THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION

December 2019

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access Law Section, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law Section.

Copyright © 2019 Canadian Bar Association

TABLE OF CONTENTS

Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA

Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA

I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law Section (CBA Section) is pleased to comment on the *Strengthening Privacy for the Digital Age* consultation document (consultation document) released by Innovation, Science and Economic Development Canada (ISED) in May 2019. The Section represents specialists in privacy law and access to information issues from across Canada.

The CBA Section has a history of contributing to the creation and development of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as to other issues that impact Canada's privacy landscape (for example, Canada's Anti-Spam legislation).[1] In general, our members' experience is that PIPEDA has worked well and is achieving its intended purpose. If it is determined that there are new challenges that require amendments to the legislation, we suggest that they be approached cautiously. In this submission, we raise various proposals and suggest different considerations before significant changes are contemplated or pursued.

II. PART 1 – ENHANCING INDIVIDUAL'S CONTROL

A. Consent and Transparency

The consultation document states that the increased volume and complexity of data flows have strained the traditional knowledge-and-consent system and left individuals without meaningful control over their personal information and privacy. ISED states that new frameworks are required to address the unethical use of data and to build trust.

1 See, for example, Canadian Bar Association submissions on the Personal Information Protection and Electronic Documents Act (PIPEDA) (March 2017); available online: https://www.cba.org/CMSPages/GetFile.aspx?guid=1775ca6e-e80c-4bee-a1bb-a8b9c8857a5a, and also Statutory review of Canada's Anti-Spam Legislation (2017) https://www.cba.org/CMSPages/GetFile.aspx?guid=de3b33ca-511c-4f48-bf61-843a530eecbc.

The CBA Section has long taken the position that PIPEDA and its knowledge-and-consent regime works—it is technology neutral and stands the test of time, allowing organizations to evolve their privacy practices to reflect changing business models, technologies and customer expectations. It has proven to be flexible in adapting to rapidly evolving technologies (including the internet and "big data"), business practices and individual privacy expectations.

Consent has an important role to play in privacy protection and is achieved by the current PIPEDA framework, including in the context of accountability and other principles. Individuals should be empowered in decisions that impact their privacy rights, which is underscored by the consent regime outlined below. The right to revoke consent is also an important element of the consent regime. While there may be concerns about consumer privacy "literacy" lagging behind the evolution of business models, the CBA Section does not believe that this necessarily means that the consent-based regime does not work.

At present, organizations must make a reasonable effort to ensure that individuals are advised of the purposes for which information collected will be used and/or disclosed. PIPEDA currently requires that consent be reasonably understandable by the individual. The PIPEDA consent model, supported by the broader legal framework, continues to be robust in protecting the privacy of Canadians – including vulnerable groups – in the face of emerging technologies and business models that increasingly rely on the collection of personal information. Further, while PIPEDA is consent-based, it already offers practical exemptions to consent where impractical or unnecessary, including exemptions for publicly available information, with the understanding that all other privacy obligations and safeguards outlined in PIPEDA would continue to apply. While we do not see a compelling case for significant legislative change to the consent framework, we support continued efforts to improve understanding and compliance under PIPEDA for both small and medium businesses, as well as large businesses.

We do not agree with those who argue that doing away with the knowledge-and-consent regime in PIPEDA will improve privacy rights for individuals. Doing that would result in more reliance on the accountability principle, when accountability itself is a standard that many businesses are struggling to achieve. For example, the recent Equifax case shows that Equifax was not meeting its existing accountability obligations under PIPEDA. Other recent cases involving privacy issues arise from weaknesses in security measures or training.

Distinctions are already made between disclosures and transfers for processing, and between express and implied consent. In *Royal Bank of Canada v. Trang*[2], the Supreme Court of Canada (SCC) unanimously adopted an objective test for determining whether implied consent is appropriate. Importantly, implied consent does not rely on particular disclosures by the organization. Instead, consent is implied based on a "reasonable person" test. The SCC noted that PIPEDA Schedule 1, clause 4.3.6 acknowledges that consent can be implied when information is less sensitive (para. 34). However, it emphasized that even information that would ordinarily be considered sensitive – that is, financial information – must be assessed in the total context to determine the actual degree of sensitivity for the purposes of assessing whether implied consent is appropriate: "the degree of sensitivity of specific financial information is a contextual determination" (para. 36). In addition to considering the sensitivity of the information, the SCC noted that PIPEDA clause 4.3.5 directs the organization to consider the reasonable expectations of the individual when determining the form of consent (para. 35). When considering reasonable expectations, "the whole context is important" (para. 43). The SCC specifically stated that privacy interests must not be unduly prioritized over legitimate business concerns (para. 43), which is consistent with the purpose clause of PIPEDA.

The consultation document points to consent fatigue and overly complicated privacy policies. The Office of the Privacy Commissioner's (OPC) guidance on consent addresses this point by outlining that organizations should allow individuals to control the amount of detail provided and obtaining consent should be innovative and encourage the use of interactive and dynamic tools. In addition, there are many opportunities to invest in public education including through an increase in staff and budgetary resources allocated to the OPC.

Even if PIPEDA were overhauled, privacy would not suddenly become a simple exercise—a complex privacy framework in Canada has almost forty privacy statutes covering the public and private sectors, not to mention, where applicable, international law (in particular the European Union's *General Data Protection Regulation* (GDPR)) under which many Canadian businesses operate. Further harmonizing rather than differentiating the application of these varied laws will improve data privacy knowledge of individuals and organizations in private and public sectors. Any changes to PIPEDA in light of the GDPR should carefully consider the resulting impact on those same organizations, and if there are preferable ways to enable

2 *Royal Bank of Canada v. Trang*, 2016 SCC 50.

continuing data flows to and from the EU without unduly restricting, in pursuit of the goal of adequacy, organizations' legitimate commercial activities occurring wholly within Canada.

