Osler, Hoskin & Harcourt LLP
Suite 1900, 340 Albert Street
Ottawa, Ontario, Canada K1R 7Y6
613.235.7234 MAIN
613.235.2867 FACSIMILE

OSLER

Ottawa
Toronto
Montréal
Calgary
Vancouver
New York

August 6, 2019

Office of the Privacy Commissioner of Canada
30 Rue Victoria
Gatineau QC J8X 4H7

Attention: Daniel Therrien, Privacy Commissioner of Canada

Re: OPC Consultations on Transborder Dataflows

Dear Commissioner:

Thank you for the opportunity to provide comments in the context of your Office's consultations on your proposed change of position regarding transfers of data for processing under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**").[1]

This submission is made on behalf of AccessPrivacy, by *Osler*, informed by the many stakeholder comments received during the half-day workshop we held specifically on this topic on April 26th, attended by over 90 business representatives (Chief Privacy Officers, Senior Counsel and privacy professionals) across multiple industry sectors. In addition, our submissions are informed by the many client queries, concerns, and questions we have received since the launch of the initial consultations on April 9th, the Supplementary discussion document of April 23, 2019 and the Reframed discussion document of June 11, 2019. By relaying these comments, we hope you will find them useful and informative background for your deliberations.

The primary focus of this submission is on the legal and policy reasons why we respectfully disagree with the Office of the Privacy Commissioner of Canada ("**OPC**")'s proposed change of policy position that would require consent for transfers of personal information for processing. In our view, the OPC's *Guidelines on Personal Data Across Borders* ("**2009 Guidelines**")[2] encapsulate the correct statutory interpretation of PIPEDA and should be maintained.

Our submission is intended to respond to the questions you ask in your Reframed discussion document with respect to the proper interpretation of PIPEDA as it currently

---

1 *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [PIPEDA].

2 "Guidelines for processing personal data across borders" (27 January 2009), online: *Office of the Privacy Commissioner of Canada*, www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

stands. As for the additional questions regarding how PIPEDA could be amended to deal more effectively with data transfers for processing in the future, we will be considering these as part of our submission to Innovation, Science and Economic Development (ISED) in the context of its broader proposals for PIPEDA reform[3] and would be pleased to provide you with a copy of our submission to ISED at that time.

Background

- On April 9, 2019, the Office of the Privacy Commissioner (OPC) released its Report of Findings in the Investigation of Equifax Inc. and Equifax Canada (PIPEDA # 2019-001).

- In it, the OPC found that Equifax had contravened various provisions of PIPEDA, including its accountability obligations under Principle 4.1.3 to provide a comparable level of protection for Canadians' personal information transferred to its parent company, Equifax Inc. in the U.S., for the purposes of processing their requests for certain direct to consumer products or fraud alerts.

- According to the 2009 Guidelines and the Office's previous interpretation of Principle 4.1.3, Equifax Canada would have had to take reasonable steps to provide a comparable level of protection for the data while in the hands of Equifax Inc., including by way of contract to ensure adequate policies and procedures, as well as effective security safeguards, subject to monitoring and audit.

- Also consistent with the OPC's previous position, Equifax Canada would have had to give appropriate notice to consumers informing them that their personal information would be processed in a foreign jurisdiction, and while located there, would be subject to the courts, law enforcement and national security laws of that other jurisdiction.

- It is important to note that this previous policy codified in the 2009 Guidelines was the encapsulation of the consistent position the Office had taken in several of its past reports of findings resulting from major investigations, including in the matters of CIBC (PIPEDA Case Summary #2005-313), SWIFT (PIPEDA Case Summary #2007-365) and CanWest Publishing Inc. (PIPEDA Case Summary #2008-394).

---

[3] Innovation, Science and Economic Development Canada, "Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*" (last modified 21 May 2019), online: *Government of Canada* www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

- In the context of the Equifax investigation, however, the OPC revisited its earlier interpretation of Principle 4.1.3 and ultimately departed from the Office's earlier position on transfers of data for processing, particularly transfers across borders, by requiring not only effective notice, but express consent on the part of consumers for the transfer of their personal information to the US for processing.

- Notwithstanding its finding that Equifax Canada retained control of the data transferred to Equifax Inc., the OPC considered the transfer of personal information as constituting a "disclosure" within the meaning of PIPEDA. The OPC determined that as there did not appear to be an explicit consent exemption for this type of disclosure for processing, consent was required for such transfer.

- Moreover, because the personal information in question was sensitive in nature (financial data) and that certain individuals requesting this service may not have expected their personal information to be sent to the U.S. (given what the OPC deemed to be erroneous indications to the contrary), the OPC reasoned that express consent was required.

- The OPC recognized that its finding that consent was required for transfers of data for processing resulted in a marked departure from the OPC's 2009 Guidelines.

- The OPC launched a consultation on the same day as the release of its Equifax finding (April 9, 2019) in order to invite views on this change in position on transborder dataflows for processing, recognizing that this affects all organizations subject to PIPEDA (not only Equifax) and may have impact on many other pieces of related guidance (including, in particular, the OPC's *Guidelines on Obtaining Meaningful Consent*)[4].

- On April 23, 2019, the OPC then launched a Supplementary Discussion Document providing further details on specific points on which the Office is seeking stakeholder input, calling for submissions by June 4, 2019.

- On May 16, 2019, the OPC made a further announcement extending the timeline for responses from June 4, 2019 to June 28th, 2019.

- On May 23, 2019, in the context of his keynote remarks at IAPP Canada, the Commissioner announced that he was suspending the consultations.

