Centre for Information Policy Leadership
Hunton Andrews Kurth

27 September, 2019

CIPL Comments on Innovation, Science and Economic Development Canada's Proposals to Modernize the Personal Information Protection and Electronic Documents Act

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to Innovation, Science and Economic Development Canada's (ISED) recently released white paper entitled "Strengthening Privacy for the Digital Age",[2] which puts forward general proposals for amending Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). CIPL agrees with many of the issues raised and specific proposals made in the white paper and hopes that our responses below are helpful in thinking through these issues and ultimately amending PIPEDA. For background, CIPL also recently responded to three other Canadian consultations – two by the Privacy Commissioner's Office on cross-border data transfers and one by the Department of Justice on the issue of amending the Privacy Act[3] -- which include discussions of issues related to some of the issues addressed below.

Comments

I. General Comment

The Dual Goals of an Effective Privacy Law

CIPL strongly agrees with ISED that data collection, management and use must be "built on a strong foundation of trust and transparency between citizens and government" and that PIPEDA should be updated to help deliver on this goal. As ISED makes clear in its consultation paper, the underlying goal, as identified in Canada's Digital Charter and the current PIPEDA review, is a "strong and vibrant digital economy for Canada." PIPEDA, according to ISED, "is a key element of Canada's marketplace framework" that must deliver not only information security and privacy, but also predictability for business and

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Strengthening Privacy for the Digital Age, Innovation, Science and Economic Development Canada, 21 May 2019, available at https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

[3] See CIPL Comments on the Office of the Privacy Commissioner of Canada's Consultation on Transborder Dataflows, 17 May 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_office_of_the_privacy_commissioner_of_canadas_consultation_on_transborder_data_flows.pdf; CIPL comments on the Office of the Privacy Commissioner of Canada's Reframed Consultation on Transfers for Processing, 5 August 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_opcs_reframed_consultation_on_transfers_for_processing.pdf; and CIPL response to Justice Canada's Technical Engagement with Experts on the Modernization of Canada's Federal Privacy Act, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_justice_canadas_technical_engagement_with_experts_on_the_modernization_of_canadas_federal_privacy_act__21_augu.pdf.

international competitiveness in a data-driven, digital global marketplace. We fully agree with ISED's concise statement that the goal of Canada's modernization of its private-sector policy and regulatory framework must be "to protect privacy and support innovation and prosperity" (emphasis added). CIPL believes that Canada should take the modernization of PIPEDA as an opportunity to state this goal more explicitly in PIPEDA.

Currently, Section 3 of PIPEDA states that its purpose is to establish "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals [. . .] and the need of organizations to collect, use or disclose personal information. . . ." Thus, PIPEDA already acknowledges both privacy and the need to be able to use personal information as its goals. ISED's white paper affirms PIPEDA's dual purpose of "protect[ing] privacy and support[ing] innovation and prosperity," and notes that because of "the importance of data- and digitally-driven innovation to Canada's economy and prosperity, the legislative marketplace must be balanced and fit for purpose." We therefore recommend that in its next iteration, PIPEDA should even more clearly articulate the law's mandate to balance privacy with the ability of organizations to innovate and use personal information effectively.

Modern data protection authorities are at the epicenter of not only privacy protections but also how we leverage and manage the most valuable resource of the digital economy. Their traditionally primary responsibility of protecting individual privacy must be carried out in light of an additional responsibility of enabling accountable innovation and beneficial data uses. In practice, this would mean that interpretations of the law should be made with consideration of the implications for legitimate and beneficial information uses, and decisions about how personal information may be used should consider legitimate privacy rights and interests. Accordingly, we recommend that the dual goal of PIPEDA and dual responsibility of the Privacy Commissioner be clearly stated in the revised law.

II. Comments on ISED's Paper "Part 1: Enhancing individuals' control"

CIPL agrees with ISED that the volume and complexity of data flows has strained the traditional knowledge- and consent approach to privacy protection, which is at the heart of PIPEDA. This approach has become ineffective in the modern digital economy as it places too much responsibility on the individual to protect him or herself by continually having to understand what is happening with their personal information and making appropriate choices and giving or withholding consent. This approach is not sustainable in an increasing number of modern information use contexts and the problems with this approach are aptly described in ISED's discussion paper.