ISED should conduct further analysis and consider potential issues with GDPR adequacy and monitor those developments carefully. If legal changes are required to maintain adequacy status, we believe that ISED should wait and see what specific changes will be called for and amend PIPEDA simultaneously to avoid confusion on the part of individuals and organizations.

If ISED moves forward with amendments in any event, including amending the definition for publicly available information, the CBA Section suggests that consultations on reform be structured as widely as possible to also include groups that represent racialized people and other historically disadvantaged groups, particularly concerning the relationship between privacy issues and human rights and discrimination issues. The most significant impact would be felt through more public education about PIPEDA, rather than changing the framework of PIPEDA itself.

Having said that, there are key gaps in the legislation that, if addressed, would create real improvements for individuals and the overall privacy framework in Canada. Gaps that the CBA Section has identified as requiring change are:

1. Political parties should be subject to the same privacy laws as private and public organizations. The CBA Section made already made submissions on this legislative gap.[3] The recent requirement that political parties create and publish a privacy policy pursuant to the *Elections Modernization Act* is insufficient, as there is no third-party oversight nor mechanism for electors to lodge a complaint beyond the party.[4] PIPEDA is a logical and appropriate framework to address political parties.

   The lack of robust privacy laws for political parties has a real and substantial impact on individuals. Not only do political parties collect massive amounts of data from individuals, from public and private sources, they are known targets of data mining and hacks.[5] This is especially concerning as political parties have no legal obligation to

3 CBA submission on Bill C-76, *Elections Modernization Act*, https://www.cba.org/CMSPages/GetFile.aspx?guid=26701422-9559-4b6b-b089-401662c5a8d8.

4 *Elections Modernization Act*, section 254.

5 British Columbia's PIPA legislation covers political parties, as covered in Commissioner McEvoy's order 19-02. See also, House of Commons, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process* : Report of the Standing Committee on Access to Information, Privacy and Ethics (June 2018) (Chair: Bob Zimmer); House of Commons, International Grand Committee on Big Data, Privacy and Democracy: Report of the Standing Committee on Access to Information Privacy and Ethics (June 2019) (Chair: Bob Zimmer); Elizabeth Judge and Michael Pal, "Privacy and the Electorate: Big Data and the Personalization of Politics" (October 2017), online: < https://techlaw.uottawa.ca/news/privacy-and-electorate-big-data-and-personalization-politics>.

inform individuals that their personal information has been compromised.

2. There is a common perception that the "commercial activities" requirement places Canadian charities and not-for-profit entities outside the scope of PIPEDA. However, the nature of specific activities of an organization may attract PIPEDA requirements and no bright-line test is available to determine whether an activity is commercial in nature. For this reason, many lawyers in the charity and not-for-profit area advise their clients to assume that, regardless of their tax status, they may be engaged in commercial activity in the meaning of PIPEDA, may be subject to PIPEDA and so should comply with it. As a result, many charities and not-for-profits choose to obtain consent and abide by the other "fair information principles" in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (the CSA Model Code), Schedule 1 to PIPEDA, when collecting, using or disclosing personal information. The application of PIPEDA to not-for-profits and charities should be clarified.

RECOMMENDATIONS:

1. **The CBA Section recommends that PIPEDA's consent regime be bolstered through additional information provided to individuals.**
2. **The CBA Section recommends that any changes to consent account for adequacy with the GDPR and be made in that context.**
3. **The CBA Section recommends that gaps in the legislative framework be addressed: a) the inclusion of political parties, and b) clarification of the application to charities and not-for-profit industries.**

B. Data Mobility

As a general proposition, the CBA Section recognizes that a right to data mobility and data portability[6] could be valuable for Canadians and the digital economy. Those rights would help to rebalance the relationship between individuals and organizations by increasing consumer control and choice, which in turn would likely stimulate competition, growth and innovation. There are also risks associated with prolonged inaction. For example, in the context of open banking, maintaining the *status quo* poses real risks to privacy and cybersecurity. Consumers

6 As ISED has done, we use the term "data mobility" to refer to an individual's right to request that an organization move their personal information directly to a third party organization. "Data portability", on the other hand, refers to an individual's right to request their personal information directly from an organization and, upon receipt, transfer it to a third party organization themselves.

who are eager to port their data turn to third party offerings, many employing inherently risky practices that they do not take the time to appropriately understand, such as screen scraping.

However, we have seen from the GDPR experience[7] that there are practical challenges with delivering data mobility to end users. If data mobility is to become a right in Canada, more must be done than simply codifying the right under PIPEDA, as was done with the GDPR in the EU. To be meaningful, i.e., real for consumers and not too costly or burdensome for businesses, there must be comprehensive cross-sectoral consultations, clarity regarding implementation, and a deliberate attempt to meet stated objectives and consumer expectations.

Cross-Sectoral Approach

The multifaceted nature of a right to data mobility and the impact it would have across sectors, including competition and consumer protection, require that discussions not occur through a siloed privacy lens. Input must be sought across the industries likely to be affected, including from the Competition Bureau and other regulators. Corresponding reform to PIPEDA's sister statutes may also be warranted.[8] This is not solely a practical consideration. There may be constitutional implications as the right to data mobility extends into the economic realm.

Affected industries should have ample opportunity to comment on elements of the right and communicate any operational concerns. In particular, industry views should be solicited on the meanings of authorized entities, authorized activities, standardized format, and the types of data to which the right applies.

