The Honorable Daniel Therrien
Privacy Commissioner of Canada
Office of the Privacy Commissioner

Dear Mr. Therrien,

The American Chamber of Commerce in Canada (AmCham Canada) welcomes the opportunity to comment on your office's consultations on cross-border data flows under the *Personal Information Protection & Electronic Documents Act* (PIPEDA).

AmCham Canada is directly affiliated with U.S. Chamber of Commerce, the world's largest business federation, representing the interests of more than three million firms of all sizes and sectors. In Canada, our members are major employers and significant investors who contribute to a bilateral economic relationship of unrivalled breadth and depth. In 2018 alone, U.S. goods and services trade with Canada stood at $714 billion, while, in 2017, U.S. foreign direct investment in Canada exceeded $390 billion. The digital economy touches on or encompasses all aspects of this bilateral trade and investment partnership, from information technology and manufacturing to defense, healthcare, and financial services. Consequently, the free flow of data between Canada and the United States is a foundational matter, as the transfer and processing of data is essential for the continued growth and competitiveness of our two economies.

AmCham Canada therefore voices our serious concern about the Office of the Privacy Commissioner's ("OPC") proposals, which may impose consent requirements on companies processing data outside of Canada. Put simply, such a requirement would impede the flow of data across borders and cause great harm to Canadian and U.S. businesses. For many global businesses operating Canada, any such proposal will serve as a data localization requirement, as they may be unable to obtain consent from all Canadian employees, contractors, and customers needed to transfer their data outside of Canada.

AmCham Canada shares the OPC's aim of promoting effective data privacy protections for Canadians. The continued success of the U.S.-Canadian digital

economy, however, requires governments on both sides of the border to uphold their trade obligations and pursue a stable, interoperable regulatory environment. The OPC's proposal runs counter to both of these imperatives. As described in further detail below, placing such a restriction on cross-border transfers of data runs counter to Canada's obligations under the United States-Mexico-Canada Agreement ("USMCA"), which generally prohibits the participating nations from restricting the flow of personal information between one another.[1]

AmCham Canada requests that the OPC refrain from further action on this issue, unless otherwise directed by the Canadian Parliament. We firmly believe that fundamental changes to PIPEDA and the Canadian privacy regime, such as those contemplated by the OPC, should be left to Canada's elected representatives. The upcoming federal elections in October, together with the proposed ratification of USMCA, only underscores the need for the OPC's restraint, as further action by your office may preempt the legislative process. We have outlined detailed comments below.

The Proposal will Disrupt U.S. & Canadian Businesses

In its past and current consultations, the OPC has proposed to reinterpret PIPEDA in a manner that would require companies to obtain consent from data subjects before transferring data outside of Canada for processing. The proposal will affect nearly all cross-border business that relies on the flow of data to and from Canada, in sectors ranging from information technology, agriculture, and manufacturing to healthcare, defense, and financial services.

If enacted, this proposal will cause serious disruption to Canadian and U.S. firms. The measure will create a de facto data localization requirement in Canada, as global companies will find it difficult to obtain consent from all Canadian employees, contractors, and customers. Consequently, many companies may reluctantly withdraw their operations from the Canadian market, negatively impacting consumer expectations and brand engagement for both Canadian consumers and businesses. Such a requirement would also limit the access of Canadian businesses , including to U.S.-based cloud computing infrastructure. The proposal will also disrupt existing Canadian and U.S. businesses who may have infrastructure and business processes established across the border and who do not segregate customers and employee information by country.

As well, the OPC should consider the impact these guidelines will have on the services available to Canadian businesses. By reducing the choice of providers

[1] See the U.S.-Mexico-Canada Agreement, Article 19.11

operating in Canada, the proposal will diminish competition, resulting in higher prices for cloud computing services and reduced choice and innovation in the Canadian market.

The Proposal will Not Advance Canadian Privacy Protections

AmCham Canada agrees with the OPC about the importance of promoting effective privacy protections in the context of cross-border data flows. Our parent, the U.S. Chamber has been a leader on data privacy matters both in the United States and internationally and has promulgated principles that balance robust privacy protections with the need for innovation.[2] What remains unclear is how the OPC's consent requirement will enhance individual privacy protections.