---

[4] "Guidelines for obtaining meaningful consent" (May 2018), online: *Office of the Privacy Commissioner of Canada* www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

- On June 11, 2019, the OPC announced that it was resuming its consultations on the basis of a Reframed Consultation document which was re-entitled to cover data transfers for processing more broadly and had the effect of superseding the first two consultation documents.

Assumptions

For the purposes of this submission, we are assuming that:

- the transferring organization has the requisite legal authority to collect and use personal information for the purpose for which it is purporting to do so -- whether that be through valid consent, or through one of the prescribed exceptions to consent;

- the third-party processor is acting on behalf of the transferring organization, the transferring organization retains control over the personal data through the imposition of contractual provisions, and such contractual provisions bind the processor to comparable level of protections; and,

- the purpose for which the transferring organization is transferring personal information to the processor is aligned with the lawful purpose for which the personal information was collected in the first place and the processor will not use the data for any new or different purpose outside the scope of the consent or other legal authority.

The Central Issue

The key principle at issue in this consultation is Principle 4.1.3 of PIPEDA which reads as follows:

> *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 central question being raised in this consultation is whether in addition to an organization's accountability obligations under Principle 4.1.3 of PIPEDA, an organization must also obtain consent of individuals prior to transferring their personal information to a third party for processing.

The Fundamental Approach to Statutory Interpretation

The fundamental approach in interpreting legislation is that the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.[5]

The overarching object and purpose of PIPEDA are set out at section 3 as being:

> *… to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.*

The most extensive interpretation of the purpose of PIPEDA remains to this day that of Justice Decary of the Federal Court of Appeal in *Englander v Telus Communications Inc.*[6] Recognizing that the Act seeks to reconcile "to the best possible extent, an individual's privacy with the needs of the organization", Justice Decary calls PIPEDA "a compromise both as to substance and as to form." After an extensive review of the history of the Act, Justice Decary concludes his analysis as follows at para 46:

> *All of this to say that, even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests. Furthermore, because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction. In these circumstances, flexibility, common sense and pragmatism will best guide the Court.* (our emphasis)

The Federal Court of Appeal's decision draws heavily from *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*[7] (the "**Annotated Guide**")

---

5 *Re Rizzo & Rizzo Shoes Ltd.*, [1998] SCJ No. 2 at para 21, 154 DLR (4th) 193 [*Rizzo Shoes*].

6 *Englander v Telus Communications Inc.*, 2004 FCA 387.

7 Stephanie Perrin et al, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, (Toronto: Irwin Law Inc., 2001) [*Annotated Guide*].

which was written by some of the original drafters of PIPEDA at the time. Justice Decary's observations are heavily inspired by "these learned authors" to whom he expresses his gratitude and "apologize(s) for using their material often verbatim."[8]

It is with the legitimate authority of the Federal Court of Appeal, therefore, that we turn to this *Annotated Guide* for assistance in placing PIPEDA in its proper historical context and deciphering its underlying policy objectives. An understanding of both the "substance" and the "form" of PIPEDA are critical for informing an enlightened exercise of statutory interpretation.

In terms of *substance*, this historical account makes it unmistakably clear that the very "raison d'etre" for PIPEDA, and why the CSA Code was developed in the first place, was to protect privacy while enabling transborder dataflows that were already seen back then as indispensable to Canada's competitiveness in the world of international trade and its success in the digital economy.

In the mid-1990's, Canada came under increasing pressure to harmonize its privacy protections in line with international developments at the time, including the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[9] and the draft EU *Data Protection Directive*[10] (introduced in 1990, adopted in 1995 and entered into force in 1998). As a result of these growing pressures from Europe, the Federal Government was urged to find a harmonized approach that would be deemed "adequate" in the eyes of the EU to allow free flow of data to and from Canadian organizations and establish the right regulatory environment for the Canadian digital economy to thrive.

Many of the debates leading up to the adoption of PIPEDA focused on the best approach for achieving this goal, i.e. a self-regulatory versus legislative approach; more protection versus less paternalism; federal power versus provincial power, etc. However, the policy intent of PIPEDA remained consistent throughout: to *enable* cross-border dataflows, not to frustrate them. This is evident from the testimony of the (then) Minister of Industry, the Honorable John Manley, who framed the discussion of Bill C-54 (PIPEDA) at Second Reading as follows:

---

8 *Supra* note 6 at para 8.

9 "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (original 1980 version), online: *Organisation for Economic Co-operation and Development* www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

10 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31.

> *Bill C-54 also has the great advantage that it builds upon the existing CSA voluntary measures. It is designed to provide a regime that is simple, yet effective, consumer friendly, not overly burdensome for industry, especially small and medium sized enterprises, cost-efficient and with a minimal administrative burden, and in conformity with Canada's international agreements and trade obligations*.[11] [**our emphasis]**

Consistent with this overarching objective, the authors of the *Annotated Guide* describe one of the key motivations for the Federal Government to act in this regulatory arena in the following terms:

> *Companies that cannot have access to customer and employee information, and process it where and when necessary, are at a disadvantage in today's highly competitive global economy. A credit card company may be collecting applications by printed forms mailed in or on an Internet site, and it may be processing the data in the Caribbean for a fraction of the cost of such transactions in Canada. It may be transmitting the data back electronically to other points in Canada. How can a province regulate such activities, relying on powers within the province? How can companies compete if they are unable to take advantage of global data-processing resources that cut costs?*[12] **[our emphasis]**

In terms of *form*, PIPEDA's unique drafting style can also be explained in historical terms. The pressure to find a harmonized approach for enabling dataflows prompted a response from the business community long before PIPEDA was ever even conceived. In a proactive move, (perhaps in an attempt to stave off legislation, at least initially), the Canadian Standards Association ("CSA") was approached to create a technical committee comprised of consumer representatives, government, business, labor and professional associations, to develop an industry standard for data protection. This CSA Code was eventually adopted unanimously in 1995 and published as a standard in 1996. The next year, the Information Highway Advisory Council to then Minister of Industry John Manley recommended that government develop a flexible statutory framework based on the CSA standard, which the government accepted to do.[13]

A whole period of public consultation and negotiation ensued about the relative pros and cons of self-regulation versus legislation. There were proponents of the voluntary CSA Code who wanted it incorporated *as is* into the legislation, so as not to risk unraveling the

---

[11] "Bill C-54, Personal Information Protection and Electronic Documents Act", 2nd reading, *House of Commons Debates*, 36-1, No 137 (October 19, 1998) at 1215 (Hon John Manley).

[12] *Annotated Guide*, *supra* note 7 at 8.

[13] *Ibid* at xiv.

carefully conceived and well-accepted compromises that had been reached by stakeholders. Others, namely technical drafters and legal scholars expressed consternation how such a code, written in a language so foreign to traditional legal drafting, could be included *holus bolus* into law given all the inherent difficulties this would mean for statutory interpretation. Yet others, including consumer and human rights advocacy groups, pushed for altogether stronger protection.[14]

All of these perspectives and options were thoroughly considered. In the end, and for many policy reasons clearly articulated in the *Annotated Guide*,[15] including to respect constitutional division of powers and give effect to the underlying policy intent of *facilitating* international trade, the government incorporated the entire CSA Code intact as a Schedule to the Act.

> *For all these reasons, with the full support of the industry players who contributed to the CSA Standard, but to the great bewilderment of privacy experts and scholars everywhere, the drafters of this legislation set about the task of incorporating the text of the standard intact in the law. It was decided to incorporate it as a Schedule and make the modifications in the body of the law that would inevitably be required to retrofit the language of the code to a legal text.*[16] **[our emphasis]**

This legislative choice has caused considerable interpretation challenges for courts, regulators and stakeholders ever since. In fact, as part of the government's current proposals to modernize PIPEDA prospectively, it explores the possibility of doing away with the Schedule altogether and incorporating the relevant principles into the body of the Act itself.[17] While the government's proposal to simplify PIPEDA for the future and clarify its scope (including in respect of transborder dataflows) is critically important, it should not affect the legal analysis of the law as it currently stands.

This historical background that led to the strange and unique form of PIPEDA is relevant for several reasons. First, it is important for understanding that this legislative choice was not taken lightly. Rather, it was the subject of intense reflection and controversial debate before the Government, and ultimately Parliament, decided to incorporate the CSA Code, as is, into proposed law despite acknowledging all the inherent difficulties this would entail. It is also helpful background for appreciating the very careful and deliberate exercise

---

14 *Ibid* at 5-6.

15 *Supra* note 7 at 9-11.

16 *Ibid* at 11.

17 "Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*", *supra* note 3 at *Part 4: Areas of Ongoing Assessment*.

the legislative drafters undertook to systematically comb through the CSA Code and retroactively "fix" whatever was unclear or undesirable through the front-end provisions and qualifying clauses included in Part 1 of the Act.

Second, this historical background is critical for guiding a logical approach to interpreting PIPEDA that begins with the Schedule first. This approach is strongly reinforced by the authors of the Annotated Guide as follows:

> *This guide addresses the legislation in logical order, namely by examining Schedule 1 first because the basic requirements for the protection of personal information are all contained in the standard, and the Act itself addresses exceptions and elaborations that are not self-explanatory without the core concepts of the standard being thoroughly understood first. The drafters of the Act had to provide more precision where the language was too general for a statute, and delete certain definitions and notes when policy had been introduced in non-statutory language* (page xv) *... The code is at the heart of the Act, and it is essential that it be read first to understand the operation of the provisions in the body of the legislation.*[18] **[our emphasis]**

This "Schedule-first" approach to interpretation is supported by the Act itself. The very *first* operative provision, following definitions, purpose and scope of application, begins with section 5(1) in Division 1 under "Protection of Personal Information" which reads as follows:

5(1) *Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.*

The Words of the Act

This Schedule-first approach leads us directly to Principle 4.1.3. in Schedule 1 which sets out the requirements for organizations that transfer data to a third party for processing. The principle reads as follows:

> *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*

[18] *Annotated Guide*, *supra* note 7 at 13.

> *comparable level of protection while the information is being processed by a third party.* **[our emphasis]**

It is particularly noteworthy that the word "processing" appears only twice in the entire Act. Other than Principle 4.1.3, the only other instance where "processing" is referred to is in Principle 4.1.1 which reads as follows:

> *Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).* **[our emphasis]**

It is presumed that the legislature uses language carefully and consistently so that within a statute or other legislative instrument, the same words have the same meaning and different words have different meanings.[19] In keeping with this statutory rule of consistent expression, therefore, we must read Principles 4.1.1 and 4.1.3 together.

As per Principle 4.1.1, the word "processing" is understood as being akin to the day-to-day collection of personal information, in other words, the daily, routine and operational treatment of data. When read together with Principle 4.1.3, the organization remains responsible for this day-to-day, routine processing of personal information whether the data is in its own possession or custody or has been transferred to a third party for processing. In other words, the Act provides organizations with the needed flexibility to operationalize that day-to-day routine processing activity, whether that means using an organization's own employees working in the office or teleworking, contracting out the activity to individual contractors working onsite or offsite, or outsourcing the activity to a separate third-party organization in Canada or abroad.

Because "possession", "custody" and "transfer to a third party" are all intended to be part of the same category through the use of the term "*including*" in Principle 4.1.3, there must be some common thread that connects these words together. In our respectful submission, the common thread ("le fil conducteur") is the concept of "control". This unifying concept is guided by the opening paragraph of Principle 4.1 which holds an organization "responsible for personal information under its control".

---

[19] Ruth Sullivan, *Sullivan on the Construction of Statutes*, 6th ed. (Markham, Ontario: LexisNexis, 2014) at 217 [Sullivan].

It is our respectful view that Principle 4.1.3, when read together with Principles 4.1 and 4.1.1, provides *a clear and full* answer to what an organization must do to enable data transfers to third parties for processing namely:

> ***As long as 1) the transferring organization remains in control of the data and the processing is merely the operational means by which the lawfully authorized purpose is being carried out; 2) the purpose for processing is aligned with the lawfully authorized purpose without introducing any new or different purpose; and, (3) the personal information remains safeguarded by a "comparable level of protection", an organization may transfer data to a third party for processing.***

Our interpretation of Principle 4.1.3 in the context of the other Accountability principles is supported by the informed commentary provided in the *Annotated Guide*:

> *Clause 4.1.3 is important because it is the only area in the Act where transborder dataflow issues are addressed. An organization remains responsible for information in its possession or custody, including information that has been transferred to a third party for processing. The concept of custody and transfer is an important one, as opposed to disclosure, because when an organization discloses information, it must assure itself that it has the right to disclose, and once that is fulfilled and the disclosure has taken place securely, its responsibility is at an end.*
>
> *However, if the information has been transferred for processing of any kind, and the organization expects to maintain an interest in the data, it retains responsibility and must use contractual or other means to provide a comparable level of protection.* [20] **[our emphasis]**

The question remains however, whether in addition to the above statutory rule, an organization must also obtain individual consent before transferring their personal data to a third-party processor. In our view, when the words of Principle 4.1.3 are properly interpreted according to the fundamental approach, analyzed in their entire context, harmoniously with the 1) scheme of the Act, 2) its intents and purposes, and 3) Parliament's intention, the answer is clearly *no*.

[20] *Annotated Guide*, *supra* note 7 at 16.

The Scheme of the Act

As remarked by the Federal Court of Appeal, the "non-legal drafting" of Schedule 1 and its awkward incorporation *as is* into the Act, makes for a unique structure that "does not lend itself to typical rigorous construction".[21] Rather, the guiding principles for interpreting PIPEDA must be "flexibility, common sense and pragmatism".[22]

Had the legislator intended for consent to apply as an additional condition to the statutory rule set out in Principle 4.1.3 for data transfers for processing, it would have clarified this in the provisions of Part 1 of PIPEDA where it painstakingly made many other clarifications, exceptions or qualifications to the Principles of Schedule 1. Part 1 of PIPEDA contains several such examples:

> Section 2(2): *In this Part, a reference to clause 4.3 or 4.9 of Schedule 1 does not include a reference to the note that accompanies that clause.*
>
> Section 5(2): *The word should when used in Schedule 1, indicates a recommendation and does not impose an obligation.*
>
> Section 6: *The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organization of the obligation to comply with the obligations set out in that Schedule.*
>
> Section 6.1: *For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.*

among many others at the following sections: 7(1); 7(2); 7(3); 7(4); 7.1 (2); 7.1(3); 7.2(1); 7.2(2); 7.3; 7.4(1); 7.4(2); 8(1); 8(8); 9(1); 9(2.4); 9(3); 10.2(3); and 10.2(4). In keeping with the Schedule-first approach described above, the fact that there is no qualification to Principle 4.1.3 in the body of the Act means that the words of the Accountability Principle were intended to speak for themselves.

Furthermore, in our view, the Accountability Principle is not necessarily linked to the Consent principle as the OPC has suggested. Had this been the intention, Principle 4.1 or any of its sub-principles would have expressly stated which principles or sub-principles they are linked to or must be together read with as is currently the case for many other

---

[21] *Englander v Telus Communications Inc*., 2004 FCA 387 at 46.

[22] *Ibid*.

Principles or sub-principles that explicitly reference other parts of the Code. For example, see: Principle 4.2 (sub-principle 4.2.1; 4.2.2; 4.2.4; and 4.2.6), 4.4 (sub-principle 4.4.1 and 4.4.3); Principle 4.5 (sub-principle 4.5.1 and 4.5.4); Principle 4.7 (sub-principle 4.7.2 and 4.7.5) and Principle 4.10 (sub-principle 4.10.1).

When the words of Principle 4.1.3 of PIPEDA are interpreted as we posit they should be above, then there is no new trigger that would require fresh consent. According to Principles 4.2.4[23] and 4.3.1[24], an organization shall identify the purposes for which personal information is being collected, obtain consent for that purpose, and seek further consent for any new purpose not previously identified. However, to the extent that the processing remains for the *same purpose* for which the data were originally collected, then there is no new purpose being introduced which has not previously been identified. What triggers a new consent requirement, therefore, is a change of *purpose* or a change of legal *control*, not merely a change of *processor*.