ISED is seeking comments on how to improve PIPEDA's individual control or consent model, for example by adding further exceptions to the consent requirement, by adding control mechanisms such as data portability, by introducing heightened consent requirements for "sensitive" personal information, and by improving transparency. On these issues, CIPL would like to make the following comments and recommendations:

(1) **De-emphasize consent and make it one of several co-equal bases for processing.** Essentially, PIPEDA requires individual consent to the processing of personal information unless an exception applies that permits processing without consent. This approach is based on an "individual control" paradigm for privacy and data protection. CIPL submits that this is an outdated model for legitimizing the processing of personal information as it privileges consent over other bases for processing. As outlined in ISED's

paper itself, that paradigm is unworkable in the complex modern digital economy. In addition to unreasonably burdening individuals, it also has the potential to preclude or undermine completely legitimate, necessary or beneficial processing activities if they are not covered by one of the existing statutory exceptions to consent and/or if consumers withdraw consent or fail to give consent. As ISED notes in its paper, "complex data flows involving numerous parties strain an individual's ability to fully comprehend what they are consenting to." Given that, it is inevitable that consumers will make incorrect assumptions about certain types of potentially beneficial processing.

ISED suggests updating this approach by adding additional exceptions, such as one for common uses of personal information for standard business practices or for "common business practices," such as providing a service or for sharing information with a third party processor. However, we believe that merely adding these additional exceptions would leave in place the current structure that makes consent the principal and most important legitimizer of using information. We believe that this would be a mistake and a lost opportunity to truly modernize the law and to align it with other important global data protection frameworks that employ a more balanced approach. Not only would such alignment with global frameworks more effectively reflect the needs of modern data processing, it would also improve interoperability between different privacy regimes.

Thus, we recommend instead that Canada adopt the approach followed by other modern privacy laws and provide for a number of co-equal grounds for processing from which businesses can choose the most appropriate options in a given context. Following the GDPR model, in addition to consent, these grounds would include processing that is necessary for the performance of a contract, necessary for compliance with a legal obligation, in the vital interest of the data subject, in the public interest, and for a legitimate interest.[4] Applied properly, all possible processing scenarios should be covered by these processing grounds, although there is room for improvement even in the GDPR grounds for processing.[5]

Among these grounds for processing, "legitimate interest" takes on a particularly important function in the fast moving, rapidly developing and changing digital economy. This is because it is capable of legitimizing any processing operations (including those that might be as of yet unknown or unimagined and thus not susceptible to specially-designed exceptions to consent) in which the legitimate interests of the business or a third party are not outweighed by the rights and freedoms of an individual, as determined by a risk/benefit assessment.

To ensure that such processing does not remain unchecked, it is essential that it be considered in light of PIPEDA's already-existing fair information principles including Accountability, Identifying Purposes, and Limiting Collection.[6] Further, as noted, the legitimate interest ground for processing requires that organizations conduct risk assessments with respect to their proposed processing operations. These

[4] Article 6 GDPR

[5] For example, "necessary for a core activity" is more flexible and future proof than the EU lawful basis of "necessary for the performance of a contract" and could accommodate certain legitimate and non-contentious processing activities better than the current GDPR grounds for processing. EU Member States, in fact, have had to introduce additional lawful bases for non-contentious processing to make up for the narrowness of the contractual necessity lawful basis. For example, UK law contains lawful bases for things like employment activities, equality monitoring, counseling, safeguarding children, anti-doping in sport, non-profit activities, and legal proceedings.

[6] PIPEDA Schedule 1.

risk assessments require organizations to engage in a balancing and cost/benefit analysis between the purported legitimate interests and any countervailing risks to individuals as well as to tailor any mitigations and controls specifically to the identified risks. The risk assessments must be demonstrable to relevant authorities such as the OPC and should occur within commonly agreed parameters for such risk assessments that include guardrails for what risks and harms to consider and how to measure and weigh them.[7] Such guardrails could be staked out in the law itself, or, provided and/or further developed by the OPC or other relevant authorities. Guidance could include lists of standard business practices that would be covered by the legitimate interest ground for processing, such as fulfilling a service, using information for authentication purposes, sharing information with third-party processors, risk management, etc., as already suggested in ISED's discussion paper.

Such restructuring of PIPEDA around co-equal bases for processing would leave consent available for contexts where it can be truly effective and useful. For example, it could be used in circumstances where the use of the information is of such high and unavoidable risk and potential impact, even after putting in place mitigations for such risk, that asking for consent would be appropriate, as ISED's paper already suggests. However, it is important to note that consent is not necessarily always the proper legitimizer of information uses "that have the biggest impact on individuals," as suggested in one of ISED's proposals. Indeed, it would be inappropriate to require consent on the basis that the use has a significant impact where, in fact, that use is necessary for an activity to occur. For example, various background checks typically are needed before a bank can provide credit or a loan, and not getting the credit or loan could have a significant impact on an individual. However, such checks cannot be optional or reliant on consent.

Should ISED decide not to pursue our suggested approach, additional exceptions to consent must be introduced to the current regime if PIPEDA is truly to deliver on its promise for a balanced approach to privacy and innovation. Specifically we would recommend a further exception for processing activities in which the business or a third party has a "legitimate interest" (which is one of the processing grounds under the EU General Data Protection Regulation (GDPR) and other modern privacy laws) so long as such interest is not outweighed by the interests and rights of the individual data subjects.

(2) **Exempt anonymized or truly de-identified information from relevant requirements of PIPEDA.** ISED indicates a desire to align PIPEDA's treatment of anonymized/de-identified or pseudonymized data with other privacy laws in order to protect privacy and enable innovation. CIPL agrees with this

[7] See CIPL's white paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf; CIPL white paper on Protecting Privacy in a World of Big Data, The Role of Risk Management, 16 February 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf; CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data, 27 April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf; and CIPL white paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

sentiment, though we, again, recommend against trying to accomplish this through an exception to consent, and instead through a broader exception for truly de-identified information from all relevant statutory requirements (such as consent) after PIPEDA has been re-organized around multiple co-equal bases for processing. However, regardless of how it is incorporated into the law, anonymization and de-identification can be important measures for organizations to use personal information effectively while also protecting individual privacy. Accordingly, these tools should be encouraged in the law.

Incentives for de-identification, in addition to exemption from consent, would be the ability to use the de-identified data for internal research or for AI development without having to set pre-defined retention periods or the data being in scope for the exercise of individual rights such as access, correction and deletion.

ISED rightfully points to the increasing ability to re-identify previously anonymized and de-identified information through sophisticated techniques and asks what protections are available to address this problem. CIPL believes that in light of the fact that complete and permanent anonymization or de-identification is increasingly difficult, technical anonymization techniques must in some contexts be complemented by enforceable administrative, technical, physical and legal safeguards that prohibit attempted re-identification of personal information except for certain permissible purposes.

One useful standard for such de-identification plus safeguards, which CIPL supports, was articulated by the US Federal Trade Commission in 2012: Personal information should be subject to fewer privacy protections or legal requirements if (1) the data is not reasonably identifiable; (2) the company publicly commits not to re-identify it; and (3) the company requires downstream users of the data to keep it in de-identified form.[8] This standard could be translated for the Canadian legal framework to mean that anonymization or de-identification requires reasonable technical anonymization or de-identification in light of the purpose for which the information is being used, coupled with appropriate contractual and legal safeguards that ensure an enforceable obligation not to re-identify the information.

Finally, some re-identification is legitimate in a few specific circumstances and must be protected by appropriate exceptions. For example, in situations where genuine security research aims to test security measures and techniques, re-identification of data that has been de-identified should not be subject to penalties. Those carrying out such genuine testing could be obliged to inform the company first before going public with their findings. This would mitigate the risk of people making public disclosures that could negatively impact individuals and claiming a defense of security testing.