As the OPC acknowledges in its most recent consultation, organizations will still be subject to the accountability principle under PIPEDA if the change to its guidelines are enacted. A consent requirement adds nothing to these standards, as data privacy and security protections are not based on location, but on the underlying infrastructure and administrative and technical safeguards being implemented by organizations. Moreover, a consent requirement will burden end-users with confusing information, obscuring relevant information about how personal data is used and imparting a false sense of security. The OPC's proposal will arguably reduce the privacy protections of Canadian citizens, as state-of-the-art cybersecurity practices entail aggregating and analyzing data from across different markets to protect networks.

Considerations for any Future Privacy Law or PIPEDA Amendments

As Canada considers long-term amendments to PIPEDA or the consideration of a new privacy law, we encourage consideration of the following principles that will enhance personal data protection, further the trust relationship between companies and their customers, and enable innovation while also avoiding regulatory fragmentation that undermines all three goals.

Individuals should have the right to exercise control over the use of their personal data where reasonable to the context surrounding the use of personal data. These individual control rights, consistent with the rights and legal obligations of other stakeholders, include the right to access, correct, port, delete, consent, and object to the use of personal data about themselves.

---

[2] U.S. Chamber of Commerce Privacy Principles.

Sensitive Data: Individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, unless such use is necessary based on the context or otherwise permitted under applicable law.

Access, Objection, Correction, Deletion, and Portability Controls: Subject to the context considerations of the following subsection, where reasonable, individuals should have the right to the following:

- be informed about the categories of companies who are collecting their personal data and how they are using it;
- access in a timely manner personal data collected from them;
- object to the use of their personal data
- rectify, complete, or delete inaccurate or incomplete personal data;
- have an entity delete their personal data; and
- obtain and port personal data that they provided to the entity across different services.

Enabling Context-Based Individual Control: While individual control mechanisms may differ in design features and deployment, and may also evolve over time, they should always provide individuals with reasonable transparency and the means to exercise the rights laid out above to the extent they are appropriate to the context surrounding the use of that personal data.

Key considerations in determining the appropriate level and means of enabling individuals to exercise control over the use of their personal data in a particular context should include, but are not limited to:

- extent, frequency, nature, and history of interactions between individuals and an entity, if any, and whether the personal data being used is inferred;
- expectations of reasonable users about how an entity uses their personal data, including through any notice it provided;
- extent to which personal data is exposed to public view;
- extent to which personal data is pseudonymized and the probability and ease of reversing that pseudonymization for any given entity that has access to such data;
- practical difficulty or infeasibility of accessing or deleting data from backup systems or archives, or segregating the individual's personal data from others in order to enable access;
- benefits to individuals and society of a certain use of personal data;

- types of personal data that need to be used for an entity's customary internal operations;
- age and sophistication of individuals to whom an entity targets or markets its goods or services, including whether it is directed toward minors or the elderly;
- sensitivity of the personal data being used;
- reasonably discernible potential privacy risks of an entity's planned use of personal data; or
- extent to which personal data is processed to protect the vital interest of the individual or necessary for the performance of a task carried out in the interest of public safety, for law enforcement purposes, or in the exercise of the official authority vested in the controller entity.

General organizational accountability for data protection should be the foundation to ensuring consumers data is processed in accordance with consumer expectations. This includes where data is being transferred between the same entity across borders, or between entities across borders. The requirements for an accountable data protection program may vary depending on the organization but may include aspects like an independent office of data protection, impact assessments on processing activities (including data transfers where appropriate) that may be made available to regulators upon request/investigation, contractual safeguards, transparency to consumers about what data is being collected, how it is used, and when it is shared. A flexible view of accountability is necessary to ensure that small and medium size enterprises that process and transfer data across borders do not need to take on additional compliance obligations beyond what is proportional given the consumers, the types of data, and the processing activities.

