policies, practices and procedures that serve to ensure compliance with the Act, and includes policies, practices and procedures respecting …

(Recommendation 21) That accountability be strengthened in the CPPA, by:

- Introducing a provision requiring organizations to maintain adequate records to demonstrate compliance with their privacy obligations under the Act, including an explicit traceability requirement in the context of automated decision-making;
- Amending ss. 9(2) so that the scaling of accountability and record-keeping obligations be dependent on the nature and importance of the personal information under an organization's control, the size and revenue of the organization, as well as relevant risks and threats.

8. Trans-border data flows and service providers (#23)

That organizational requirements with respect to trans-border data flows be set out explicitly and separately, in a manner consistent with the recommendations set out in Annex B of our May 2021 C-11 Submission.[9]

[9] Recommendations 6, 7, and 11 in Annex B of OPC's submission on the former Bill C-11, which make reference to "substantially the same protection of personal information", should be updated to mirror the new "equivalent level of protection" provided for under ss. 11(1) of Bill C-27. Recommendation 5, which suggests that offshore service providers should not be able to avail themselves of the business activities exemption that was contained in former Bill C-11's paragraph 18(2)(e) is no longer relevant as this provision is not in Bill C-27.

9. Safeguards (#24)

That subsection 57(2) of the CPPA be replaced by:

In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the risks to consumers, in the event of a breach, associated with the nature, scope, and context of its use of personal information, in light of the organization's business activities.

10. Domestic Service Providers (#26)

That recommendations 3, 4, 5, and 7 of Annex B of our May 2021 C-11 Submission also be applied in the context of domestic service providers.

11. Automated Decision-Making – Level of explanation (#28)

That a right to contest automated decisions be included in the CPPA.

12. Right to Reputation – De-indexing (#30)

That Parliament enact a clear and explicit right with respect to the de-indexing and/or removal of personal information from search results and other online sources, considering the OPC's recommendations in its 2018 Draft Position on Reputation and the approach taken under Quebec's Law 25 (formerly Bill 64).

13. Data Mobility (#31, #32)

(Recommendation 31) That section 72 of the CPPA be expanded to include all personal information about an individual, including derived or inferred information.

(Recommendation 32) That a clear consultative, advisory or approval role be established for the OPC with respect to data mobility frameworks.

14. Rules of Procedure and Evidence in Investigations and Inquiries and Relevant to Orders (#33)

That the following amendments be made with respect to the inquiries and investigations under the CPPA:

- 98(1)(a) (99(1)(a)): Reduce the threshold by which the OPC can compel the production of evidence, and rephrase this power as "order" rather than "compel";
- 98(1)(h) (99(1)(h)): Clarify that this provision also applies to information stored on remote servers, but accessible within the premises in question;
- 103(2) (104(2)): Make orders under 98(1)(a) and 98(1) (99(1)(a) and 99(1))

enforceable in the same manner as an order of the court;

- 103(2) and 104 (104(2) and 105): Appeal provisions relating to interim orders made pursuant to paragraph 98(1)(d) (99(1)(d)) should be amended to ensure that such orders are not unduly delayed or undermined pending appeal;
- 90(2) (91(2)): Enact necessary amendment to allow the OPC to request and receive information subject to solicitor-client privilege, for the purpose of assessing claims of statutory exemptions in the context of access-related complaints;
- 92(2) (93(2)): Strike the necessity test, which is not found in any comparable statute;
- 92(4) (93(4)): Remove the one-year maximum period for extensions to completion of an inquiry.

15. Breaches – Reparation for Damages Suffered (#34)

That a paragraph be added under subsection 92(2) (93(2)) which permits the OPC to order an organization to "take measures which allow individuals to be compensated for damages suffered, financial or otherwise, stemming from a breach or violation of security safeguards required by law."

16. Administering Administrative Monetary Penalties (AMPs) (#39 & #40)

(Recommendation 39) That subsection 93(2) (94(2)) be amended by:

- Rephrasing paragraph 93(2)(c) (94(2)(d)) to focus on history of non-compliance; and
- Incorporating paragraphs 94(5)(b) and (c) (95(5)(b) and (c)).

(Recommendation 40) That subsection 93(3) (94(3)) be removed from the CPPA.

17. Private Right of Action (#41)

That section 106 (107) of the CPPA be amended to expand the private right of action, by replacing paragraphs 106(1)(a) and 106(1)(b) (107(1)(a) and 107(1)(b)) with requirements similar to section 77 of the Official Languages Act.

18. Codes and Certifications (#44 & #45)

(Recommendation 44) That the Commissioner's obligation to review an application for approval of a code of practice or certification program be conditional on the payment of a cost recovery fee.

(Recommendation 45) That all references to regulations in sections 76, 77, 78, 81 and 122 (a)-(j) (125 (a)-(j)) of the CPPA be removed, leaving to the Commissioner the authority, as is the norm in other jurisdictions, to adopt fair procedures to

approve codes of practice and certification programs pursuant to the standards found at subsections 76(2) and 77(1) of the Act.

19. Section 108 (#46)

That section 108 of the CPPA (109) be amended to encourage the Commissioner, in the exercise of his powers and duties, to consider the size of the organization and other factors mentioned. Alternatively, include these factors in a purpose clause.

20. Proactive Investigations/Commissioner-initiated Complaints (#47)

That subsection 82(2) of the CPPA be amended as follows:
~~If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act,~~ ~~t~~The Commissioner may initiate a complaint to ensure compliance with this Act ~~in respect of the matter~~.

21. Proactive Compliance Audits (#48)

That the condition "if the Commissioner has reasonable grounds to believe that the organization has contravened Part 1" be removed from s. 96 (97).

OPC's 15 key recommendations on Bill C-27

Privacy as a fundamental right

1. Recognize privacy as a fundamental right.
2. Protect children's privacy and the best interests of the child.
3. Limit organizations' collection, use and disclosure of personal information to specific and explicit purposes that take into account the relevant context.
4. Expand the list of violations qualifying for financial penalties to include, at a minimum, appropriate purposes violations.
5. Provide a right to disposal of personal information even when a retention policy is in place.

Privacy in support of the public interest and Canada's innovation and competitiveness

6. Create a culture of privacy by requiring organizations to build privacy into the design of products and services and to conduct privacy impact assessments for high-risk initiatives.
7. Strengthen the framework for de-identified and anonymized information.
8. Require organizations to explain, on request, all predictions, recommendations, decisions and profiling made using automated decision systems.
9. Limit the government's ability to make exceptions to the law by way of regulations.
10. Provide that the exception for disclosure of personal information without consent for research purposes only applies to scholarly research.

Privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens

11. Allow individuals to use authorized representatives to help advance their privacy rights.
12. Provide greater flexibility in the use of voluntary compliance agreements to help resolve matters without the need for more adversarial processes.
13. Make the complaints process more expeditious and economical by streamlining the review of the Commissioner's decisions.
14. Amend timelines to ensure that the privacy protection regime is accessible and effective.
15. Expand the Commissioner's ability to collaborate with domestic organizations in order to ensure greater coordination and efficiencies in dealing with matters raising privacy issues.

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada