August 6, 2019

Daniel Therrien
Commissioner
Office of the Privacy Commissioner
of Canada
30, Victoria Street
Gatineau, Quebec
K1A 1H3
Via email OPC-CPVPconsult2@priv.gc.ca

RE: Canadian Chamber of Commerce Submission to OPC *Consultation on transfers for processing – Reframed discussion document*

Dear M. Therrien,

Thank you for the opportunity to comment on enforcement guidance proposed by the Office of the Privacy Commissioner ("**OPC**") as it pertains to consent requirements for the transfer of personal information to third parties, whether domestic or trans-border, for processing. The Canadian Chamber of Commerce ("**Chamber**") is the voice of business in Canada, representing over 200,000 businesses through the Canadian Chamber Network.

Global data flows underpin global value chains, creating new opportunities for participation. The majority of Canadian businesses are small to medium size enterprises and are substantial contributors to employment and GDP. Small and medium sized enterprises have been able to harness digital platforms to export goods and provide services which can be purchased and consumed online, enabling these smaller businesses to reach customers globally at a pace and scale that was not possible a decade ago. Access to digital inputs such as cloud computing provides on-demand access to computing power and software that was previously reserved for large companies. Digital services can be used to reduce fixed information technology costs and increase business competitiveness.

Reasonable Expectations of Customers:
The business community values its customers. Without customers, there is no business ecosystem. Violating customer trust and loyalty by stepping outside of what customers expect will inevitably harm the relationship between a business and its customers; there is a built-in, self-regulating motivation that drives responsible corporate behavior. All of a company's actions must be viewed through the eyes of

its customers to ensure actions meet expectations. Customers respect and value a company that provides them with consistent and good experiences. These actions earn and build customer trust.

Customers are busy and want convenience.[1] Convenience includes customers having the ability to choose how to interact with companies in a way that best fits their needs. This includes companies offering a variety of communications and payment (electronic) options.[2] Customers want to interact with companies across channels.[3] Almost half of Canadians purchase goods and services from their mobile devices, and most Canadians shop online. [4] Most Canadians expect companies to be transparent about how they collect and use information.[5]

Amidst the negative publicity surrounding major breaches of security safeguards, industry has responded with changes in practice and is guided by organizing principles and codes of practice, like the International Chamber of Commerce (ICC) *Advertising and Marketing Communications Code*. Industry has also evolved its response to data breaches, implementing new protocols for cyber security and sharing cyber threat information through organizations like CCTX as a means to improving on meeting customer expectations.

The view of our members is that the accountability principle already makes organizations liable when they transfer information and this this principle is robust within Canada's *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***"). Under *PIPEDA*, organizations are accountable for protecting the privacy and personal information under its control of Canadians when such information is collected, used or disclosed. There are strict limits to such data collection, use and disclosure. Companies must consider the impact on individuals and the sensitivity of their data. They must be transparent with those whose data they process. When information is transferred for processing on behalf of an organization for its own purposes, it is not disclosed. In fact, often that information is encrypted and not legible by a third party processor in a meaningful way. Disclosing information means that control of personal information no longer resides with the organization that collected it.

---

[1] *The Blended Commerce Imperative: Insights on Today's Consumer with Advice and Tips for Retailers* (Whitepaper). December 2018. Retail Council of Canada: https://www.retailcouncil.org/research/understanding-the-canadian-consumer-2018/, page 9.

[2] *2017 Canadian Payment Methods and Trends*: *Payments Canada Discussion Paper No. 8*. December 2017. Payments Canada: https://www.payments.ca/sites/default/files/14-Dec-17/paymentscanada_trendsreport2017_final.pdf, page 8.

[3] *Delivering for the New Consumer: The Move to Ubiquitous & Ultra-Personal Shopping*. September 6, 2018. Accenture: https://www.accenture.com/_acnmedia/PDF-85/Accenture-Report-The-Changing-Consumer-And-The-New-Definition-of-Retail.pdf

[4] *2019 Canada's Internet Factbook*. CIRA: https://cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019.

[5] *Ibid*.

Response to OPC Questions on Future Law:
Members of the Canadian Chamber have given considerable thought to future of data governance, the opportunity for Canada to emerge as a knowledge center, and the compatibility of Canada's existing privacy framework with that of other countries as it goes forward in a digital world. Please refer to the following policy papers as a statement of the Chamber's position on the future of data and privacy in Canada:

Data for Good: The $32-billion Boost (October 2018)

A Data Deficit: The Risk of Getting It Wrong (December 2018)

Data Fast Forward: A Prescription for Innovation, Balance and Trust (January 2019)

Automation Not Domination: AI and Inclusion (June 2019)

Automation Not Domination: Legal and Regulatory Frameworks for AI (June 2019)

Automation Not Domination: AI and the Workforce (June 2019)

Please be also advised that the Canadian Chamber will be responding to the consultation issued by Innovation, Science and Economic Development ("**ISED**") on Canada's Digital Charter, which will cover the questions posed in this consultation. A copy of the Chamber's submission to ISED on the Digital Charter will be forwarded to the OPC.

Response to the OPC's Revised Legal Interpretation of Data Transfers:
With respect to the question of the application of consent to the transfer of data to third parties for processing, we note the OPC consultation document references the dictionary definition of the word "disclose". We underline that the terms "disclosure" and "transfer" are separate and distinct:

> **"Disclosure"** in the privacy context is the action of making personal information known to a third party in a way that provides the third party with control over that information.
> **"Transfer"** by contrast, is an act of moving personal information to another organization for a specific purpose and under strict controls.

The Parliament of Canada's intent was clear when it adopted *PIPEDA*. It used different terms to refer to the sharing of personal information between entities: "disclosure" and "transfer." *PIPEDA* requires consent for disclosure to another organization for the latter's own purposes, unless an exception applies. *PIPEDA* does not, however, require consent for the transfer of personal information to a third party for processing. If Parliament had wanted to require consent for transfers to third parties for processing, it would have chosen not to use the term "transfer" in the law instead it would have used "disclosure".

If Parliament had wanted to fundamentally change long-standing commercial practices as they pertain to outsourcing by requiring "data controller" organizations to obtain an individual's consent before a third party could process personal information on the controller's behalf, it would have not only made it clear in *PIPEDA*, but there would have been considerable consultation and debates over

the issue. There have been no such debates. As noted in ISED's white paper on PIPEDA reform, sharing information as part of a business practice (processing) doesn't require consent.[6]

PIPEDA does not contain any prohibitions or restrictions on data transfers. In addition, it does not prohibit outsourcing or the use of service providers who transfer information outside Canadian borders, rather it specifically enables transfers to third parties for processing under specific circumstances without consent. The Accountability principle in Schedule 1 obliges organizations to ensure adequate provisions are in place for a comparable level of protection.

> **PIPEDA Schedule 1 Section 5 Clause 4.3.1 Accountability**
> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

The distinction between transfer and disclosure are confirmed in the following decisions issued by previous Privacy Commissioners as precedent:

> In PIPEDA Case Summary #2008-394, CanWest, an email service provider notified customers that it was transferring its processing services to a company in the US. Complainants argued that transferring personal data to a US service provider put that information beyond the control of PIPEDA and subject to US law, therefore violating *PIPEDA*. The OPC determined, as in previous findings, that the sharing of information with a third-party service provider constitutes a "use" for the purposes of the Act. The OPC also found that CanWest had maintained custody and control of the information that was processed by its third-party service provider in the U.S. The service agreement between the two parties relied on unambiguous language that provided guarantees of the confidentiality and security of personal information, and it allowed for oversight, monitoring and audit of the services being provided. The contractual provisions with regard to information protection were no less stringent than if the service provider had been located within Canadian borders.
>
> In PIPEDA Case Summary #2007-365 Society for Worldwide Interbank Financial Telecommunication (SWIFT), which involved the disclosure of personal banking information from the customers of 6 Canadian financial institutions to US authorities as a result of a subpoena. In this case, the OPC confirmed that the exceptions to consent permitted under section 7(3)(c) and 7(3)(c.1) of *PIPEDA* were valid and that the contractual arrangements met the requirements of 4.3.1 of Schedule 1 and further acknowledged that *PIPEDA* could not prevent the disclosure of personal data to authorities as a response to a legal obligation.
>
> In PIPEDA Case Summary #2005-313, where CIBC customers complained about an amendment to Visa cardholder agreements, indicating that personal information would be processed in the US

[6] Strengthening Privacy for the Digital Age, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

and could potentially be accessed by US law enforcement agencies. The OPC determined that, while anti-terrorism measures and outsourcing are a continuing public debate, CIBC had met its obligations under PIPEDA.

Members of the Canadian Chamber urge the OPC to acknowledge that the 2009 OPC Guidelines are accurate. The "Processing Personal Data Across Borders" guidelines issued in January 2009 were based on the actual letter of *PIPEDA*, as passed by the Canadian Parliament. The 2009 Guidelines have actually formalized business practices and the common understanding by all parties that goes back to the development of the CSA Model Code, parliamentary debate and since PIPEDA's coming into force.