Finally, given that there is no basis upon which to require new consent as per Principles 4.2.4 or 4.3.1 above, there is no reason why the transferring organization would have to find itself within one of the explicit exceptions to consent in section 7(2) or 7(3) to permit the transfer. The fact that there is no consent exception under PIPEDA that would appear to expressly allow data transfers for processing is irrelevant, since the need for consent is not triggered in the first place. In other words, as the consent rule does not apply to transfers for processing, there is no obligation to fit within one of the exceptions at sections 7(2) or 7(3).

The Objects and Purposes of the Act

Under the fundamental approach to statutory interpretation, the words of an Act must also be read harmoniously with its objects and purposes. As described in much detail above, PIPEDA was intended to serve dual purposes – to protect individuals' rights to privacy, while also facilitating the collection, use and disclosure of personal information by the private sector, including to enable transborder data flows that allow Canada's digital economy to thrive.

---

[23] Principle 4.2.4 PIPEDA: *When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).*

[24] Principle 4.3.1 PIPEDA: *Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).*

If PIPEDA is interpreted as requiring consent (especially express consent) in order to transfer data for processing, the net effect will be to significantly impede outsourcing as a legitimate and viable means by which organizations choose to manage their day-to-day operations in order to enhance quality and timeliness of service while remaining competitive and viable in the global marketplace. Such an interpretation would frustrate or defeat the legislature's purpose and should therefore be rejected if there is a plausible alternative that would be more consistent therewith, as is the case here.[25]

Further, it is a well-established principle of statutory interpretation that the legislature does not intend to produce absurd consequences.[26] Reading a consent requirement into PIPEDA's Accountability Principle would lead to absurd consequences that would ultimately frustrate the purposes of the Act and therefore should be avoided.

As noted above, AccessPrivacy convened a workshop at our Toronto offices on April 26th specifically to discuss the OPC's consultation on transfers for processing, which was attended by over 90 Chief Privacy Officers, senior in-house counsel, trade association representatives, and other privacy compliance professionals, from major Canadian organizations across multiple industry sectors. During this workshop, attendees discussed the severe, adverse practical impact of the OPC's new position on consent for transfers of personal information for processing. In sum, there was a consensus among attendees -- which was echoed by numerous client calls about the OPC's consultation thereafter – that it would it would be practically unfeasible (if not impossible) to operationalize a requirement for consent for transfers to third party processors in a manner that complies with the requirements under PIPEDA Section 6.1 for valid consent and Principle 4.3 of the Schedule, and also meets the expectations set out in the *OPC's Guidelines for Meaningful Consent*.

Common concerns cited by attendees of the April 26th workshop and many clients since include the following:

- Service provider arrangements involving the processing of data are a staple feature of the emerging data environment across all industry sectors, and a large proportion of these service provider arrangements involve the processing of personal information. Organizations in many sectors indicated that they have hundreds (and, for larger organizations, several thousand) active third-party service provider arrangements in place involving the processing of personal information, including arrangements with numerous independent contractors, a growing array of smaller scale service providers and large third party outsourcers. As such, the OPC's new

---

[25] Sullivan, *supra* note 19 at 288.

[26] *Rizzo Shoes*, *supra* note 5 at para 27.

position on consent impacts at least hundreds of thousands of service provider arrangements currently in existence across all industry sectors.

- To comply with PIPEDA's consent requirement, organizations would be required to provide meaningful choice for individuals to decide whether they wish their personal information to be transferred to the service provider in question. To ensure that individuals are able to understand the "nature, purposes and consequences" of such processing (as required by Section 6.1 of PIPEDA), an organization would need to provide notice containing a list of third-party service providers that may be involved in the processing of an individual's personal information, the types of personal information that would be transferred and processed by the service providers, a description of the purposes for the transfer, and the location of the processors' services and/or servers. By implication, stakeholders commonly indicated such a requirement would add significant length and unmanageable detail to their current notices and privacy statements. Notably, such notices would presumably have to (somehow) expressly contemplate sub-contracting arrangements, thereby further adding length and complexity of necessary disclosures to end users.

- Many stakeholders maintained that, since all organizations subject to PIPEDA would have to provide notice to end-users, the bewildering number of notices required to satisfy this "additional" consent requirement would undoubtedly overload and overwhelm users. There were significant concerns that the OPC's new position will cause serious notice "fatigue". Moreover, since service provider arrangements (let alone sub-contracting arrangements) are regularly amended, renewed or expire, this would require organizations to provide consent notices on a continuous basis.

- In addition to notice, stakeholders cited severe practical issues with the operationalization of choice mechanisms for the consent requirement. For instance, where the transfers to processors may involve more sensitive types of personal information, organizations would be in the practically untenable position of being prohibited under PIPEDA from transferring personal information to the service provider unless and until the individual in question provided their express consent for such transfers. Moreover, to comply with the consent requirement (whether express or implied), organizations would have to obtain consent for all existing service provider arrangements, thereby inundating individuals with communications and choice options. Thereafter, individuals would then be forced to continually assent to a countless number of service provider arrangements.

- Stakeholders across sectors have indicated that, in many instances, a withdrawal of consent would be effectively meaningless since in the vast majority of cases there

would be no reasonable alternative for extricating individuals from certain standard business processing activities that are legitimately rendered by service providers. Stakeholders unanimously maintained that consumers would clearly not expect to receive the volume, length and types of different notices (from organizations across all industry sectors) that would legally be required to satisfy a consent requirement for transfers for processing. Rather, the prevailing view expressed by stakeholders was that the consent requirement would invariably serve to frustrate the user experience and stifle the near-instantaneous benefits that individuals expect to receive in the online and digital environment.

