nNovation LLP

Submission to the Office of the Privacy Commissioner of Canada

Consultation on Transfers for Processing

August 6, 2019

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

Contents

1. Introduction

The 2018 edition of *A Guide to the Personal Information Protection and Electronic Documents Act* (LexisNexis Canada) noted that organizations could expect that there would be pressure on the Office of the Privacy Commissioner of Canada ("OPC") to revisit its historical approach to transfers of personal information, with the result that the OPC might tighten the conditions on which personal information may be transferred to suppliers, and especially the conditions on which personal information may be transferred internationally.

This has come to fruition in the *Equifax*[1] finding and the subsequent consultation on transfers for processing (both domestic processing and transborder processing).

There is no question that your Office is grappling with the most complex and pressing issues that the OPC has faced in its history. It is clear that you and your staff are ready for the challenge, with some of the most thoughtful and nuanced guidance and Reports of Findings that we have seen since PIPEDA was enacted.

We also believe that your Office should be applauded for being open to rethinking past positions. As you are well-aware (with noted frustration), you are an Ombudsman and not an adjudicator. You are not bound by precedents set by former Commissioners or even your own previous findings. If times have changed and policy positions need to be rethought, you should be free to do so.

Of course, if organizations believe that your interpretations of PIPEDA are incorrect, they are also free to choose to proceed otherwise. If necessary, issues will be resolved in the courts should you believe that your position should and will prevail over the interpretation of industry.

To be clear – ultimately, our concern is not with the outcome of the Equifax case. Indeed, we believe that most of the outcome on the consent issue in the Equifax case can be explained on the basis of section 6.1 of PIPEDA and cl. 4.1.3 of Sch. 1 to PIPEDA. It is likely that you will receive many submissions from stakeholders coming to a similar conclusion.

Where our position parts company with the one under development by your Office is the idea that transfers for processing are a "disclosure" (or, for that matter, even a "use") within the meaning of PIPEDA, and the idea that PIPEDA could be interpreted as requiring "explicit" consent for the "how" of a use/disclosure as opposed to the "purpose" of a

[1] Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2019-001, Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, April 9, 2019.

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

use/disclosure.[2] This submission explains our view on how PIPEDA is to be interpreted and we hope that you will give it due consideration in coming to your own view.

2. Principles of statutory interpretation

As lawyers, we are well-trained by the Supreme Court of Canada to begin the construction of statutes with reciting the famous words of Elmer Driedger, a long-time Department of Justice lawyer who wrote many treatises on legislative drafting. His famous words on the construction of statutes was adopted by the Supreme Court of Canada and found in the frequently cited case of *Bell ExpressVu Limited Partnership v. Rex*[3] at para. 26:

> *Today there is only one principle or approach, namely, 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.*

Close attention to this one principle or approach reveals that it involves consideration of:

- the entire context of the Act;
- the grammatical and ordinary sense of the words;
- the scheme of the Act;
- the object of the Act; and
- the intention of Parliament.

Although the Supreme Court of Canada noted in *Bell ExpressVu Limited Partnership* that each of the factors need not be canvassed separately in every case, this is only because the interpreter, if faithful to the principle, understands that they are closely related and interdependent.

However, sometimes an interpreter will fish out one aspect of the principle – say, for example, the ordinary sense of a word (e.g. "disclose") – and neglect the other interpretative factors, even if they might lead to a different conclusion. However, as the Supreme Court of Canada noted (at para 27) with approval, "*words … take their colour from their surroundings*".

In our view, if you intend to overturn a longstanding interpretation of PIPEDA, you must have due regard for the breadth of considerations to be taken into account in Driedger's one principle or approach.

---

[2] If your Office maintains and adopts the position that a transfer is a disclosure, we also part company with the suggestion that express, separate consent would be required. The only workable solution is to rely on implied consent.

[3] *Bell ExpressVu Limited Partnership v. Rex*, [2002] 2 SCR 559, 2002 SCC 42 (CanLII).

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

2.1. The purpose of PIPEDA

Any interpretation of PIPEDA should begin with its purpose clause, which is set out in section 3:

> *The purpose of this Part is 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.*

Writing with reference to this purpose clause, the Supreme Court of Canada has explicitly acknowledged that the overall intent of PIPEDA is "*to promote both privacy and legitimate business concerns*": *Royal Bank of Canada v. Trang*,[4] at para. 44, citing Professor L.M. Austin. As the Supreme Court of Canada pointed out in that case (at para. 44), the OPC must not interpret PIPEDA in a way that would "*unduly prioritize privacy interests over the legitimate business concerns that PIPEDA was also designed to reflect*."

It is important to emphasise that the purpose clause is not a mere trifling thing to be given occasional lip service. A purpose statement gives context for the entire Act: *Council of Canadians with Disabilities v. Via Rail Canada Inc.,*[5] at para. 287.

In *Oceanex Inc. v. Canada (Transport)*,[6] the Federal Court stated that a purpose statement such as the one quoted above from PIPEDA carries the authority and weight of duly enacted law. In *Oceanex* (at para. 334), the Federal Court quoted approvingly the following statement of the binding nature of purpose clauses from Ruth Sullivan's definitive work on the interpretation of statutes:

> *14.39 Purpose statements may reveal the purpose of legislation either by describing the goals to be achieved or by setting out governing principles, norms or policies. Unlike preambles purpose statements come after the enacting clause of the statute and are part of what is enacted into law. This makes them binding in the sense that they carry the authority and weight of duly enacted law. However, like definitions and application provisions, purpose statements do not apply directly to facts but rather give direction on*

[4] *Royal Bank of Canada v. Trang*, [2016] 2 SCR 412, 2016 SCC 50 (CanLII) ("*RBC v. Trang*").
[5] *Council of Canadians with Disabilities v. VIA Rail Canada Inc*., [2007] 1 SCR 650, 2007 SCC 15 (CanLII)
[6] *Oceanex Inc. v. Canada (Transport)*, 2018 FC 250 (CanLII).

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

how the substantive provisions of the legislation – that do apply to facts – are to be interpreted.

Accordingly, an interpretation of PIPEDA must withstand the litmus test of PIPEDA's purpose clause when other provisions of PIPEDA, such as section 7(3) and cl. 4.1.3 of Sch. 1, are applied to real life facts.

Thus, even though the clarion call of your tenure is to provide individuals with greater control over their personal information – and there may be compelling reasons for transforming PIPEDA into a human rights-based statute - we must apply the law with the purpose of the current statute in mind, which involves reconciling these two interests.

Interestingly, the very origin and structure of PIPEDA have led the courts toward an interpretive approach that focuses on flexibility, common sense and pragmatism. The Federal Court of Appeal has said that, in light of the origin of the Schedule in the non-legal provisions of the Model Code, the Schedule does not lend itself to typical rigorous construction in which case "flexibility, common sense and pragmatism" should guide the courts in interpreting the Schedule: *Englander v. Telus Communications Inc.*[7] (at para. 46). The Federal Court of Appeal has also said that since the body of PIPEDA refers, in various places, to the Schedule and requires organizations to comply with the obligations set out therein (s. 5(1)), the interpretation of the body of the Act should also be approached in a less rigorous way than one would normally approach a statute: *Wansink v. Telus Communications Inc.*[8] (at para. 19).

Thus, recognizing a legitimate desire to protect the privacy of individuals, we must be skeptical of any interpretation of PIPEDA that results in the undue priority of individual rights over business interests, particularly if it is based on excessive formalism in interpreting a word such as "disclose" that neglects to honour faithfully Parliament's intention and the context of the globalized economy in which outsourcing across borders is not only prevalent, but as the OPC stated in the 2009 Guidance, a "*fact of life*".