(3) **Require relevant and actionable transparency.** ISED proposes "requiring organizations to provide individuals with the information they need to make informed decisions, including requiring specific,

[8] U.S. Federal Trade Commission report, "Protecting Consumer Privacy in an Era of Rapid Change, Recommendation for Business and Policymakers," March, 2012 at 22, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

standardized, plain-language information on the intended use of the information, the third parties with which information will be shared, and prohibiting the bundling of consent into a contract."

CIPL agrees that understandable user-centric transparency is foundational to effective privacy protections and creating trust in the digital economy. It is important to keep in mind that transparency serves different or multiple purposes, depending on the context. For example, it enables consent in appropriate contexts, provides information about other individual rights, such as how individuals can access or correct information, block or opt out of certain uses, or seek redress in the event of erroneous decisions or some legal violation, and it builds trust where the goal is to generally explain an organization's data uses and accountability measures.

While it is helpful to determine what kinds of information organizations must provide to individuals, it is not necessarily helpful to try to standardize the approach so that it becomes proscriptive and inflexible. Organizations need to be able to provide the required information in a format and style that makes sense for their customers in light of the purpose of providing the information (e.g. obtaining consent, providing other actionable information or providing general information) and the nature of their products and services. For example, a mobile app is very different from an online website, and a financial services product is very different from a weather app. Transparency rules should not be one-size-fits-all but be flexible enough to support varying levels of detail depending on the purpose of the information.

It may be helpful to allow organizations to distinguish between information necessary for the core product or service they provide or for a particular feature to work, and situations where providing information would be voluntary. For example, individuals must provide their location if they want to get the weather forecasts where they are now, but they would not be required to provide their location or email address to receive marketing, unless they want receive marketing. Thus, transparency must be tailored to the specific purposes at hand.

In the context of automated decision-making, we do not recommend a different transparency standard than for other types of processing. Transparency standards in the law should be generally applicable to all data processing, focusing on the delivery of understandable, actionable and relevant information to individuals. In particular, we do not recommend algorithmic transparency when that term is understood to refer to disclosing the algorithms, as algorithms are proprietary and because most individuals would not be able to understand complex algorithms. However, individuals should be able to find out what kind of data goes into AI and automated decision making models, how decisions generally are made, how to correct false information and how to remedy erroneous decisions.

(4) **Include a right to data portability that reflects technical feasibility**. Data portability is an important right for improving individual control over one's personal information, especially given that other jurisdictions are including it and many businesses are implementing it. The right to receive one's personal data so that she can port it to another service if she chooses should be applied broadly with minimal exception. Additionally, we believe that it is important for laws to encourage direct service-to-service transfers where such transfers are technically feasible, as is required in the GDPR, and upon receipt of a verifiable request from the individual. However, it is important to recognize that there are technical issues that should be further considered to facilitate the ability to transfer data from one

service to another. For example, this is an area where standardization of process and instructions for how companies should respect portability signals would be helpful, particularly before strict service-to-service portability obligations are enacted.

As to the specific data that is subject to portability, a portability provision should be limited to data provided by individuals themselves, transactional data, and to some, but not all, forms of observed data about them (e.g. it could include data observed through tracking devices where such observed data is part of the service desired by an individual). It should not apply to inferred data or to de-identified data or to call-notes and complaints (some of which might still be subject to access requests, however). Further, as mentioned, the right should be limited to personal data that is linked to the reason for the porting request rather than to all covered data. (see examples above).

Also, the contexts and nature of businesses to which data portability should apply should be considered and limited to those types of businesses where portability makes sense. Given the need for developing and implementing appropriate technical standards, processes and infrastructure to operationalize this right, sufficient time should be given for this, possibly by applying a phased approach to implementation. In addition, there is a need for defining the appropriate level of authentication of a porting request that protects both the data subject and the organization and prevents fraud.