Further, industries cannot – and should not – be expected to build infrastructure hastily to meet a new data mobility right. Full mobility should be conditional on the implementation of sector-compatible frameworks and infrastructure (e.g., the use of Application Program Interface (APIs) or third party accreditation) that permit interoperability and secure data flow. Using banking as an example, challenges that are unique to the banking industry must be considered in designing a consumer-directed flow of data between financial institutions. This would include practices compliant with anti-money laundering and anti-terrorist financing requirements.

7 Recently, the EU introduced a sweeping data portability right under Article 20 of the GDPR, but with little clarity as to its implementation. As a result, the EU has seen a spike in cybersecurity incidents involving social engineering, among other unintended consequences.

8 E.g., Finance and open banking; Transportation and autonomous vehicle data-sharing; CRTC and telecommunications.

RECOMMENDATIONS

4. **The CBA Section recommends that ISED avoid a siloed privacy approach in considering data mobility, but instead work closely with other impacted sectors, including competition and consumer protection.**

5. **The CBA Section recommends that any right to data mobility be conditional on the implementation of sector-compatible frameworks and infrastructure that permit interoperability and secure data flow.**

Scope

Subject to broader, cross-sectoral consultation, the CBA Section can offer a privacy perspective on the potential scope of a right to data mobility in Canada. We stress the need to ensure certainty around elements of the right, which might be accomplished through regulation.

i. What Data?

The CBA Section recommends focusing only on user-provided personal information in a digitized format to improve individuals' control over their own data. Beyond this baseline, the right could extend to certain data elements created through interactions with products and services, such as transactional data or raw data collected by a wearable device.[9]

The CBA Section suggests that the law explicitly exclude certain types of data from the right to be ported, including data that:

- is proprietary in nature, including derived data or insights;
- would adversely affect the rights or freedoms of a third party or parties if it were ported;
- does not amount to "personal information" as defined under PIPEDA;[10]

9 Under the GDPR, data portability only applies to personal data provided by an individual to a controller. This does not include additional data created by an organization based on the data an individual has provided, such as a user profile. However, the ICO has interpreted "provided to a controller" as including personal data that is observed, such as website usage or search activities, location data or raw data processed by connected objects such as wearable devices or smart meters. See the ICO Guide to the General Data Protection Regulation (GDPR).

10 Australia's data portability equivalent, the Consumer Data Right (CDR), allows individuals to port data about themselves from one business to another, and also gives individuals a right to request that the originating organization share information about that business' products with an accredited third party. The CBA Section does not recommend this approach as it would create confusion with respect to the proprietary exemption and add little value as most of this information is publicly available.

- is neither linked nor conducive to the primary objective of data mobility, such as call notes or complaints; and
- if ported, would be contrary to law enforcement or prejudice an investigation.

Each exclusion should be applied in a case-specific manner. While there will be instances in which observed data amounts to proprietary information (e.g., where a business derives value by developing profiles based on observed data using unique algorithms), on other occasions it may not (e.g., raw data on the number of daily steps taken as collected by a wearable device).

Importantly, certain types of data that are excluded from a data mobility request, such as call notes or complaints, would remain subject to an access request in the ordinary course under PIPEDA. The right to access and the right to mobility serve different purposes and should be distinguished. Any expectation that organizations make data available in a standardized digital format and/or port it directly to another organization should not extend to data that would not serve the mobility right. That said, sector-specific frameworks or baseline standards could include broader data sets where that is valuable.

ii. What Format?

The right to data mobility should be focused on digital data in technology neutral formats; the right should not apply to physical records that have not been digitized for business purposes and cannot be digitized without significant effort.

The consultation document references a "standardized digital format, where such a format exists." Market-driven solutions often evolve over time from simple to far more complex. To manage the transition, "standardized digital format" could be prescribed by regulation. For instance, full mobility rights involving direct transfer of information between organizations might be conditional on the third-party organization being a member of a sector-based framework, such as an API. These frameworks could be selected through collaboration between industry and regulators (e.g., the current open banking consultations) and recognized by government through regulation.

iii. Transferred to Whom?

Data mobility rights are, first and foremost, about increasing individual control and giving consumers real choice, to encourage full participation in the digital economy. With that in

mind, there is value in allowing individuals to request that their information be ported directly between organizations, without having to act as an intermediary. However, the right infrastructure must be in place to securely facilitate those transfers and to offer certainty that the individual has been thoroughly authenticated and has given full and informed consent.

To ensure optimal data security, the data mobility right may be formulated as an obligation to provide the information directly to the requestor unless the third party to whom the individual seeks to port the data uses a designated method of transfer or is accredited by a recognized body. This is particularly important where requests are received from a third-party organization on an individual's behalf, in which case organizations must be able to trust that the third party is operating with the individual's full and informed consent. Consent should not be buried in contracts with third parties, nor should the data mobility right support automated requests issued by third parties. The evolution of a broker business created by bulk third party requests and mass portability must be avoided.

iv. In what Circumstances?

The GDPR affords a data portability right only to individuals when the legal ground for processing is consent or performance of a contract. The CBA Section believes that, in Canada, we must consider whether a right to data mobility should extend to situations where the basis for processing is other than consent. This is particularly important for revisiting the approach to consent under PIPEDA and extending the exceptional circumstances where consent is not required.