We believe that ensuring organizational accountability (see above for non-exhaustive examples of elements for organizational accountability) can effectively protect consumer data privacy by placing the onus on organizations to ensure they are considering the impacts on consumers of data transfers both within and outside the organization and holding the organizations accountable where harm occurs by virtue of a transfer and where reasonable precautions to protect consumer data were not taken.

The Aim of the OPC's Consultations Is Unclear

While AmCham Canada thanks the OPC for its efforts to refine its consultations, what remains unclear in the original, supplementary, and reframed documents is

whether the OPC is reacting to specific inadequacies in the Canadian accountability-based privacy regime that has been in place under PIPEDA.

The consultation documents reference the OPC's investigation of the Equifax data breach, but do not elucidate how this represents a failure of organizational accountability beyond the circumstances applicable to the findings from the investigation. Instead, the OPC has put forward a reinterpretation of PIPEDA to justify the imposition of a consent requirement on cross-border data transfers, conflating the act of "transferring" data with the "disclosure of information." Yet two different terms were used in the law. If the Parliament of Canada had wanted to require consent for such a transfer, it would have chosen not to use the term "transfer" in the legislation in the context of third-party processors and would have used instead the word "disclosure".

Contrary to the OPC's consultation, the AmCham Canada believes Parliament was clear when drafting PIPEDA. As per s.5 (3), consent is required for the collection, use and disclosure of personal information for a purpose that a reasonable person would consider appropriate.[3] Once consent has been obtained for a certain collection and use, organizations are free to process the data collected to satisfy that purpose, whether the processing occurs in-house through its own personnel and equipment or through third party processors. Third party processors are not data controllers of their own rights, but rather merely act on behalf of and as per the instructions of the parties that have hired them to perform certain functions. As a result, legally, the operation of s.5(3) and of principle 4.1.3. of Schedule 1 of PIPEDA confirm that making personal information available to a third party for the sole purpose of processing is not a disclosure—but rather an activity that supports the use for which consent was obtained—and for which the transferring organization remains accountable. We add that, if the OPC perceives PIPEDA to be deficient, it should clarify the specific deficiencies in the current regime and how a consent requirement would advance effective privacy protections.

The OPC correctly recognizes that, by issuing its *Digital Charter* and its whitepaper on *Strengthening Privacy for the Digital Age*, the Government of Canada will review the status of the Canadian privacy regime and determine whether any updates to PIPEDA are needed. Yet the OPC has chosen to move forward with its consultation, noting that "legislative changes could take years." **While the OPC is an independent Agent of Parliament, given the impact its proposal will have on cross-border business and investment activity, we firmly believe that such fundamental questions regarding PIPEDA should be left to Canada's elected representatives**.

[3] Personal Information Protection & Electronic Documents Act

The Canadian Government and the Canadian Parliament are best suited for weighing the high-stakes and various interests represented in this matter. Any action to continue beyond this consultation will exacerbate uncertainty in the business community.

The Proposal is Inconsistent with Canada's Trade Obligations

As a global leader in the digital economy and as an active supporter of open digital markets, the Government of Canada has recently undertaken trade obligations to uphold the free flow of data across borders. It made these obligations under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the new U.S.-Mexico-Canada Agreement (USMCA). The OPC's proposal is inconsistent with both the spirit and the letter of these agreements.

Under the CPTPP, Canada has agreed to not impose restrictions on transfers of data greater than is required to achieve a legitimate public policy objective. The protection of personal information is a legitimate public policy objective. As indicated above, though, the OPC's proposal to require consent for cross-border transfers for processing does not enhance data privacy protections, and thus violates this commitment. Similarly, Canada had agreed to promote mechanisms that encourage compatibility between different privacy regimes. The OPC's proposals run counter to this commitment.[4] While the U.S. is not party to CPTPP, many Chamber members engage in cross-border trade between Canada and other CPTPP parties, thereby benefiting from the regulatory stability the agreement is meant to confer.