(5) **Any definition of "sensitive" data should be rebuttable rather than definitive.** In the context of strengthening meaningful control and consent for individuals, ISED asks whether sensitive personal data should be defined and heightened protections (such as prohibitions or explicit consent) be required. CIPL is of the view that restricting the use of certain data by labelling them *per se* "sensitive" does not necessarily ensure appropriate protection for individuals and can even have the opposite effect. For example, in the context of AI and machine learning, including sensitive data in the datasets may be necessary to detect and avoid unintended biased and discriminatory algorithmic results. A Human Resources file containing the fact that a person had three days' absence for the flu is very different from a hospital medical record, yet both are sensitive data subject to the same restrictions and conditions under the EU GDPR.

Any list of what is deemed to be sensitive personal information runs the risk of being both under-inclusive or over-inclusive, depending on context. Because the sensitivity of personal information is contextual, we recommend that the level of sensitivity (and hence risk) and the necessary corresponding protections for certain categories of data (as well as for certain types of data uses) be captured through a rigorous risk-based approach to all data use activities. Organizations should be required and enabled to determine the risks associated with their own specific processing activities through risk assessments and to create appropriate mitigations and controls on that basis. (See further discussion on risk assessments below in Section V.) Such risk assessments should be demonstrable to the OPC pursuant to the powers afforded to the Office under PIPEDA as well as conducted within applicable general parameters set forth in the law or regulatory guidance.

Thus, we do believe that it would be appropriate to require the Office of the Privacy Commissioner to provide regulatory guidelines as to what types of personal information might be particularly sensitive or risky, but the sensitivity of the included categories should be rebuttable through risk assessments that determine the actual level of risk and the necessary mitigations in a specific context. This approach would strike an appropriate balance of providing guidelines for industry as to what kinds of

personal information may be sensitive and thus deserving of heightened protections and leaving sufficient flexibility for organizations to use demonstrable risk assessments and tailored mitigations to rebut "sensitivity" status in particular contexts.

III. Comments on ISED's Paper "Part 2: Enabling responsible innovation"

ISED's discussion paper points out the ever-increasing demand for access to personal information in the digital, data-driven economy. It notes that that this, in turn, triggers the need for increased accountability and higher standards of care to ensure privacy and data security. However, according to ISED, there is a concern that "it is not always clear how a principles-based law applies to new business models/technologies." Accordingly, ISED is looking for new ways to make the legislative frameworks that support the digital economy fit for purpose.

One possible area of improvement on that front that ISED points to is "self-regulation and technical standards." CIPL believes there is tremendous untapped potential for making use of industry codes of conduct, privacy certifications and the use of technical standards in lifting the general level of compliance and accountability across all industries. As an initial matter, we would suggest that the more appropriate term for these tools would be "co-regulation", as they typically are, or should be, subject to government/DPA backstop enforcement. Also, frameworks like the APEC Cross-Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP) were developed in multi-stakeholder processes led by governments and data protection authorities and thus were significantly shaped by them. Referring to them as "self-regulation" would be misleading. Indeed, ISED's paper itself also proposes regulation-making authority by ISED and formal recognition and enforcement by the OPC in connection with such schemes, indicating a formal government role in their creation and operation. Thus, to be more accurate -- and also to avoid the traditional skepticism about industry self-regulation -- we think "co-regulation" would be the more apt term.

An important development is the introduction of ISO/IEC 27701, a new international standard designed to help organizations reconcile privacy regulatory requirements. The standard outlines a comprehensive set of operational controls that can be mapped to various regulations, including PIPEDA and GDPR. These operational controls can be implemented by privacy professionals and audited by internal or accredited third-party certification bodies resulting in a certification and comprehensive evidence of conformity. Since the use of ISO standards is, by definition, adherence to WTO Technical Barriers to Trade (TBT) practices, ISO/IEC 27701 can be helpful for Canada to assure adequate data protection without risking negative impact to trade.

Codes of conduct and privacy certifications can be used both as effective domestic compliance tools and as mechanisms for ensuring accountable cross-border transfers of personal information, as pointed out in ISED's paper. Thus, CIPL strongly agrees with ISED that these mechanisms should be further enabled, encouraged and specifically incentivized under an updated PIPEDA.