Additional Challenges

i. Security of Data

Ensuring security of data at the request and porting stage will be paramount for both consumers and organizations. Lessons can be learned from the experience with the GDPR's data portability right, which has not unfolded as expected. Due to issues with implementation and a regulation light on logistics, data portability under the GDPR has created a swath of cybersecurity issues involving social engineering.[11] Fearing heavy fines for failure to meet data portability response times, some organizations have opted for speed over diligence, neglecting appropriate steps to authenticate requestors before porting their data. Logistics around

11 https://www.theregister.co.uk/2019/08/09/gdpr_identity_thief/.

authentication warrant particular attention as an approach to implementing this right is developed in Canada. To avoid a spike in mobility-related cybersecurity incidents, fraud, anti-money laundering and anti-terrorist financing, authentication issues must be carefully considered in a manner that reduces exploitable vulnerabilities at the request stage.

RECOMMENDATIONS

6. **The CBA Section recommends that any proposals in the area of data security consider authentication issues.**

ii. Sensitivity of Data

Appropriate technical, administrative and physical controls must be in place to prevent unintended uses of data and to ensure that a data mobility right does not permit through the backdoor what PIPEDA and other applicable regulatory standards prohibit through the front door. For example, a data mobility right must not permit comingling of insurance and banking information in contravention of the longstanding regulatory barrier between these sectors. In addition, it may be advisable to limit data fields that can be ported to address increased risks associated with transferring particularly sensitive data. Alternatively, higher authentication standards could be used for requests to port highly sensitive data.

RECOMMENDATION

7. **The CBA Section recommends that data mobility be limited to the same principles as currently exist in PIPEDA.**

iii. Liability

As organizations will be required to share potentially sensitive data with third parties, a data mobility right should exclude liability for organizations responding to a data mobility request. If a recipient fails to adequately protect the information they receive, no action should lie against the originating organization for subsequent access, use or disclosure, assuming the originating organization complied with the established framework for completing the transfer. Originating organizations who comply with data mobility obligations should not be responsible for educating recipients on how to protect or store personal information.

RECOMMENDATION:

8. **The CBA Section recommends that subsequent liability for personal information be removed from organizations where data recipients have not adequately protected that data.**

iv. Accountability

Once information is transferred from the originating organization to the data recipient, accountability for that data should also transfer as data mobility is effectively a directed disclosure of data from one controller to another. However, if the originating organization holds on to the data for any continued business purpose of its own, that organization should continue to be accountable for the information.

RECOMMENDATION:

9. **The CBA Section recommends that organizations remain accountable for continuing to hold data for any ongoing business purposes.**

v. Retention

The impact of data mobility on the retention and destruction obligations of the originating organization should be considered. Data mobility does not necessarily mean that the data ported to a third party must concurrently be deleted by the originating organization. Rather, the assumption should be that original obligations under PIPEDA remain in effect according to normal business practice.

vi. Enforcement

The issue of data mobility is fundamentally about marketplace competition, consumer access to goods and services, and the creation of favourable conditions for economic growth. It may be best enforced by sector-specific regulators, and not solely by the OPC. We suggest limiting the role of the OPC to overseeing individual access rights and related privacy considerations that typically fall in the scope of PIPEDA (such as appropriate safeguards and accuracy of information). The OPC's role should not extend to determining the framework for porting data to third parties. As data mobility is as much about competition and consumer protection as it is

about privacy, the Competition Bureau may be better positioned to administer mobility from the competition and consumer welfare perspectives.[12]

Further, introducing data mobility is likely to attract new third-party providers to the field, many of whom may operate internationally, raising concerns about enforcement powers of Canadian regulators. It will be necessary to ensure that all parties who might receive ported information remain accountable to consumers in Canada for privacy and confidentiality.

RECOMMENDATION

10. The CBA Section recommends limiting the role of the OPC to overseeing individual access rights and related privacy considerations typically falling within scope of PIPEDA (such as appropriate safeguards and accuracy of information) and that other government agencies are better suited to determining industry specific frameworks for data porting.

C. Online Reputation

The CBA Section has previously made submissions to the House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) Committee in March 2017[13] and the OPC in May 2018[14] about online reputation, the right to de-indexing and the right to be forgotten.

The evolution of the internet and other digital technologies has created a sea change in terms of the volume, accessibility and durability of information readily available to Canadians. Online reputation and disclosure (and subsequent use or further disclosure) of personal information online are important issues for regulators, policy makers and legislators to carefully consider as to how control of this information should be exercised, if at all, and by whom.

Some experts believe that online reputation is a multifaceted issue that may not be entirely resolved as a "privacy" issue. In some cases, the issue is not the fact that personal information remains available online, but that some uses may be discriminatory. In other cases, the issue is not collection, use and disclosure of information by an organization for commercial activity, but

12 Australia's CDR is jointly regulated by the Australian Competition and Consumer Commission and the Office of the Australian Information Commissioner.

13 CBA submissions on the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (March 2017); available online: https://www.cba.org/CMSPages/GetFile.aspx?guid=1775ca6e-e80c-4bee-a1bb-a8b9c8857a5a.

14 CBA letter to Commissioner Therrien (May 1, 2018); available online: https://www.cba.org/CMSPages/GetFile.aspx?guid=6558cb2e-e375-48a0-9e2f-a57f186f8398.

dissemination of information by an individual for personal purposes that are harmful to the subject of that information. Therefore, care must be taken not to fashion a blunt instrument to deal with online reputation but to address different facets of the issue in the contexts in which they arise.

As an example, a defined retention period under PIPEDA may be unworkable. Clause 4.5.2 of Schedule 1 to PIPEDA currently provides that organizations should develop data retention periods. Clause 4.5.3 of Schedule 1 provides that information no longer required to fulfill the identified purposes should be destroyed, erased or made anonymous. A change to PIPEDA to require that personal information be deleted or destroyed based on a fixed retention period would be complex given the different statutorily mandated minimum retention periods under federal, provincial and territorial law. Even where there is no statutorily mandated minimum retention period, organizations may have legitimate reasons to retain information, including limitation periods for potential causes of action (which may be lengthy due to discoverability). ISED should also consider whether mandating a defined retention period is within the constitutional authority of Parliament given its impact on matters under provincial jurisdiction.