Since the law has not changed with respect to disclosure, transfer and organizational accountability since its passing, we conclude it is unreasonable to posit that a new, unnecessary and unsubstantiated interpretation of the law can now be advanced. We further note that the courts have not interpreted the provisions at issue differently, nor has any order been issued for the language of *PIPEDA* to be reconsidered.

Our members conclude that consent is not required to transfer personal information to a third party for processing and therefore, questions posed in the consultation about consent to transfer data are not relevant. The "data controller" is (and remains) accountable for the data it collects and must ensure sufficient contractual controls and other vendor management controls are in place with third party processors to protect the integrity of personal information.

Consent is not required under *PIPEDA* for every single data processing activity that an organization undertakes, and organizations remain free to manage their internal operations as they wish (e.g. storage, archival, transmission). Under *PIPEDA*, consent is required for collection, use and disclosure. Transferring personal information to a service provider is a mere processing activity, like storage.

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. 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. Therefore, transfers do not require consent.

The OPC's new interpretation of PIPEDA would impede the ability of business both small and large to engage new cloud computing services due to the risk of data loss and would also limit competition in the marketplace for cloud services. It would also inhibit the ability to actually increase security of data by limiting the use of service providers with better security practices and solutions. Organizations should

remain free to manage their internal operations as they wish, including relying on third party data processors (subject to appropriate due diligence and contract clauses).

Not to be lost in this discussion is the gap between enforcement of OPC's new interpretation and the expectation of changes to *PIPEDA* post-election 2019, where all political parties have signaled an intent to address how personal information is handled in the digital age. There is a massive administrative cost to business in adopting a new approach to consent where it was previously not required, – and this will be compounded if businesses are expected to align with the OPC's new interpretation now, with alignment with a Digital Charter or similar near-term change in PIPEDA post-election 2019. It is unreasonable to impose new, untested requirements on business for a law that is currently under review (and that, post-election 2019 is expected to be amended or replaced). It is unreasonable to impose new, untested requirements on business for a law that has not been amended to require consent for transfers and that is likely to be reviewed in short order.

Canada as an Outlier

Should the OPC proceed and enforce based on the interpretation of transfer as a disclosure as proposed in this consultation, Canada would be a global outlier. No other jurisdiction in the world requires organizations to give individuals choice as it pertains to whether their personal information can be processed by a third party service provider domestically. No other jurisdiction in the world requires private sector organizations to give individuals choice as to whether their personal information can be processed outside of the country of collection - not even the General Data Protection Regulation (GDPR).

Substantially similar laws do not have this provision. For example, most health privacy laws, including those deemed "substantially similar" to *PIPEDA* such as Ontario's Personal Health Information Protection Act (*PHIPA*), explicitly treat the sharing of information with an agent or service provider as a "use" of information by the custodian, rather than a "disclosure" to a third party that would require additional consent.

Currently, the Alberta *Personal Information Protection Act* (*PIPA*) is the only private sector privacy regime of general application (albeit some provinces such as BC have restrictions around specific personal information like health care data) that contains any statutory requirements regarding the transfer of personal information outside of Canada. Under *PIPA*, an organization that intends to transfer personal information outside of Canada for processing (i.e. outsourcing) must previously have provided notice to individuals of its policy and procedures addressing such transfer as well as contact information of its representative who can respond to questions regarding such activities. Although not expressly stated, the *PIPA* provision should be read to require as well, notice to such individuals that the organization may make such transfers. PIPA, for instance, is quite clear that if the control of data remains with the organization that collected it, any transfer of data outside the province for processing is incidental and PIPA still applies. Should the OPC adopt the opposite interpretation with respect to *PIPEDA*, organizations may find themselves subject to conflicting rules and obligations.

Adverse practical consequences

As a matter of practice, based on long standing guidance and legal precedent, organizations currently are not obligated to permit individuals to determine whether their personal information can be processed by third parties domestically or abroad. Requiring individuals to consent to the use of service providers for processing data will result in the following consequences:

1. Reclassifying the transfer of personal information to affiliates or third party vendors as "disclosures" is a waste of resources
2. Providing alternatives that would allow the customer to continue receiving services without transferring data internationally is often not commercially feasible.
3. Interpreting PIPEDA in a way obligates new consent requirements when no legislative amendments to the former have yet been proposed is not in compliance with the Canadian legislative system.
4. Irritate consumers by the myriad new pop-up notices that will appear every time individuals interact with an organization that transfers personal information for processing purposes, resulting in user fatigue.
5. Disadvantage Canada's business as compared to the rest of the world.