- Stakeholders indicated that they currently do not have consent management processes for service provider arrangements, and that the costs of designing, implementing and maintaining such a framework would be immense. Multiple larger organizations advised us that the cost of designing, implementing and maintain such a system would cost millions of dollars. Several small to medium organization advised us that the overall compliance cost of operationalizing this new consent requirement (which ironically, they would likely have to outsource) would be very high and exceedingly difficult to absorb.

- Finally, many organizations expressed serious concerns about the confidentiality issues associated with this consent for transfers to processers. Stakeholders specifically indicated that, often, the existence of these arrangements are commercially sensitive information and that it is necessary to maintain their confidentiality for competitive purposes.

In keeping with the well-established principle of statutory interpretation that the legislature does not intend to produce absurd consequences, an interpretation that would lead to the above consequences should be avoided.

The Intention of Parliament

In accordance with the fundamental approach, the words of Principle 4.1.3 must also be read in harmony with the intention of Parliament. As described above, the intention of Parliament at the time of the enactment of PIPEDA was clearly to enable digital commerce and transborder data flow, not to impede it. Despite ETHI's recommendation that PIPEDA be amended to address the issue of "principal-agent relationships", the Government's response[27] stated its preference that education and guidance be used as an alternative to

---

[27] *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics* at recommendation 8, (2007) 39th Parliament, 1st session.

legislative amendment and called on the Privacy Commissioner of Canada to adopt interpretive guidelines in this regard, which it did with its 2009 Guidelines. Presumably, the Legislature was aware of the existence of these very Guidelines it had recommended when it amended PIPEDA in 2015 with the adoption of Bill S-4[28], and still saw no need to waver from Parliament's original legislative object by amending PIPEDA in respect of its provisions on transfers of personal data for processing.

The legislature is presumed to know its own statute book when it drafts new legislation taking into account the substantive law embodied in existing statutes.[29] An interpretation of Principle 4.1.3 that requires organizations to retain *control* over the data, maintain *consistency of purpose* and ensure a comparable level of protection through *contractual* or other means -- without requiring additional consent -- is also consistent with the approach that had been taken in the Federal public sector almost two decades prior to the adoption of PIPEDA under the *Privacy Act*, as supplemented by applicable *Treasury Board Guidelines*.[30]

In interpreting Parliament's intention, it is also standard practice for courts to refer to the laws of other jurisdictions dealing with similar subject matter.[31] Interpreting Principle 4.1.3 as we suggested above -- without imposing a requirement for additional consent -- is completely aligned with *all* of the provincial health laws[32] and private sector privacy laws[33] that have been declared substantially similar to PIPEDA. Each one of these substantially similar laws underwent a similar evaluation process by Governor in Council which included an assessment of whether they incorporated the ten principles in Schedule 1 --

---

28 *Digital Privacy Act*, SC 2015, c 32.

29 Sullivan, *supra* note 19 at §13.35.

30 Treasury Board of Canada Secretariat, "Guidance Document: Taking Privacy into Account Before Making Contracting Decisions" (last modified 25 August 2010), online: *Government of Canada* www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-document-taking-privacy-into-account-before-making-contracting-decisions.html. See also "Guidance on Preparing Information Sharing Agreements Involving Personal Information" (last modified 25 August 2010), online: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html.

31 Sullivan, *supra* note 19 at §13.41.

32 *Personal Information Protection Act*, SA 2003, c P-6.5 [Alberta PIPA]; *Personal Information Protection Act*, SBC 2003, c. 63 [BC PIPA]; *An Act respecting the protection of personal information in the private sector*, CQLR, c P-39.1 [Quebec Privacy Act].

33 *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A [ON PHIPA]; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 [NB PHIPAA]; *Personal Health Information Act*, SNL 2008, c P-7.01 [NL PHIA]; *Personal Health Information Act*, SNS 2010, c 41 [NS PHIA].

with "special emphasis" placed on the principle of consent.[34] If, as previous Commissioners have said, PIPEDA is the "floor" not the ceiling[35], then how could these laws have ever been deemed to be substantially similar if they do not require new consent for transfers of data for processing, while PIPEDA (according to the OPC's proposed reinterpretation) does? If these provincial laws diverged so significantly on an issue as fundamental as consent, they would likely never have achieved substantially similar status.

On the other hand, where legislatures have wanted to require consent for data transfers for processing, they have done so explicitly, as in the case of British Columbia's *Freedom of Information and Protection of Privacy Act*[36] and Nova Scotia's *Personal Information International Disclosure Protection Act*[37]. It is especially noteworthy however, that both these acts are in the public sector, *not* the private sector, and reflect a deliberate policy choice by those specific provinces to deal with the special case of transborder flows of personal data.

Finally, when compared with the privacy laws of other jurisdictions beyond Canada's borders, if one were to interpret PIPEDA as requiring consent as the only lawful basis for permitting transfers of personal data for processing, this would put Canada entirely offside the rest of the world, including its closest economic counterparts: Europe[38], Brazil[39], Singapore[40], Hong Kong[41], Australia[42], and United States (California)[43]. Such an interpretation should not be favored over one which is more consistent with similar laws of other jurisdictions and which furthers the intention of Parliament to promote a harmonized international approach that enables international dataflows.

---

34 *Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council*, (2002) Gaz I, 2388 (Vol. 136, No. 31) [*Gazette*].

35 *Gazette*, at 2387.