Although the CBA Section does not recommend defined retention periods, we believe that organizations could be encouraged to be more thoughtful and transparent about the criteria to define their retention periods for different categories of personal information and how their retention periods are rationally connected to the identified purposes for collection and use.

RECOMMENDATION

11. The CBA Section recommends that ISED consider amendments to PIPEDA to require organizations to disclose the criteria they use to define retention periods for broad categories of personal information.

The CBA Section recognizes that children and youth present a special case when considering online reputation.[15] The CBA Section supports ISED's exploration of additional means to afford Canadian children expansive privacy protection in accordance with their constitutional rights. The Supreme Court of Canada has stated that "recognition of the inherent vulnerability of

15 *Ibid.*, Canadian Bar Association letter to Commissioner Therrien (May 1, 2018).

children has consistent and deep roots in Canadian law."[16] It is also consistent with the *United Nations Convention on the Rights of the Child* (UNCRC), which Canada has ratified.

Although Parliament must not intrude on provincial or territorial jurisdiction to determine the appropriate age of majority, ISED should explore means to work cooperatively with provinces and territories to ensure that individuals under the age of majority in their region of residence, particularly children under 13 years of age, have nationally uniform tools to control information or misinformation that they or others have publicly posted or is shared about them other than through recourse to litigation in certain circumstances.

For example, federal, provincial and territorial governments could cooperate to develop uniform laws within the respective jurisdictions of Parliament and the Legislatures to give effect to the following rights in the UNCRC that are rationally connected to online reputation:

- Article 8: the right of a child to preserve his or her identity;
- Article 16: the right to be free from unlawful attacks upon his or her honour and reputation;
- Article 32: the right to be protected from economic exploitation; and
- Articles 34: protection from sexual exploitation and abuse.

In particular, there is a reasonable argument for widening the scope for removal when disseminated material concerns a child, without having to rise to the level of being criminal, defamatory or, in the sense of PIPEDA, inaccurate or incomplete. In balancing freedom of expression against the interests of the minor, the CBA Section believes that it is appropriate to consider the psychological effects on a child during crucial years of development and challenges children may face in accessing justice, particularly children whose families do not have resources to engage in protracted disputes with the perpetrators and online platforms. While improved protection of children may be accomplished in part through PIPEDA, the CBA Section believes that this issue requires broad provincial and territorial cooperation to be effective. In particular, the CBA Section encourages ISED to consider the following issues:

- Is a three-step process (negotiate with the source or platform, complain to OPC, and then seek a remedy under section14) appropriate as a primary means for a child to obtain a remedy for harmful content posted about that child?

16 *A.B. v. Bragg Communications Inc.*, [2012] 2 SCR 567, 2012 SCC 46 at para 17.

- Would a bright line rule on the right of a child to take down information about that child negatively impair the ability of youth to participate in online media? On the other hand, is there an age below which the benefits of participation are outweighed by risks of doing so, without bright line rules requiring the take-down of information?

- If a bright-line rule is appropriate, is it more in the nature of provincial or territorial consumer protection and human rights?

RECOMMENDATION

12. The CBA Section recommends that ISED work with provincial and territorial governments to develop a multi-jurisdictional approach to enhancing protections for children from unlawful attacks on their honour and reputation, which may include, but should not be limited to, strengthening the protections for children under PIPEDA.

III. PART 2 – ENABLING RESPONSIBLE INNOVATION

A. Enabling Data Trusts for Enhanced Data Sharing

The CBA Section generally supports the proposal to amend PIPEDA to support ethically responsible innovation through trusted data exchanges. However, the focus on and use of the term "data trust" is unhelpful. Trusted data exchanges should be neutral concerning the chosen business or legal structure supporting the data exchange. Instead, the focus should be on setting minimum criteria for transparency, standards for the de-identification of data, and independent audit or verification.

Much of the discussion on "data trusts" overlooks the complexity associated with adapting a common law trust or its Quebec civil law counterpart to the types of data sharing that could facilitate innovation.[17] That adaptation would require substantial cooperation from provincial and territorial governments given their jurisdiction for property and civil rights in section 92(13) of the *Constitution Act, 1867*.[18] Except for a "purpose trust",[19] trust property must be managed for the benefit of a legal or natural person that is identified or identifiable. The idea that beneficiaries would be identified or identifiable runs counter to the underlying purpose of

17 In the English common law context, some of these problems were discussed in a report commissioned by the Open Data Institute as part of a project funded by the UK Government's Office for Artificial Intelligence and Innovate UK: "Data trusts: legal and governance considerations" (April 2019) (https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf).

18 30 & 31 Vict, c 3, as amended.

19 M.E. Hoffstein, *Halsbury's Laws of* Canada - *Trusts* (2015 Reissue) ("Hoffstein"), HTR-77.

the data exchange to facilitate the use of de-identified data. Further, although it is possible to have a "purpose trust", the prevailing view is that it must be charitable in nature,[20] which would greatly diminish their overall utility in driving innovation.