3. A transfer is not a disclosure

In applying the principles of statutory interpretation to PIPEDA, it becomes clear that the only reasonable conclusion is that a transfer is not a disclosure.

3.1. Clause 4.1.3: Disclosure and transfer are distinct concepts

Clause 4.1.3 of PIPEDA states as follows

[7] *Englander v. Telus Communications Inc.*, 2004 FCA 387 (CanLII).
[8] *Wansink v. TELUS Communications Inc.*, [2007] 4 FCR 368, 2007 FCA 21 (CanLII).

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

> *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* [Underlining added].

The drafters of PIPEDA chose to use the word "transfer" in clause 4.1.3 for an obvious reason: there are important differences between a "transfer" for processing purposes and a "disclosure".

An outsourcing organization that transfers personal information to another organization for processing purposes (referred to here as the "processor") does so solely to fulfil its own, legitimate purposes for which it has consent to use that personal information. The processor can only process that personal information on behalf of and for the purposes explicitly authorized by the outsourcing organization. The processor has no authority to decide the purposes for which personal information can be collected, used or disclosed.[9] In this scenario, the outsourcing organization remains entirely accountable for the transferred personal information.

Thus, the processor in an outsourcing arrangement is an extension of the outsourcing organization. A disclosure is different. When personal information is disclosed, the receiving organization has at least some, if not all, authority over the personal information once it is in its control.

This distinction accords with commercial reality[10] and the way in which the terms "disclose" and "transfer" are used in PIPEDA.

It is also worth considering the importance of the word "including" in cl. 4.1.3. The ordinary meaning of "including" is, according to the Canadian Oxford English Dictionary, "inclusive of". This means that the authors of the Model Code most likely had in mind that information transferred to a third party for processing remains in the possession or custody of the outsourcing party for the purposes of PIPEDA. That information is therefore "included" in the information that the organization has possession or custody of.

Our experience is that businesses perceive of such transfers in exactly this manner. To take an everyday example, no organization believes that by using Microsoft Office 365 (a cloud-based offering), that the information is thereby no longer in the possession or custody of

[9] We use the term "collected" here because the same considerations from an accountability perspective apply if a processor collects personal information on behalf of the outsourcing organization.

[10] Consider the absurdity of having to obtain consent from individuals to allow independent contractors working inside of an organization to handle personal information, to use a cloud-based word processor, or to use the internet.

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

the entity that has outsourced the hosting of the word processing platform to Microsoft. The organization may no longer control the infrastructure, but it is very doubtful that the organization would view the personal information as somehow not within its possession and custody when the service provider is acting on its behalf.

Other examples abound. It is highly unlikely that an organization believes that they are no longer in possession and no longer have custody of personal information being handled by temporary staff employed by the temp agency but assigned to work within an organization's call centre.

Even where the *indicia* of possession and custody are weaker, such as the outsourcing of payroll to a third party where the data may be within the factual possession and custody of the third party with no immediate access by the outsourcing organization, responsible organizations take great pains to ensure that contractual provisions are strong enough to ensure that there is still legal control over that information and the right to recall possession and custody (and require the destruction of remaining copies) of the personal information once the personal information is recalled. Any disruption in factual possession and custody is paired with the right of recall.

Contrary to the incredulity[11] with which your Office has met the argument that transfers for processing are *sui generis* under PIPEDA and must be distinguished from disclosures, this also appears to be the contemporaneous understanding of those who had first-hand knowledge of the development of PIPEDA. Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, Q.C. made this point in the *Annotated Guide to the Personal Information Protection and Electronic Documents Act* (Irwin Law) published in 2001. As you likely are aware, Ms. Perrin was the Director of Privacy Policy for Industry Canada's Electronic Commerce Task Force and led the legislative initiative at Industry Canada that resulted in PIPEDA. It is worth quoting Ms. Perrin and her co-authors at length since it represents the prevailing understanding from the coming into force of PIPEDA right down to the OPC's change of position in the Equifax case (underlining added):

> *… 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*

[11] The reframed discussion document states as follows: "*This is an interesting interpretation but it is certainly not apparent from the explicit words of the Act*".