36 RSBC 1996, c-165, section 30.1.

37 SNS 2006, c. 3, section 5(1).

38 Regulation (EU) 2016/679 (General Data Protection Regulation).

39 *Brazil's General Data Protection Law* (Law No. 13,709, of August 14, 2018).

40 *Personal Data Protection Act 2012* (No. 26 of 2012) [Singapore].

41 *Personal Data (Privacy) Ordinance (Cap. 486)* [Hong Kong]

42 *Privacy Act 1988* (Act No. 119 of 1988). See also *Australian Privacy Principles*.

43 *California Consumer Privacy Act of 2018* (SB-1121).

Canada's International Commitments

It is also a well-established principle of statutory interpretation that a jurisdiction's legislation will be presumed to conform with its international commitments. The presumption of conformity is based on the rule of judicial policy that, as a matter of law, courts will strive to avoid constructions of domestic law pursuant to which the state would be in violation of its international obligations, unless the wording of the statute clearly compels that result.[44]

If PIPEDA is interpreted as requiring consent before personal information can be transferred to a third party for processing -- particularly outside Canada-- this would *in effect* be tantamount to imposing a data localization requirement on organizations for all of the practical, operational reasons explained above. This in turn would likely contravene Canada's existing commitments under several international agreements. More specifically:

- Under both the pending Canada-United States-Mexico Agreement[45] ("**CUSMA**") and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership[46] ("**CPTPP**"), Canada has committed "to allow"[47] or not to "prohibit or restrict the cross-border transfer of information, including personal information".[48] While a party may restrict such transfers if necessary to achieve a legitimate public policy objective, it can only do so in a way that is minimally impairing[49] (i.e., if it does not impose restrictions on transfers of information greater than necessary to achieve the objective).

- Imposing a consent requirement for international data transfers for processing is arguably not necessary to achieve a legitimate public policy objective that was never even contemplated or debated in Parliament, nor could it be said to minimally impair on Canada's international trade obligations. Hence, reinterpreting PIPEDA

---

44 *R. v. Hape*, 2007 SCC 26 at para 53.

45 *Canada-United States-Mexico Agreement*, (2019), online: *Government of Canada* www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/toc-tdm.aspx?lang=eng [*CUSMA*].

46 *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (signed in 2016), online: *Government of Canada* www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/toc-tdm.aspx?lang=eng [*CPTPP*].

47 Article 14.11(2) (*CPTPP)*.

48 Article 19.11(1) (*CUSMA*).

49 Article 19.11(2) (*CUSMA*) and Article 14.11(3) (*CPTPP*).

in such a way as to require consent would, in our view, likely contravene Canada's trade obligations under both CUSMA and CPTPP.

- Moreover, it is unlikely that Canada would have further committed to Article 19.12 of CUSMA which prohibits Canada from requiring the use or location of computing facilities within its own territory as a condition for conducting business in Canada[50], had it known or believed it already had, on its statute books, a federal data localization requirement applicable to organizations conducting commercial activity in Canada at the time it signed the agreement.

- Similarly, under both CUSMA and the Canada-European Union Comprehensive Economic and Trade Agreement[51] ("**CETA**"), Canada has committed to maintaining a legal framework that provides for the protection of personal information of users of digital trade in a manner that "take(s) into account the principles and guidelines of relevant international bodies, such as 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)".[52]

- Both the Asia-Pacific Economic Cooperation ("**APEC**") *Privacy Framework*[53] and the Organization for Economic Cooperation and Development ("**OECD**") *Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

---

[50] *CUSMA, supra* note 45 at 19.12: *No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.*

[51] *Canada-European Union: Comprehensive Economic and Trade Agreement* (2016), online: *Government of Canada* www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/toc-tdm.aspx?lang=eng [*CETA*].

[52] *CUSMA* at 19.8(2). See also *CETA* at preamble: *ENCOURAGING enterprises operating within their territory or subject to their jurisdiction to respect internationally recognised guidelines and principles of corporate social responsibility, including the OECD Guidelines for Multinational Enterprises, and to pursue best practices of responsible business conduct*.

Also, *CETA* article 13.15(2): 2. *Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers shall be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.*

Also, "Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*" at *Possible options — self-regulation and technical standards*.

[53] Asia-Pacific Economic Cooperation, "APEC Privacy Framework" (2005), online: www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

("**Revised Privacy Guidelines**")[54] have as their very object to promote the interoperability of privacy laws and enable transborder data flows between member authorities.[55] By interpreting PIPEDA as imposing a consent requirement as the only lawful basis for permitting data transfers for processing, Canada's privacy regime would significantly diverge from that of its co-signatories, contrary to the common purpose of greater harmonization. Again, it would seem highly unlikely that Canada would have endorsed the APEC Privacy Framework in 2005 and the OECD Revised Privacy Guidelines in 2013, and then further committed under CUSMA and CETA to uphold these very principles and guidelines, if it knew at the time of signing these agreements that it was already in breach of them.

As a result, such an interpretation that runs contrary to Canada's conformity with international commitments should be avoided.

Presumption of Constitutionality

Also, under the presumption of compliance, it is presumed that the legislature intends to make legislation that complies with the Constitution, and to the extent possible, legislation is therefore interpreted to achieve that result.[56]

Put another way, "[i]f a legislative provision can be read both in a way that is constitutional and in a way that is not, the former reading should be adopted."[57]

Interpreting Principle 4.1.3 as requiring organizations to obtain new consent prior to transferring personal information to a third-party processor would cripple some of the most important economic advantages of outsourcing particularly across borders to leverage global economies of scale, driving organizations to keep processing activity internal to the company or very close to home instead. The inevitable effect of such an interpretation may actually weaken the constitutional underpinning of PIPEDA as a valid exercise of the federal Parliament's authority to legislate in respect of trade and commerce, particularly under the first branch.