Generally speaking, trustees have exclusive authority over trust property.[21] The trustees will commonly have the power to invest, sell, lease, and take other administrative action for management of the trust property, as set out in the trust deed or provincial/territorial legislation.[22] The vulnerability of the beneficiaries when legal title and administrative powers over property belong to the trustee requires that the law impose fiduciary duties on trustees. Even though it would be possible to design a unit trust to give beneficiaries the right to oversee the trustees by electing the trustees (as is commonly the case in trust declarations for income trusts), this may expose the beneficiaries to liabilities for the management of the trust. This became an issue of concern for trusts used for publicly traded businesses. For example, Ontario enacted the *Trust Beneficiaries' Liability Act, 2004*,[23] to protect beneficiaries of Ontario trusts governed by the *Securities Act*.[24]

Except for unit trusts where unitholders may replace the board of trustees, disputes about management of trusts often require court intervention. Further, any individual beneficiary may start litigation if they believe that the trustees are not abiding by the terms of the declaration of trust or have breached their fiduciary duties. Without a breach of fiduciary duty, courts afford trustees significant discretion.[25] Assuming the beneficiaries of the trust were the individuals whose information is the subject matter of the trust, the inability to manage litigation risk makes it improbable that a trust would be widely adopted in the private sector as a mechanism to facilitate data sharing in the innovation economy.

It may be that the term "data trust" is meant to invoke a new special purpose vehicle not yet developed by the federal government through legislation. If that is the intent, the case has not been made for developing such a vehicle. Further, the language used to describe these trusted data exchanges should not obscure whether they are being used for a profit-making purpose.

---

20 Hoffstein, ibid., HTR-82.

21 Paul B. Miller, *The Future for Business Trusts: A comparative Analysis of Canadian and American Uniform Legislation* (2011), 36 Queen's L.J. 443-502, at para. 26 (QL Advance).

22 See e.g. *Trustee Act,* R.S.O. 1990, c. T.23, ss. 17, 19, 21, 22, 24, 27(2), and 48.

23 S.O. 2004, c. 29, Sch A.

24 R.S.O. 1990, c S.5.

25 Hoffstein, *supra*, note 19, HTR-148.

RECOMMENDATION

13. The CBA Section recommends that regulations relating to trusted data exchanges be neutral with respect to the chosen business or legal structure.

ISED's proposal appears limited to "establishing a regime for use of de-identified data in PIPEDA".[26] The CBA Section recommends that ISED not limit trusted data exchanges to de-identified data. Trusted data exchanges could be used to facilitate sharing of personal information that has not been de-identified. This could be valuable for research and the activities of Statistics Canada and others. PIPEDA sections 7(2)(c) and 7(3)(f) create a high threshold to meet prior to using or disclosing information for statistical, scholarly study or research.

However, the CBA Section agrees that whether and to what extent data is de-identified should be one criterion among others that may be relevant to whether the personal information can be contributed to a data exchange without the consent of the individual. Other criteria may include sensitivity of the information and controls in place to prevent misuse, such as independent ethical review, confidentiality obligations and other contractual protections, and also in the case of data not fully de-identified, whether the individual is able to opt-out.

RECOMMENDATION

14. The CBA Section recommends that how appropriate the use of a trusted data exchange is be assessed by whether and to what extent the data is de-identified, and also other criteria, such as the sensitivity of the information and controls in place to prevent misuse.

To the extent de-identification is a relevant criterion, the CBA Section cautions against prescriptive regulation. The U.S. experience under the *Health Insurance Portability and Accountability Act* of 1996 and the "safe harbour" de-identification standard under the *HIPPA Privacy Rule*, section 164.514(b)(2) illustrate one of the dangers of setting a prescriptive standard. The safe-harbour allows the de-identification threshold to be met by removing

26 " Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act", Part 2, Section A ("ISED Proposal"); online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

certain identifiers. However, this may not be sufficient de-identification in many contexts. One answer might be to set a very high threshold, but this may ultimately stifle the use of data exchanges.

RECOMMENDATION

15. The CBA Section recommends that standards for de-identification not be prescriptive.

B. Self-Regulation and Technical Standards

In our view, the inevitable cost increase to businesses resulting from the certification mechanism should be weighed against potential benefits for consumers.

The OPC is an oversight agency and the CBA Section believes it should not be given authority to review an organization's adherence to a certification scheme. We suggest that the Standards Council of Canada should instead be given the sole authority for the certification scheme. It accredits Standards Development Organizations (SDO) to develop the National Standards of Canada (NSCs). An SDO develops a standard/certification scheme by consulting with subject matter experts, who become members of a technical committee. Participants in these committees give technical expertise and input and are often stakeholders in different sectors.

Similar to Schedule 1 of PIPEDA, "Principles Set Out in the National Standard of Canada Entitled Model Code or the Protection of Personal Information",[27] additional NSCs could be developed by the Standards Council of Canada and added to PIPEDA through approval by Parliament. The NSCs could act as accreditation schemes.

When developing NSCs, we believe that the Standards Council of Canada should:

- identify the need for the standard;
- review the existing standards landscape;
- engage affected stakeholders;
- notify the public at the project start;
- develop the standard (with technical experts);

27 CAN/CSA-Q830-96.

- publicly consult on the proposed standard;
- deal with comments received and revise as determined by the technical experts;
- conduct a vote and gain approval of the NSC;
- publish promptly; and
- maintain the NSC.

To be recognized as an NSC developed by a Standards Council of Canada accredited SDO, the standard must be developed in accordance with:

- consensus from a balanced committee of stakeholders;
- public scrutiny;
- consistency with (or incorporating) existing international and pertinent foreign standards;
- not acting as a barrier to trade; and
- ongoing maintenance, generally through periodic review (five-year cycle) or as needed.

The Standards Council of Canada has a thorough development and review process for accreditation standards. An NSC is developed with a balanced committee of stakeholders and experts, and accreditation and review of accreditation is generally performed by the Standards Council of Canada. Given this, we suggest that the degree of involvement of the OPC and ISED should be weighed carefully in these matters.