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

> *responsibility and must use contractual or other means to provide a comparable level of protection.*
>
> *Although this clause was drafted before the development of the internet as the engine of electronic commerce, it works particularly well in the new global environment of the collection and sharing of data through Internet browsers. The word "processing" was chosen because it was as technologically neutral as possible, and when used in the sense that it is used in the British Data Protection Act to refer to all kinds of data use and manipulation, it provides a simple broad rule. Contracts referring to the obligations of the standard would be appropriate when dealing with business partners, contractors, or data processing operations, while "other" anticipates the possibility that in cases of parent companies or affiliates, all parties may be required to comply with the same data protection code so that separate contracts between parties are not necessary.*

With this in mind, we should not lightly set aside the interpretation of "transfers" as distinguished from "disclosures", which has prevailed for over 18 years.

3.2. Sections 7(3) and 7.2 of PIPEDA support the distinction between transfer and disclosure

As your Office notes, the first definition for the word "disclose" in the Canadian Oxford Dictionary is to "make known" or to "reveal". Another common dictionary meaning is "to expose to view".[12] The meaning of "transfer" is defined first as to "move from one place to another" or to "hand over the possession of to a person".

But, as we know from the Supreme Court of Canada, words take their colour from their surroundings. So, the dictionary definitions are a beginning, but only a beginning. The exceptions to consent for disclosure of personal information in PIPEDA provide further interpretive context.

[12] It goes beyond the main thrust of this submission to address the various problems with identifying what is a "disclosure" in the context of outsourcing. However, it is important to acknowledge that the OPC would be required to answer some very difficult questions, including the following: Are some transfers disclosures while others are not? For example, is a transfer to a cloud computing provider where the cloud service provider agrees not to view the data in a human readable form or cannot technically do so (e.g. because the data is encrypted, and the client holds the key) a disclosure? If not, then what are the circumstances in which a transfer not a disclosure? Further, when exactly does the disclosing/transferring organization continue to be accountable for information that is disclosed/transferred? This is a problem that the OPC will have created, and must be prepared to address through clear, and comprehensive guidance on these very difficult questions.

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

Section 7(3) of PIPEDA begins by referencing cl. 4.3 of Schedule 1. Clause 4.3 states that the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. Section 7(3) qualifies and limits the note that accompanies cl. 4.1.3 and states that the only situations in which consent is not required for disclosure are those listed in section 7(3).[13]

When we look at section 7(3) of PIPEDA, each of the circumstances addressed by PIPEDA involve disclosures to another organization, person, or government institution that will use the personal information for a purpose other than the purpose for which the disclosing organization has consent. In most of these cases, the recipient will use the information for its own purposes as a controller rather than as an extension of the disclosing organization. This is true even in the cases of s. 7(3)(a) (to a barrister, solicitor or notary) and s. 7(3)(b) (to collect a debt). Parliament must have been aware that barristers, solicitors and notaries are not merely outsourced processors of personal information. They have independent duties to the court and to their regulators which constrain their ability simply to act on the instructions of their clients. In the context of debt collection, it may be necessary to disclose information for the purposes of skip tracing. These disclosures may involve the personal information no longer being within the effective control of the disclosing party.

Other textual evidence for why treating transfers for processing differently from disclosures is found in Section 7.2, enacted in 2015 to facilitate certain business transactions. Section 7.2 provides important insight that your Office's interpretation of "disclosure" as including transfers for processing might not be correct. In short, determining that a transfer is in fact a disclosure, and therefore could require express consent, would be absurd in light of section 7.2. As the former Chief Justice of the Supreme Court of Canada advised in *Rizzo & Rizzo Shoes Ltd. (Re),*[14] [1998] 1 SCR 27, 1998 CanLII 837:

> *It is a well-established principle of statutory interpretation that the legislature does not intend to produce absurd consequences. According to Côté, supra, an interpretation can be considered absurd if it leads to ridiculous or frivolous consequences, if it is extremely unreasonable or inequitable, if it is illogical or incoherent, or if it is incompatible with other provisions or with the object of the legislative enactment (at pp. 378-80). Sullivan echoes these comments noting that a label of absurdity can be attached to interpretations which defeat the purpose of a statute or render some aspect of it pointless or futile (Sullivan, Construction of Statutes, supra, at p. 88).*

[13] However, we know from the Supreme Court of Canada that section 7(3) does not necessarily cover the field when we consider implied consent (which is objective and does not necessarily rely on particular disclosures by the organization): *RBC v. Trang*.
[14] *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 SCR 27, 1998 CanLII 837 (SCC).

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

In the case of a prospective business transaction, the contemplated new uses are for due diligence purposes and to consummate the transaction. The potential types of transactions are broadly defined – not just asset sales – but also financing arrangements, creating security interests, and licensing, among other things. What each of the enumerated types of business transactions have in common is that the transaction would involve the recipient using the personal information for its own purposes – not as a processor on behalf of the disclosing organization.

Pursuant to section 7.2(1), if the transaction is not completed, no notice of the disclosure is required, much less consent. If the transaction is completed, section 7.2(2) permits the disclosure and use by the recipient organization of the personal information without consent provided that, among other things, the purposes for which the personal information are to be used are those to which the individual previously consented and the disclosing party or the recipient provides notice to the individual of the disclosure within a reasonable time after the transaction was completed. Importantly, however, even though the purpose might remain the same the party for whose benefit the information will be used and who will be accountable (either as a successor controller – e.g. in the case of an asset transfer – or a co-controller – e.g. in the case of an asset based lender) will have changed.

It would be absurd if a disclosure for business transactions where the recipient organization would end up using the personal information for its own business – whether as the acquiror of a business or as part of the security in asset based lending – could occur with after-the-fact notice (but no prior consent), but transfers for processing where the recipient is using the information solely on behalf of the outsourcing organization should require notice and prior consent.

Parliament could not have intended such an absurd and anti-business result. Of course, there is no reason to believe it did. On the contrary, Parliament is presumed to know all that is necessary to produce rational and effective legislation. As Sullivan has stated in the *Construction of Statutes, Sixth Edition* (LexisNexis Canada) at §8.9 (underlining added):

> *The legislature is presumed to know all that is necessary to produce a rational and effective legislation. This presumption is very far-reaching. It credits the legislature with the vast body of knowledge referred to as legislative facts and with mastery of existing law, common law and the Civil Code of Québec as well as ordinary statute law, and the case law interpreting statutes. The legislature is also presumed to have knowledge of practical affairs. It understands commercial practices and the functioning of public institutions, for example, and is familiar with the problems its legislation is meant to address. In short, the legislature is presumed to know whatever facts are relevant to the conception and operation of its legislation.*

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

At the time of enacting section 7.2 of PIPEDA, Parliament is presumed to have knowledge of:

- the commercial reality of the prevalence of outsourcing in Canada; and
- the long-standing guidance of your Office that a transfer for processing is not a "disclosure".

It seems absurd to impute to Parliament an intention to facilitate business transactions but to "leave" outsourcing stymied by a requirement to obtain prior consent. Although Parliament can legislate illogically, it is hard to believe, in light of the purpose of PIPEDA, that this would be the intended result.

4. Applying the litmus test of section 3 of PIPEDA

If PIPEDA is about rules to govern the collection, use and disclosure of personal information in a manner that recognizes not only (i) the right of privacy of individuals with respect to their personal information but also (ii) the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances, does your Office's new view that a transfer for processing is a disclosure better achieve the purpose of PIPEDA that the canonical interpretation of a transfer for processing being *sui generis*?

