August 6, 2019

Submission in response to Consultation on transfers for processing

This note is respectfully submitted by Borden Ladner Gervais LLP in response to the call for comments issued by the Office of the Privacy Commissioner of Canada (OPC) in its *Consultation on transfers for processing – Reframed discussion document* dated June 11, 2019 (the Consultation), which reframed its original *Consultation on transborder dataflows* dated April 9 and updated on April 23, 2019 (the Initial Consultation). Our submission incorporates the positions and concerns of our clients, who operate businesses in various industries that are impacted by the present Consultation.

INTRODUCTION

In the Consultation, the OPC indicates that it is revisiting its position regarding cross-border data flows under PIPEDA, which were detailed in its *2009 Guidelines for processing personal data across borders* (the 2009 Guidelines).[1]

Under PIPEDA, the transfer of personal information from one organization to another is generally considered a "communication" or "disclosure" that requires the consent of the individual concerned, even if the two organizations are affiliated. However, PIPEDA recognizes an exception known as the "service provider (or agency) exception", which treats transfers of personal information to an agent or service provider for the purposes of processing as a use, not a disclosure, by the transferring organization. This "use" does not require further consent of the individual concerned if specific conditions are met[2] such as using contractual or other means to ensure that service providers "provide a comparable level of protection while the information is being processed" by them.

The 2009 Guidelines confirmed past practices and distinguished between a "transfer" and a "disclosure", making it clear that the transfer to another organization for processing was a mere "use" of the information, which does not require the concerned individual's consent since said information cannot be used by the processor for purposes other than the one(s) for which it was collected. Before transferring personal information outside of Canada, whether or not such transfer would constitute a "disclosure", the legal requirement has always been one of openness, *i.e.* simply notifying individuals of the cross-border transfer via the privacy policy.[3] Parliament has not indicated any disagreement with the OPC's long-standing interpretation of PIPEDA.[4]

---

[1] OPC, Guidelines for Processing Personal Data Across Borders, January 2009: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

[2] Clause 4.1 of Schedule 1 PIPEDA.

[3] 2009 Guidelines. See also See also OPC, PIPEDA Case Summary #394 - Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers; OPC, PIPEDA Case Summary #2007-365, Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered and OPC, PIPEDA Case Summary #313 - Bank's notification to customers triggers PATRIOT Act concerns.

[4] When Parliament enacted PIPEDA, Parliament could have followed the approach taken by the *European Union Directive 95/46* and imposed restrictions on cross-border data transfers, but Parliament did not do so.

In the Consultation, the OPC now takes the position that consent from individuals is required prior to any transfer of their personal information across a provincial or national border, including for mere processing purposes. For the reasons detailed below, we respectfully submit that the revised position be reconsidered by the OPC. Our reasoning is detailed in response to the questions asked by the OPC in the Consultation. Please note that we have not provided responses for questions 1 through 3 of the Consultation and have only addressed the questions that were included in the Initial Consultation as we are focusing our comments on PIPEDA as it is currently in effect.

RESPONSES – to the questions asked by the OPC in the Consultation

1. **In your view, does the principle of consent apply to the transfer of personal information to a third party for processing, including transborder transfers? If not, why is the reasoning outlined above incorrect?**

No. PIPEDA incorporates the principles of Fair Information Practices and was conceived, drafted and amended by Parliament as a principle based ("soft law") and technology-neutral law.[5] When adopting the Act in 2001, the legislator deliberately decided not to follow the European Directive[6] model – which restricted transfers outside of the EEA since 1996 – and did not include any restriction to transborder transfers. To the best of our knowledge, neither the Parliament nor the Canadian government has ever indicated that it will support such a restriction pertaining to private organizations' activities. Canada being a federation, in which PIPEDA applies unless a substantially similar provincial law is adopted, means that personal information should be able to flow from one province to the other without restriction. Since privacy requirements are harmonized across the country, a requirement applicable to interprovincial transfers appears to contradict the very purpose of our legislative framework.

We understand from our clients that this position is in line with the inherent openness of the Canadian economy, which depends heavily on the free inbound and outbound flow of goods and services, including data. Restricting such flows by imposing consent requirements for organizations' operations would amount to localization requirements that would be detrimental to the Canadian economy and Canadians.

In 2019, it is not unreasonable for individuals to expect that their personal information will be processed outside of their province or country of residence. They regularly access foreign websites, use credit cards to pay for their daily transactions, use social media, stream digital content, access their pay stubs online, book flights and hotels… all of which require that their personal information be processed by one or several providers located outside of Canada.[7] They also expect the organization they are transacting with to safeguard such information, including when it is in the hands of a third party processor, and will hold that third party processor accountable for that information.

---

[5] See section 1.1 "The Historical Background Leading to Laws Protection Personal Information" from Eloïse Gratton, Understanding Personal Information: Managing Privacy Risks, LexisNexis, 2013.

[6] Directive 95/46 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 the free movement of such data.

[7] Indeed the vast majority of this electronic activity is performed using devices whose diagnostics are remotely monitored and updated by offshore manufacturers.

In the context of a transfer to a third party for processing, the purposes for which the information is used are not modified: the organization in control retains the services of the third party processor to accomplish certain tasks on its behalf and must, by virtue of the Accountability Principle, ensure that such third party cannot use the information for other purposes.