RECOMMENDATION:

16. The CBA Section recommends that the Standards Council of Canada be considered when determining accountability for a certification regime.

IV. PART 3 – ENHANCING ENFORCEMENT AND OVERSIGHT

A. Enhancing the Commissioner's Powers

In this section, the CBA Section proposes a package approach intended to ensure a meaningful and more robust enforcement regime, in the context we describe below.

When the entire legal framework for privacy in Canada is considered – PIPEDA, provincial and territorial laws, and common and civil law – Canadians are generally well-protected and companies have real incentive to protect personal information. PIPEDA's principles-based model will always mean some uncertainty when trying to apply principles to new products and services. In our view, Canadians and organizations will benefit most from a collaborative model that allows the OPC and organizations to work together to confront these challenges and develop new tools, like the new non-binding advance opinions program offered by the OPC.

The ombudsperson model for the OPC works well and is a valuable aspect of Canada's legal privacy framework. However, its effectiveness will suffer if it transforms into more of a prosecutor or enforcer model. The courts should remain the appropriate place for remedies.

Further, there is insufficient evidence that PIPEDA needs material fixing or strengthening. Complaints to the OPC are down and early resolution is up. In general, the public is unaware of how much Canadian businesses have done to improve handling of their personal information.

Finally, and most unfortunately, a few bad and highly publicized cases have received an inordinate degree of attention, which has added to calls for increased powers and enforcement.

Three key themes comprise the package approach that the CBA Section recommends:

1. policy considerations, guidance and procedural safeguards;
2. effective investigations and audits; and
3. meaningful tools to address offences and non-compliance, including financial impact.

Policy Considerations, Guidance and Procedural Safeguards

Mechanisms are needed to ensure that the OPC reflects government policy in carrying out its mandate as an agent of Parliament without policy making authority. Different mechanisms can achieve this goal:

- **Policy Objectives:** Adding a new explicit broad policy objectives section in PIPEDA that would apply to anyone interpreting or enforcing PIPEDA, similar to the *Broadcasting Act* and the *Telecommunications Act*. For example, policy objectives could explicitly require balancing between the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information, and consideration of innovation and economic competitiveness.

- **Policy Direction:** Introducing the ability for ISED to issue directions to the OPC requiring consideration of broader policy objectives (e.g. to consider economic development, encourage investment and innovation, balance with business needs, customer choice and experience).

Additionally, new procedural safeguards for OPC guidance would benefit both consumers and businesses by offering increased accountability and procedural fairness. For example:

- **Federal Court:** Introduce a new procedural safeguard via an amendment to the *Federal Court Act* to create a statutory ability to appeal to the Court a legal interpretation in a non-binding OPC guidance document (e.g. transfer for processing is a disclosure not a use).

- **Cabinet appeal:** Introduce an ability for ISED to review OPC guidance through a right for parties to seek Cabinet appeal.

- **Advance opinions:** The OPC has launched a program to give organizations non-binding advance opinions. ISED could support that program through structural support elements (e.g.: formalizing the OPC's authority in PIPEDA; exempting documents and communications from freedom of information requests, similar to breach reports and records under section 20(1.1); allowing cost recovery; and considering to what extent binding advance opinions might be appropriate).

Effective Investigations and Audits

There is a need to ensure the OPC conducts its investigations and audits effectively, efficiently and in a timely fashion. The CBA Section offers the following observations and suggestions:

- **Additional procedural safeguards for audit power:** PIPEDA should explicitly include administrative safeguards to the OPC's existing audit powers (e.g. long prior notice, clear indication of focus of audit, etc.) and exercise of audit powers should remain based on the current standard of reasonable grounds that there is a contravention of PIPEDA.

- **Additional discretion not to investigate complaints:** The grounds for the OPC not to investigate or to discontinue certain complaints should be expanded slightly (i.e. to refuse or cease to investigate if the investigation is unnecessary having regard to all the circumstances of the complaint).

- **Sharing with agencies:** Consider additional authority for the OPC to share information with other specific regulators (e.g. Competition Bureau), for specific purposes (e.g. similar to CASL section 58). It will be important to consider what information can be shared (e.g. exclude information that was shared with a regulator by the organization on a confidential basis).

- **Timely investigations and guidance:** The OPC has lagged on quick investigations of complaints and publishing reports of findings, delaying

outcomes for individuals and guidance for organizations. The OPC should be held to a one-year deadline for complaint investigations. This would also allow the option of seeking timelier recourse before the Federal Court.

Meaningful Tools to Address Offences and Non-compliance, including Financial Impact

The CBA Section recognizes the need for real enforcement and consequences for non-compliance but does not support any major shift in the current roles and functions of the actors that make up the PIPEDA enforcement regime (i.e. OPC, Federal Court and the Attorney General).

RECOMMENDATION:

17. The CBA Section recommends that there not be any major shift in the current roles and functions of the actors that make up the PIPEDA enforcement regime, and the OPC should instead be encouraged to use existing powers and tools.

The following tools or changes to existing tools might also be considered to expand the impact and reach of each of those actors:

- **Limited OPC cessation and records preservation orders:** As extreme powers, cessation and records preservation orders are usually not appropriate for an ombudsman model. However, those powers might be extended to the OPC and reserved for egregious cases including imminent material harm to individuals. They should not be available to challenge normal business practices or differences of opinion or interpretation. Careful consideration should be given to the timing to exercise these new powers and any right to appeal.