4.1. There are no benefits to defining a transfer as a disclosure

Let's begin with the proposition that organizations are required to get consent for the collection and use of the individual's personal information (cl. 4.3 of Schedule 1). Consent may be express or implied, but the use of sensitive personal information generally requires express consent (cl. 4.3.4). Clause 4.3.2 states that "[to] *make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed*." This is further buttressed by Section 6.1 of PIPEDA which requires informed consent of a capable person in order to be valid:

> *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.*

If the organization outsources the processing of the individual's personal information, the organization must use contractual or other means to provide a comparable level of protection while the information is being processed by the third party (cl. 4.1.3).

The fact that an individual's personal information is being processed by a third party on behalf of an outsourcing organization does not change the character of the use, provided

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

that the accountability principle in cl. 4.1 (generally) and 4.1.3 (specifically) are met. Unless the character of the use has changed by the third-party processing, no additional consent is required. As the Federal Court of Appeal stated in *Toronto Real Estate Board v. Commissioner of Competition*,[15] an individual exercises control over the purposes for which their personal information is collected and used, not the mode of use (at para 165):

> *PIPEDA only requires new consent where information is used for a new purpose, not where it is distributed via new methods. The introduction of VOWs is not a new purpose–the purpose remains to provide residential real estate services and the Use and Distribution of Information clause contemplates the uses in question. The argument that the consents were insufficient—because they did not contemplate use of the internet in the manner targeted by the VOW Policy—does not accord with the unequivocal language of the consent.*

Note that, for the same reasons, a transfer is also no more a "use" (separable from the original use for which consent was obtained) than it is a "disclosure".

That is not to say that outsourcing is irrelevant to the decision to provide consent. For example, the OPC stated that in the 2009 Guidelines that organizations need to be transparent about the transfers (bolded text in the current version posted to the OPC website):

> *Organizations need to **make it plain** to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction. They must do this in **clear and understandable** language. Ideally they should do it a**t the time the information is collected**. Once an informed individual has chosen to do business with a particular company, they do not have an additional right to refuse to have their information transferred.*

Since at least 2009, responsible organizations have identified that they use service providers and that data crosses borders.

As the OPC stated in 2009, data crossing borders is a "fact of life". These are true words. They are truer yet when it comes to outsourced processing generally.

Canada's economy relies on international trade and Canada's economic policy is to remove and prevent barriers to cross-border trade in services and electronic commerce. In 2014, Statistics Canada reported[16] on outsourcing trends to other countries between 2010 to

[15] *Toronto Real Estate Board v. Commissioner of Competitio*n, 2017 FCA 236 (CanLII).
[16] Statistics Canada, *Innovation and business strategy, outsourcing of business activities from Canada to another country in the last three years*.

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

2012. Keep in mind that this was long before the current large scale adoption of cloud-based services. At that time, Statistics Canada reported that 20.6% (1 in 5) of surveyed businesses outsourced business functions across borders. Interestingly, at that time it was small and medium sized organizations that were leading the pack with significantly higher rates of outsourcing than large businesses. This is not surprising, given that larger organizations may have economies of scale that might justify retaining processing activities in-house that SMEs would not have.

In this context, the main benefit to individuals of your Office's position would be a requirement for organizations to get specific consent to the transfer of personal information for processing as a separate matter from the use of personal information. Since the "use" of the personal information does not change in outsourcing, the practical purpose of such consent would be to provide individuals with control over "how" their personal information is processed. This would be a new right that some individuals might appreciate but it is not well-grounded in PIPEDA. PIPEDA governs rules relating to the collection, use and disclosure – not the "how" of an organization's business methods through which it uses personal information.

In any event, this new "right" would be chimerical. Given the prevalence of outsourcing, it will be the rare enterprise that would not require consent for such "disclosures". Indeed, taken to its logical conclusion, the mere use of the internet would require consent, necessitating consent in nearly every modern use of technology. Even if the OPC found some way to address that absurdity (see footnote 12 above), the fact is that no organization will want to be in a situation where it must obtain fresh consent from individuals in order to outsource all or part of an activity that was previously done in-house, particularly given the rapid pace of technology.