Not only would this contribute the tools available to Canadian companies to assist with their domestic compliance obligations, it would also help address the concerns raised by the OPC in its recent public consultation on strengthening the privacy protections for individuals in the context of cross-border transfers of personal information for processing purposes. In its consultation, the OPC proposed

introducing a consent requirement for such transfers, but just recently announced it would not be implementing such a requirement. The consent requirement not only would have been ineffective and impracticable, but also would have undermined Canada's goals of devising a privacy framework that is truly fit for purpose in the global digital economy. CIPL provided detailed comments on that proposal[9] and argued that the better way to address the OPC's concerns would be to strengthen and enforce PIPEDA's accountability provisions.

One way to strengthen accountability under PIPEDA would be the use of privacy codes of conduct and certifications. Canada has already joined one such formal accountability scheme – the APEC CBPR; but it has not yet fully implemented the rules more than four years after joining the system. Thus, we strongly encourage additional emphasis on building out the CBPR and other privacy codes of conduct and certifications in Canada. The potential benefits of these systems cannot be overstated. Based on ISED's discussion paper, it appears ISED is already fully aware of them.[10] With the newly available ISO/IEC 27701, Canada has another accountability tool at its disposal to uphold data protection. Note that ISO/IEC 27701 builds upon the already widely adopted ISO/IEC 27001 standard for information security with over 60,000 known certifications globally.

ISED does raise two common concerns with respect to certifications, codes of conducts and standards: that they are "expensive, and without appropriate oversight, they can be at best meaningless and at worst deceptive."

CIPL agrees that scalability and affordability are important issues to consider, especially given that one of the principal beneficiaries of such schemes should be small and medium-sized enterprises (SMEs). SMEs often do not have the necessary in-house expertise nor the resources to develop their own comprehensive privacy compliance programs to implement relevant privacy requirements. One of the benefits of formal accountability schemes such as certifications and codes of conduct is that they typically involve third-party certification bodies, accountability agents or other oversight entities that can provide this expertise. Providing what are essentially custom-made comprehensive privacy compliance programs to organizations that otherwise would have difficulties creating their own is a significant benefit. Thus, if

---

[9] *Supra* note 3.

[10] For a more detailed discussion of the benefits of codes of conduct and certifications and related co-regulatory formal accountability schemes, please see the following CIPL white papers: The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, 25 September 2017 available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf; and Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, 12 April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

codes of conduct and certifications are designed to be flexible, scalable and capable of being calibrated to the size, nature and level of risk of an organization's information uses, then they should also be affordable at scale.

It is also important not to conflate the cost of establishing and documenting data protection practices as part of the cost of certification because establishing and documenting these practices is a matter of legal compliance that all organizations should engage in. The cost of certification should primarily consist of the cost of organizing existing documentation and the engagement of the certification body. Assuming data protection practices are already well-documented, the cost of certification for SMEs is, in fact, nominal. While we are familiar with concerns and criticisms with respect to overly burdensome bureaucratic requirements in connection with certain existing standards,[11] CIPL believes that the scalability problem can be addressed through the risk-based calibration of the rules and requirements contained in a specific certification or code.

CIPL also agrees that oversight is an important issue. That is why there must be accreditation of certification bodies and accountability agents that can deliver strong front-line day-to-day oversight and enforcement, as well as strong and credible government backstop enforcement through the OPC or other relevant agencies. Standards Council of Canada (SCC) is the official national accreditation body of Canada. CIPL encourages the engagement with SCC to administrate the accreditation of certification bodies and accountability agents to uphold the integrity of certifications and codes of conduct. We believe that if such oversight and enforceability requirements are reflected in PIPEDA, such co-regulatory schemes will be meaningful.