- **Direct route to the Federal Court:** In more egregious cases, where it would not be efficient or effective for the OPC to first conduct an investigation and then start over again in seeking recourse before the Federal Court, both the OPC and individuals should be allowed to go directly to the Federal Court. This would need careful consideration to identify the necessary threshold when a direct route to the Federal Court is appropriate.

- **New offences for AG to prosecute:** The OPC has never yet referred a matter to the AG for prosecution. Still, likely the least controversial way to augment enforcement is to expand the offences that could be referred to the AG for prosecution, e.g. insufficient safeguards, deliberate re-identification, other material non-compliance with PIPEDA. Any expansion of offences would have to reflect any need for intent, be limited

to more egregious actions, include any necessary procedural safeguards, and offer a due diligence defence.

- **Do not introduce statutory damages:** Typically, statutory damages are reserved for situations where harm is presumed but difficult to assess. With PIPEDA, most often breaches are without direct harm. Statutory damages would open floodgates to class actions as harm would not have to be proven, and that is why courts are best placed to assess damages.

V. PART 4 – AREAS OF ONGOING ASSESSMENT

A. Clarity of Obligations

We support PIPEDA's principles-based and technology-neutral approach. Both elements have been key to PIPEDA's continued success in protecting Canadians as intended, while also offering the necessary flexibility for the law to evolve with changing technologies and circumstances.

PIPEDA's intent has been clear from its inception. It may be that difficulties in understanding PIPEDA's intent are more a problem for small and medium-sized businesses and not-for-profits, where capacity and resources are often challenges.

Redrafting the law with the suggested "housekeeping measures" in hopes of offering more clarity could risk limiting the current flexibility in interpreting PIPEDA to address rapidly evolving technological issues. While the CBA Section supports further guidance on interpreting the law[28], we are concerned that any measures to limit the flexibility of the legislation could make the law more, rather than less, complicated. For example, the proscriptive nature of the EU's GDPR, with very specific wording has arguably made interpretation of the law more difficult, as it limits organizational capacity to deal with different views regardless of the practical implications of interpretation.

B. Scope of Application, Accountability

The CBA Section understands that constitutional considerations come into play when contemplating any expansion to the current scope of PIPEDA. While we have recommended that PIPEDA be applied to political parties, and that the application of PIPEDA to not-for-profits and charities be clarified, we also appreciate the constitutional rationale for limiting PIPEDA's

28 See, CBA Submission Bill C-76, Elections Modernization Act, supra, note 3.

application to personal information that an organization collects, uses or discloses in the course of commercial activities (section 4(1)(a)). Given that there still is no bright line test for determining what will and will not be considered a commercial activity for the purposes of PIPEDA, however, we recommend that ISED consider whether alternate approaches to the demarcation of PIPEDA's scope might be more effective than the current approach. For example, ISED could consider whether PIPEDA would be clearer if all actors came under its scope by default, subject to specific exemptions or exceptions to the PIPEDA consent requirement for certain, defined activities, consistent with the existing journalistic, artistic or literary purpose exemptions of such entities as political parties, charities and not-for profits.

VI. CONCLUSION

The CBA Section believes that the issues raised by the consultation document are timely and important. We encourage further consultation with a wide cross-section of stakeholders before making changes. Our recommendations are summarized below for ease of reference.

SUMMARY OF RECOMMENDATIONS

1. **The CBA Section recommends that PIPEDA's consent regime be bolstered through additional information provided to individuals.**
2. **The CBA Section recommends that any changes to consent account for adequacy with the GDPR and be made in that context.**
3. **The CBA Section recommends that gaps in the legislative framework be addressed: a) the inclusion of political parties, and b) clarification of the application to charities and not-for-profit industries.**
4. **The CBA Section recommends that ISED avoid a siloed privacy approach, but instead work closely with other impacted sectors, including competition and consumer protection.**
5. **The CBA Section recommends that any right to data mobility be conditional on the implementation of sector-compatible frameworks and infrastructure that permit interoperability and secure data flow.**
6. **The CBA Section recommends that any proposals in the area of data security consider authentication issues.**

7. **The CBA Section recommends that data mobility be limited to the same principles as currently exist in PIPEDA.**
8. **The CBA Section recommends that any subsequent liability for personal information be removed from organizations where data recipients have not adequately protected that data.**
9. **The CBA Section recommends that organizations remain accountable for continuing holding data for any ongoing business purposes.**
10. **The CBA Section recommends limiting the role of the OPC to overseeing individual access rights and related privacy considerations typically falling within scope of PIPEDA (such as appropriate safeguards and accuracy of information) and that alternative government agencies are better suited to determining industry specific frameworks for data porting.**
11. **The CBA Section recommends that ISED consider amendments to PIPEDA to require organizations to disclose which criteria they use to define retention periods for broad categories of personal information.**
12. **The CBA Section recommends that ISED work with provincial and territorial governments to develop a multi-jurisdictional approach to enhancing protections for children from unlawful attacks on their honour and reputation, which may include, but should not be limited to, strengthening the protections for children under PIPEDA.**
13. **The CBA Section recommends that regulations relating to trusted data exchanges be neutral with respect to the chosen business or legal structure.**
14. **The CBA Section recommends that how appropriate the use of a trusted data exchange is be assessed by whether and to what extent the data is de-identified, and also other criteria, such as the sensitivity of the information and controls in place to prevent misuse.**
15. **The CBA Section recommends that standards for de-identification not be prescriptive.**

16. **The CBA Section recommends that the Standards Council of Canada be considered when determining accountability for a certification regime.**

17. **The CBA Section recommends that there not be any major shift in the current roles and functions of the various actors that make up the PIPEDA enforcement regime, but that the OPC should instead be encouraged to use existing powers and tools, as outlined above.**