Canada has agreed to more substantial commitments in the new USMCA.[5] According to Article 19.11, no party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means. While parties may adopt measures inconsistent with this commitment if it is necessary to achieve a legitimate public policy objective, the measure: 1) must not be applied in a manner that would constitute an arbitrary or unjustifiable discrimination or a disguised restriction on trade; 2) should not impose restrictions on transfers of information greater than are necessary to achieve the objective. As stated earlier, personal data that is transferred from Canada to the United States will continue to be protected by the same accountability measures, regardless of whether or not consent is obtained. It is therefore unlikely that the OPC's measure meets the standard set by the USMCA.

The USMCA further requires the Canadian privacy framework to consider principles and guidelines of relevant international bodies, such as the *APEC Privacy*

[4] Comprehensive & Progressive Agreement for Trans-Pacific Partnership, Article 14.8 and 14.11

[5] See United States-Canada-Mexico Agreement, Chapters 17 and 19

Framework and the *OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal.* Canada is a part of APEC, has helped develop and endorsed the *APEC Privacy Framework* ("Framework"), and has helped develop and joined the APEC Cross-Border Privacy Rules ("CBPR") system. The CBPRs do not provide for choice or individual consent with respect to cross-border data transfers. Such an option would be inconsistent with the APEC Framework and the CBPR's premise of providing accountability-based protections to the information regardless of geographic location. The OECD Recommendations similarly bolster the accountability approach to transborder data flows. As stated in Article 19.8, any restriction on cross-border flows of personal information are necessary and proportionate to the risks presented. The OPC has made no indication that its measures are informed by a risk-based understanding.

Global Harmonization and Regulatory Consistency

Policymakers should avoid measures that impede the global interoperability of data protection and privacy models, such as prohibitions on the transfer of personal data abroad and the extraterritorial application of privacy/data protection measures.

Regulations for cross-border data transfers should be technology and industry neutral and ensure interoperability between regional legal regimes. We favor outcome-oriented frameworks that ensure consumer rights are respected while utilizing recognized security standards (e.g., ISO and others) to safe guard consumer data during cross-border transfers.

A Consent Requirement is Inconsistent with Other Data Transfer Norms

The OPC's proposal is at odds with other international norms and not only those set by APEC and the OECD. Most prominently, the proposal runs counter to the European Union's General Data Protection Regulation ("GDPR"). The GDPR treats consent as one of many avenues for international data flows, including binding corporate rules, standard contractual clauses, and approved certification mechanisms. Binding corporate rules, in particular, require that the security and confidentiality of all proprietary information and data, including personal data, are safeguarded in accordance with applicable laws and regulations. Accountability mechanisms such as BCRs are the most effective means of protecting personal data across border.

Under the GDPR, consent is only one derogation from these mechanisms, rather than an overriding requirement imposed on cross-border transfers. Legitimate business interest is recognized under the GDPR and is the most efficient and practical means of ensuring that personal data is collected and used appropriately. Consent by a citizen can be revoked easily or arbitrarily and undermines many business models that rely on the collection of data from a customer.

Consent Requires Reasonable Context and Clear Guidance

International data transfers and meaningful privacy protection are not mutually exclusive or antagonistic goals. The collection, use and disclosure of personal data by organizations should be done in a manner that recognizes both the right of individuals to make informed decisions concerning their personal data and the need in many cases of organizations to collect, use or disclose it. We understand and respect the OPC's position that individuals should have increased say in whether and how their personal data is used, transferred, and stored. However, sole reliance on consent will not necessarily provide individuals with this control or knowledge, and it can severely limit the ability of Canadian consumers and companies to access innovative digital services. "Notice fatigue" makes consent requirements less effective, rather than more impactful, as individuals are faced with a pop up or privacy policy to click through each time they access a website, making them less – not more – likely to read through and take seriously the information provided. It also may obscure more relevant issues about how their data is used and provide a false sense of security to end-users their data is more secured as cyberattacks are not based on geographical location but the underlying infrastructure.