As to ISED's specific questions on oversight, we believe that especially where the formal accountability scheme involves officially recognized and approved certification bodies, accountability agents or other oversight entities, the OPC does not necessarily need the authority to pro-actively engage in compliance spot-checks in the absence of a formal enforcement action relating to specific alleged violations. Exercising vigorous backstop enforcement *vis-à-vis* such schemes to address specific violations should provide sufficient credibility to them. Moreover, the certification process and other oversight and front-line enforcement activities by the third-party entities, including complaint handling processes that are part of such schemes, should itself be subject to oversight and enforcement by a relevant government authority and/or the OPC or SCC, which will further strengthen the credibility of these schemes.

IV. Comments on ISED's Paper "Part 3: Enhancing Enforcement and Oversight"

[11] See CIPL Comments on the Article 29 Data Protection Working Party's "Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679" at 3 ("When considering to what extent the ISO standard should 'guide' the accreditation standards developed by the SAs and EDPB, relevant international experience dealing with certifications under ISO conformity assessments should be considered where the ISO standards have failed to ensure scalability and affordability for purposes of micro, small and medium-sized enterprises."), 29 March, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_guidelines_on_accreditation_of_certification_bodies_under_the_gdpr.pdf.

Initially, CIPL appreciates ISED's reference to CIPL's white paper "Regulating for Results: Strategies and Priorities for Leadership and Engagement,"[12] as setting out a framework that may be instructive for improving Canada's own approach to privacy oversight and enforcement under PIPEDA. As discussed in our above-referenced white paper, we believe data protection authorities must be empowered to prioritize enforcement matters based on their significance and potential impact on industry practices rather than be required to address all complaints received from individuals. Thus, they must be able to exercise discretion to select matters for investigations and enforcement based on the risks and harms involved, taking into consideration the potential impact in terms of messaging and standard setting any formal ruling and remedy will have on the wider industry. Only such ability to be selective and to prioritize in terms of what complaints to pursue and what enforcement matters to undertake will maximize the impact of the OPC's limited resources.

As already suggested in ISED's paper, to compensate for the potential reduction of focus on individual complaints by Canadian citizens, PIPEDA's oversight and enforcement framework could place more emphasis on the use of formal accountability schemes, such as codes of conduct and certifications, as discussed above. Such schemes could have (and the APEC CBPR do have) formal complaint handling and redress mechanisms designed to address the complaints of individuals. By shifting responsibility for resolving much of the less-egregious alleged privacy violations to third-party certification bodies, accountability agents and other relevant dispute resolution organizations, PIPEDA could free up OPC time and resources to focus on the significant and most important privacy violations. Under these schemes, important matters that fail to be resolved either by the businesses themselves or the relevant third-party dispute resolution providers could still be referred to the OPC for potential enforcement.

V. Comments on ISED's Paper "Part 4: Areas of Ongoing Assessment"

CIPL agrees that PIPEDA should remain a principles-based and technology neutral law. A principles-based approach to privacy protection is the right approach as it allows for organizations to implement the desired outcomes in a flexible and context-appropriate manner, based on the actual risks associated with the information uses at hand.

In fact, context-appropriate and risk-based privacy protections are at the heart of organizational accountability, which, in turn, has been at the heart of Canada's approach to privacy protection under PIPEDA. And the accountability-based model to privacy has served Canada well. It has cemented Canada's reputation as a pioneer and leader in promoting organizational accountability globally. It has also been widely regarded as a pragmatic and effective governance model for cross-border data transfers, demonstrating a compelling alternative to more cumbersome approaches that rely on a combination of transfer restrictions and various rationales and mechanisms to get around them. In connection with a possible restructuring and updating of this approach, we would like to make the following three suggestions:

[12] Regulating for Results – Strategies and Priorities for Leadership and Engagement, 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf.

- **Make implementing a comprehensive (though scalable) privacy management program an explicit requirement for businesses.** At the core of an accountability-based approach to privacy is having a comprehensive internal privacy program that enables an organization to comply with all relevant substantive requirements and handle personal information responsibly. PIPEDA, in effect, requires such programs as Principle 4.1 on Accountability requires organizations to "implement policies and practices to give effect to the principles" set forth in Schedule 1. It might be helpful if the requirement of having a comprehensive privacy management program capable of implementing, and enabling compliance with, all applicable substantive requirements of PIPEDA, be made more explicit. Because most Canadian businesses are SMEs, the scalability of such programs is a significant issue; they must be adaptable to the size of the business and the nature of its processing activities. Further, as discussed above, privacy codes of conduct and certifications (such as the CBPR) can be effective in assisting SMEs with their domestic compliance programs.