Ultimately, the interpretation of data transfer as a disclosure would have a chilling impact on business climate. It would be extremely challenging for members to implement data transfer consent requirements in a way that satisfies the Meaningful Consent Guidelines and s. 6.1 of PIPEDA. It would require companies to prepare and provide a myriad of notices (and choice options) to customers relating to a large number of third party providers (domestic and foreign) used in companies' distribution chain (e.g., customized product producers, last mile couriers, cloud storage providers, email management companies, customer service). Organizations would be required to set out in granular detail each of their identities and the reasons they process personal information, which contradicts the goal of providing simple transparency to individuals.

Organizations must then regularly review and update the above notices when relationships with third party providers change, or when companies onboard new third party providers and determine whether a new express consent is required. Finally, organizations must design, develop and implement new consent management frameworks for transfers to processors, so that organizations could respond to requests from individuals to withdraw their consent (and re-consent) to certain service provider arrangements.

In lieu of obtaining customer consent for transfers of personal information to service providers, whether in or outside of Canada, many organizations may choose to move all personal information processing in-house. This cost does not include the people, time or other resources necessary to manage these functions, including protecting customer information, once they are brought in house.

Accountability as an Effective Means of Protecting Privacy

Accountability is the practical way organizations protect customer privacy. Organizations largely engage third party providers when they do not have the expertise or resources to perform certain functions in-house. Transferring personal information to providers can better secure and protect customer information. For example, cloud-computing providers have security specialists on-hand that actively monitor for security gaps and potential threats. They can mitigate risks to customer personal information faster than a company that does not specialize in cloud computing. Organizations also engage third party providers who are compliance specialists. For example, digital marketing companies have anti-spam experts that can help companies navigate the complexities of CASL thereby ensuring company email programs are compliant with law. Businesses specializing in emerging technologies like data analytics, machine learning and artificial intelligence are better at de-identifying personal information in data sets for use in modelling. These subject matter experts can better ensure that information from data sets, compiled with other data, will not re-identify an individual.

It is important to note that our member organizations are committed to protecting privacy and complying with PIPEDA. In the absence of clear direction from the OPC on how to comply with this new directive, companies are at a risk of wasting resources in determining how to navigate their compliance programs following Equifax and in light of potential legislative change from the federal government.

A Violation of Canada's Trade Commitments

The Comprehensive and Progressive Trade Agreement for Trans-Pacific Partnership (CPTPP), the major Asia-based trade agreement that Canada implemented last year requires Canada to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business" of the company. CPTPP allows Canada to adopt measures to achieve a legitimate policy objective, as long as such measures do not result in arbitrary or unjustifiable discrimination, or a disguised restriction on trade. Moreover, any limits on cross-border data transmissions cannot be greater than necessary to achieve a legitimate policy objective. The Canada-U.S.-Mexico Agreement (also known as USMCA) contains similar language, and further requires that any restriction on cross-border data flows should be "necessary and proportionate to the risks presented."

The imposition of consent requirements for cross-border data transfers would likely be regarded as a non-tariff barrier to trade that imposes restrictions greater than those required to achieve the objective of privacy protection. The interpretation is particularly vulnerable given that *PIPEDA* has long been said to provide such protections without the need for this additional consent regime. There is no reason for this change in interpretation, nor any corresponding benefit for individuals. Our members believe that Canadians would expect that in this interconnected world, their personal information flows across the globe, contrary to the argument made by the OPC.

Furthermore, both the CPTPP and the USMCA require that, in adopting measures to protect the personal information of the users of electronic commerce and digital trade, Canada "should take into account principles and guidelines of relevant international bodies." The USMCA refers to two guidelines, the

APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), neither of which recommend a consent requirement similar to what OPC is proposing. We are not aware of any other international guidelines that do so either.

Finally, a special consent requirement with respect to the cross-border transfer of information may not only be highly disruptive to international trade, but it may have a disproportionate and discriminatory impact on foreign service suppliers, and thereby undermine or run afoul of Canada's WTO and free trade agreement commitments on trade in services. We also note that, under the USMCA, restrictions on the cross-border transmission of information are not permissible if they "accord[ ] different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party." The OPC's proposal could have just such an impact.

In conclusion we would note that the rest of the world is adopting data protection regimes that emphasize accountability. While consent remains an important aspect of accountability and the protection of privacy, it is not the only aspect and that there are better and more practical ways to protect individual privacy. In our view, this new approach to data transfers has such broad policy implications that this matter should be left to Parliament to decide.

Thank you again for the opportunity to comment on this consultation.

Best regards,

Scott Smith,
Senior Director Innovation and Intellectual Property Policy
Canadian Chamber of Commerce

Cc: Mark Schaan, Director General, Marketplace Framework Policy Branch, Innovation, Science and Economic Development Canada