Similarly, this policy may impact Canada's ability to remain globally competitive by leveraging cloud computing and other services available outside Canada. New, innovative services often don't have the ability to use data centers in every market where they work, or they provide services based around data processing at a certain location. It may also prevent Canadian individuals or businesses from using the most cost-efficient services, and limiting where those activities can take place may reduce choice or increase cost for consumers. Furthermore, many multinational companies do not separate customer information between their affiliates by country, making compliance with such a policy more difficult.

Consent is just one important mechanism that can help balance these rights, but it should not be the sole basis for managing data processing activity. Effective, meaningful consent is sensitive to context. For example, the OPC's 2018 *Guidelines on Meaningful Consent* acknowledge that, "Consent should remain central, but it is necessary to breathe life into the ways in which it is obtained." Factors such as the sensitivity of data, the risk to the person from its use and the relative value generated by its processing should

all factor in the calculation of which type of consent would be most reasonable. Therefore, it should not always be necessary to rely on specific consent; instead, consent should be given in an informed and unequivocal way, thereby balancing the protection of personal data and innovation.

While consent has traditionally been an important mechanism of individual protection, as it seeks to empower data subjects to make informed decisions about whether and how their data can be used, it has practical limits. With the rise of innovations that rely on cloud computing, big data and the Internet of Things (IoT), relying exclusively on notice and consent mechanisms as the primary means for legitimizing data collection is no longer practicable. In the absence of an interface or a direct relationship with the data subject, obtaining consent is often impossible in practice. Further, identifying the legal grounds for processing data provides more certainty for data controllers so they can comply more easily and effectively with the law. PIPEDA has upheld some key concepts and values that are critical to citizens on a range of important topics and rights. However, in order to realize and achieve the positive objectives of the consent rules, further clarity and guidance on obligations and scope are needed.

Fair and Flexible Accountability and Data Transfer Mechanism

A system where several mechanisms for data transfer are equally available would provide a much greater level of confidence amongst the different actors. The accountability model, upon which Canada's privacy laws are already largely based, already provides an approach to cross-border data governance that effectively provides the individual with protections and fosters streamlined, robust international data flows. This accountability model requires that the organizations that collect the data are responsible for its protection no matter where or by whom it is processed, as they do not relinquish control of the information. It also requires that organizations transferring data must take appropriate steps to be sure that any obligations – in law, guidance or commitments made in privacy policies – will be met.

We also believe that Individuals should be informed about the collection and use of their personal data in a fashion that is meaningful, clear, conspicuous, and useful to the individual. Such notices should be informed by state- of-the-art practices on effective disclosure, and include information regarding:

- the types of personal data collected;
- the entity that is collecting their personal data;
- how the personal data will be used;

- whether and for what purposes personal data may be accessed by or transferred to third parties and the types or categories of third parties to whom such data may be transferred; and
- an explanation of control, choice, and redress mechanisms available to individuals.

A range of instruments exist that can serve as the foundation of a robust and implementable data transfer model while flexible mechanisms should be allowed to facilitate cross border data transfers, including commercial contractual terms and industry codes and conduct. These instruments include model clauses, the EU binding corporate rules (BCRs), certifications, independent seals, and multilateral frameworks such as the APEC cross border privacy rules (CBPRs) – to which Canada is already a party – consent, and other available mechanisms or exceptions. Under the CBPR system, the principle of "accountability" makes the original data collector legally "responsible" for data by making sure the obligations of the data controller follow the data as it crosses borders. On model clauses, it provides another straightforward and low-burden way for organizations to comply with their obligations to protect personal data as they transfer it across borders. Canada should therefore seek to preserve multiple approaches to cross-border data transfers without weakening privacy safeguards.

Conclusion

The American Chamber of Commerce in Canada thanks the OPC for the opportunity to provide these comments. The American private sector has a long history of trade with and investment in Canada and is proud of its continued contributions to the vibrant U.S.-Canadian relationship. We stand ready to serve as open partners to the Government of Canada, Parliament, and to the OPC as you review the status of the Canadian privacy regime. We look forward to continuing the dialogue on this and other issues that are foundational to the digital economy.