The federal trade and commerce power is confined to two branches of legislative authority: (i) interprovincial or international trade and commerce; and (ii) the general regulation of

---

54 "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (2013 version), online: *Organisation for Economic Co-operation and Development* www.oecd.org/internet/ieconomy/privacy-guidelines.htm [*Revised Privacy Guidelines*].

55 *APEC*, at pp. 35-36 and *Revised Privacy Guidelines* at Chapter 1, p. 11.

56 Sullivan, *supra* note 19 at 16.3.

57 *R. v. Sharpe*, [2001] 1 SCR 45 at para 33.

trade and commerce affecting the whole of Canada. The federal Government has relied on both these branches in enacting PIPEDA, as evidenced by the following statements of then Industry Canada Minister John Manley: "[p]ersonal information is now a commodity which can be bought, sold and traded… [with] commercial value in and of itself… [that] is crossing all boundaries – provincial, territorial and national" and that "[p]rovinces acting alone and even together cannot pass laws that can effectively protect information crossing those boundaries."[58]

PIPEDA invites constitutional scrutiny when it purports to regulate purely intra-provincial aspects of private sector privacy matters. Following the Supreme Court of Canada's decision in *Reference re Securities Act (Canada)*[59], constitutional law experts have questioned whether the general regulation of intra-provincial trade and commerce by PIPEDA could be upheld under the second branch of the trade and commerce power alone.[60]

The constitutional justification of PIPEDA therefore rests largely on the first branch of the federal Government's trade and commerce power (interprovincial and international trade) and would necessarily depend on an interpretation of Principle 4.1.3 that is more consistent with PIPEDA's stated purposes of facilitating electronic commerce and bringing Canada's laws in line with international trade requirements.

Requiring consumers to consent to the transfer of their personal information to third party processors, particularly outside of Canada, would have an unintended chilling effect on inter-jurisdictional e-commerce by rendering it virtually impossible for organizations to outsource certain aspects of a transaction (e.g., payment processing, shipping, etc.) to external entities, let alone entities located in other jurisdictions. The net effect would be an undermining of PIPEDA's inter-jurisdictional scope that underpins the legislation's constitutional validity under the first branch of the trade and commerce power. Such an interpretation must be eschewed in favor of one which supports the law's constitutional validity.

---

58 "Bill C-6, Personal Information Protection and Electronic Documents Act", third reading, *House of Commons Debates*, 36-2, No 9 (October 22, 1999) at 1005 (Hon John Manley).

59 *Reference re Securities Act*, 2011 SCC 66.

60 Former Supreme Court of Canada Justice Michel Bastarache, "The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada's Reference re Securities Act" (June 2012), online (pdf): http://accessprivacy.s3.amazonaws.com/M-Bastarache-June-2012-Constitiutionality-PIPEDA-Paper-2.pdf.

Conclusion

In our respectful view, individuals have clearly come to contemplate, if not expect, that their personal information may be transferred to third parties for processing including in other countries; this has become a modern day reality for consumers themselves every time they choose to send photos or emails to the cloud, or every time they speak to sales representatives or technicians in a call centre across the world which has become a very common phenomenon.

More than ten (10) years ago, the OPC stated in their 2009 Guidelines that individuals should be aware of the reality of transborder dataflows. One can only expect such awareness to have increased since that time through the concerted education efforts of privacy regulators around the world.

Any change to the policy direction for allowing transfers of personal information for processing would, with respect, be better left for Government, and eventually Parliament to decide upon given the broad implications for Canada's investment in the digital economy and its commitments to various international trade obligations. ISED has already indicated that it would be clarifying this issue in the context of its consultations for PIPEDA reform.

Participants at our April 26th workshop and many other organizations have expressed significant concerns that until these PIPEDA amendments come to pass, the proposed interim change in OPC's position on the requirement for consent for transfers for processing has introduced considerable uncertainty in the Canadian digital arena. Stakeholders have also expressed concerns about the transparency, scope, and timing of the consultation process itself.

To address such concerns, we respectfully offer the following recommendations for the OPC's consideration:

- Given the fundamental nature of the legal, policy and practical impact of the OPC's reinterpretation of the consent requirement for transfers of personal information for processing, we believe that ISED's consultation process for PIPEDA review is the appropriate forum to consider these issues and that the ISED consultations should be allowed to run their proper course. As such, we are recommending that the OPC "re-instate" its 2009 *Guidelines on Personal Data Across Borders* in accordance with the statutory analysis above and provide reassurance to stakeholders that until PIPEDA is amended, organizations may rely upon such guidance for their statutory compliance efforts.

- Consistent with the approach of your Office in the context of the consent consultations, we recommend that all written submissions of stakeholders be published on the OPC's website, and that cross-sectoral meetings be held with a view to ensuring that stakeholders can engage in constructive and meaningful dialogue with the OPC on such fundamentally important issues.

- To the extent that the OPC intends on amending any of its guidance in the wake of this consultation effort, we recommend that your Office publicly list all amendments being considered and publish drafts of such guidance documentation together with a meaningful opportunity to review and provide written comment.

We thank you once again for the opportunity to provide input into this process. If you have any questions or comments, please do not hesitate to contact pkosseim@osler.com or akardash@osler.com

Yours very truly,

AccessPrivacy, *by Osler*