Of course, the consent burden will be much more strongly felt by SMEs than by large domestic Canadian organizations. Limiting the requirement to transborder outsourcing will not resolve the problem. SMEs must have the same opportunities as other organizations to access economies of scale offered by larger international service providers. Ironically, a rule that limited the requirement to Canadian organizations transferring information across borders would result in a greater burden for Canadian organizations than foreign organizations. No special consent would be required when a U.S. based organization collects information, since the transfer of their data across borders will be obvious and will occur from the outset.

We anticipate that your Office might attempt to stretch cl. 4.3.3 to argue that organizations cannot condition a service on obtaining consent to outsourcing. Clause 4.3.3 states that an organization cannot "*require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes*." However, this would involve individuals having the right to dictate the business models that

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

organizations use and would be a departure from the oft-touted technological neutrality of PIPEDA. For example, can an internet-based retail business be forced to become a mail-order business? Can a federal work that uses an outsourced payroll provider be forced to cut cheques by hand? To your Office's credit, this issue was recognized in the original consultation document: "*a transfer for processing may well be integral to the delivery of a service and in such cases, organizations are not obligated to provide an alternative*." However, will you, as the Commissioner, become the arbiter of business models to determine what is and what is not integral to the delivery of a service? This type of outcome seems to fly in the face of the Supreme Court of Canada's admonition not to give undue preference to privacy over business interests.

In our view your Office's new position will ultimately add nothing for individuals but increases risk and compliance burdens for organizations, particularly SMEs who can be expected to rely heavily on third party service providers.

By contrast, the canonical position, as aptly stated by Perrin, Black, *et al.* and incorporated into the 2009 Guidelines, achieves the purpose of PIPEDA without unduly prioritizing privacy over legitimate business interests.

Organizations must be accountable and remain accountable for personal information transferred to third party processors. The uses for which the personal information is processed must remain those for which the individual consented. In the case of transfers across borders, the sensitive consumer is accommodated with transparency, although in a globalized economy, such transfers are a "fact of life". Indeed, if anything, since 2009, such transfers are more prevalent and even the disclosure requirement seems antiquated. It would be much more surprising for an organization to say that they did not transfer information across borders or engage in outsourcing than it would be to say that they do!

While all organizations, including SMEs, must take measures to ensure personal information being processed by third parties is protected, the canonical approach produces an even playing field among organizations that are able to keep processing entirely in-house and those that rely on outsourcing and the globalized economy to achieve economies of scale that they could not otherwise achieve. And, if you will permit us the extreme example, all businesses can use and profit from the internet and the modern advent of cloud computing without organizations having to obtain fresh consent every time they change their method of processing or wonder whether your office might second-guess whether the third-party processing is really "integral" to the offering or whether they will need to litigate the issue with you.

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6

5. Summary

In conclusion, our submission can be summarized as follows:

- The term "disclose" in PIPEDA is used in the context of making information available to a third party other than when the third party is an extension of the disclosing party (e.g. a processor).
- Interpreting transfers for processing as disclosures leads to the absurd result that there are greater barriers for outsourcing activities than business transactions.
- Rather, the generally accepted interpretation at the time PIPEDA was enacted and when it was amended in 2015 is that a transfer for processing is not a disclosure.
- This canonical interpretation is supported by the plain wording of cl. 4.1.3, which treats the personal information as remaining within the custody and possession of the outsourcing organization.
- To the extent that there is any ambiguity, the genesis of PIPEDA allows for flexibility, common sense and pragmatism in its interpretation.
- Providing individuals with a right to consent to outsourcing (whether outsourcing is characterized as a "use" or "disclosure") will be a chimerical right that imposes burdens on organizations that are unwarranted given the accountability principle in cl. 4.1 (generally) and 4.1.3 (specifically).

251 Laurier Avenue West Suite 900
Ottawa ON K1P 5J6