- **Include risk-assessment as part of an accountability-based privacy program.** CIPL agrees with the sentiment expressed in ISED's paper that privacy management programs should include flexible risk assessment processes. Principle 7 in Schedule 1 on Safeguards already implies risk assessments for information security safeguards by requiring safeguards that are "appropriate to the sensitivity of the information." We suggest a broader application of risk assessments. A risk-based approach to privacy enables a more targeted focus on harm prevention, as it requires organizations to assess the risks of harm to individuals associated with their particular information uses, weigh them against the benefits of these uses to individuals and society, and to fashion mitigations and controls specifically to the identified risks. Calibrating privacy compliance measures to actual risk provides significant benefits to: (i) consumers in terms of more relevant and targeted protections; (ii) businesses by enabling them to be more effective with limited compliance resources and allowing them to engage in a broad range of information uses that are not harmful but that might otherwise be precluded by inflexible rules that apply across the board regardless of risk; and (iii) regulators whose oversight and enforcement work will be aided by demonstrable risk-assessments performed by businesses.[13] It will particularly help smaller

[13] CIPL has published several papers discussing the risk-based approach to privacy and risk assessments in detail. They include: (a) Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf; (b) A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 19 June 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; (c) The Role of Risk Management in Data Protection, 23 November 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf; (d) Protecting Privacy in a World of Big Data, The Role of Risk Management, 16 February 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf; and (e) Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679," 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf.

organizations and startups avoid unnecessary administrative burdens by allowing them to scale and calibrate their compliance based on risk to individuals. It also ensures that the law remains technology-neutral and future proof, as an appropriate risk/benefit assessment process can be applied to any current and future technology, data use and business practice.

- **Clarify that Canada's accountability-based approach applies to cross-border data flows.** To date, PIPEDA has been interpreted to allow Canadian companies to transfer personal information across borders for processing purposes so long as they had safeguards in place (e.g. contracts) that required the recipient organization to protect the information at the Canadian level. In other words, Canada's model has been to hold Canadian organizations accountable for the protection of personal information regardless of where it flows.

  The OPC recently suggested changing this approach by introducing a consent requirement for cross-border data transfers for processing purposes, though ultimately decided not to implement such a requirement. CIPL urged against introducing a consent requirement and hopes OPC does not consider a consent requirement again in the future for the following reasons: (1) It would not add protections for individuals; (2) any problems with the current approach could be addressed by strengthening organizational accountability; (3) requiring consent would be burdensome to individuals and businesses, would confuse individuals and reduce privacy protections, and, in some cases, would be impossible; (4) requiring consent would be inconsistent with other global approaches such as the GDPR; (5) it would be inconsistent with the APEC CBPR in which Canada is a participant; (6) it would be inconsistent with the OECD Privacy Guidelines; and (7) it would undermine Canada's commitments under several trade agreements.[14]

- **De-emphasize the relevance of individuals' expectations.** ISED's paper notes that a revamped PIPEDA should continue to include "respect for context, individuals' expectations and overall emphasis on reasonableness." With respect to "individuals' expectations" we would urge caution. Routinely relying on whether a data use is expected seems risky and unhelpful in the modern and increasingly complex digital economy, as many processing operations are not even remotely within most individuals' awareness and thus could not be expected. Thus, any reliance on this standard should be carefully considered and limited to contexts where it is relevant and helpful.

Conclusion

Thank you for the opportunity to submit these comments and for considering them. If you would like to discuss any of our comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.

[14] *See* Comments by the Centre for Information Policy Leadership on the Office of the Privacy Commissioner of Canada's Reframed Consultation on Transfers for Processing at note 3 above.