As reminded by the OPC in its *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act:*

> (…) in the current digital ecosystem, it is no longer fair to ask consumers to shoulder all of the responsibility of having to deconstruct complex data flows in order to make an informed choice about whether or not to provide consent. Autonomy is very important but, given the complexity of the environment, there is a strong role for regulators who have the expertise to enhance privacy protection through education and proactive enforcement. Organizations too must be transparent about their practices and respectful of individuals' right to make privacy choices. [emphasis added]

This statement echoes the WP29 *Guidelines on Consent under Regulation 2016/679*, which holds that where individuals do not have an actual control and are not offered a genuine choice with regard to accepting or declining the terms offered to them, consent becomes illusory.[8]

Consent fatigue is also a clear indicator that individuals tend to consent to practices without understanding them or taking the time to review privacy policies, making meaningful consent an empty promise in many instances. This is particularly striking in relation to cookie banners, where most users do not take any action or simply click "accept" without reviewing the related policy.

All of the organizations we are working with employ several processors to conduct their operations. They use these service providers out of necessity since most organizations today do not necessarily have the capacity, resources, infrastructure or skills to handle all of their operations internally. Many organizations rely on cloud service providers and platforms to increase the quality of the services they provide to their customers and employees, and to ensure the security and availability of the data they are accountable for. These providers increasingly obtain stringent security certifications (such as ISO 27001 or PCI-DSS standards), notwithstanding the jurisdiction where they are located. Services offered by these third parties are core to their activities and involve the negotiation of detailed contractual safeguards aimed at ensuring that they will protect the information at all times and will not use it for any purpose other than the ones allowed by the organization in control.

We therefore submit that existing openness/transparency requirements, when combined with the principles of accountability, data minimization and security safeguards, do not need to be bolstered by a new consent restriction regarding transborder flows of information, which individuals do expect in the connected world they live in. As discussed below, imposing consent requirements on such flows would be

[8] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

impossible to implement in practice without dramatically impacting the Canadian economy and Canadian consumers.

2. **Does Principle 4.1.3 affect the interpretation or scope of the principle of consent? If so, what is the legal basis or grounds for this interpretation?**

Yes. The Accountability Principle is central to PIPEDA and ensures that organizations interacting directly with individuals are responsible for ensuring compliance with its requirements. Responsibilities associated with this principle were recently clarified by the OPC in its guidance regarding privacy breach reporting, notification and record-keeping obligations. In that guidance, the OPC clarifies that the organization "in control" of personal information is primarily responsible for that information, although service providers are also subject to many of PIPEDA's requirements, such as with respect to providing adequate safeguards for information that they are processing.

This understanding is similar to the framework adopted in other modern privacy legislations around the world, including the GDPR, which makes controllers accountable for compliance with data protection requirements[9] or even the upcoming California Consumer Privacy Act in California which copies the GDPR approach of requiring certain contractual language with third party processors.[10] By contrast, processors must comply with controller's instructions, must protect the information and assist the controller in demonstrating compliance. A processor that would use the information for its own purposes loses its processor status and is considered a controller.[11]

The reason for this dichotomy is that individuals interact with organizations "in control", not processors. To be efficiently protected, individuals must be able to rely on said organizations' compliance with privacy requirements and should not be asked to verify whether the service providers used by such organization are themselves compliant or located in a given country with adequate privacy legislation. If an individual's privacy rights are infringed, individuals should be able to seek remedies from the organization with whom they are contracting.

Asking individuals for their meaningful consent to a processing-related transfer would in turn require them to verify the location of processors before interacting with a website or an app or obtaining a service. Efforts associated with such verification would be unreasonably heavy. We can think of the challenge in determining where the consent train stop, for instance whether it extends to software/hardware manufacturers or even subcontractors of processors. This would shift the burden of responsibility to the individuals, thereby altering the Accountability requirement. We also want to point out that there are no meaningful benefits associated with such increased burdens on consumers. In the case of a misuse of personal information by a processor located abroad, organizations could indeed argue that since the concerned individuals have consented to such transfer, they have accepted the risks associated therewith and should seek reparation directly from the infringing processor. Such logic appears to contradict the very intent of consent requirements under PIPEDA by removing responsibility from controllers.

---

[9] GDPR, art.24

[10] California Consumer Privacy Act of 2018, CAL. CIV. CODE §1798.140 (v) and (w).

[11] GDPR, art. 28.10

3. **What should be the scope of the consent requirements in the Act in light of the objective of Part 1 of PIPEDA as set out in section 3, the new section 6.1 (and its reference to the nature, purpose and consequences of a disclosure), and the OPC's Guidelines for obtaining meaningful consent, in force since January 1 2019? Specifically:**

   a. **In what circumstances should consent be implicit or explicit?**

      Transfers for processing should not trigger any separate consent requirement since such transfers are a necessary component of the process relied upon by the organization to accomplish the purposes for which it has obtained consent from individuals. What matters is that individuals are made aware that their personal information will be used by an organization to achieve specific purposes and that that organization will protect the information at all times in accordance with PIPEDA.

      - **Implicit (implied) consent**: In accordance with the *Guidelines for Obtaining Meaningful Consent*, when an organization in control transfers personal information to a third party for the mere purpose of processing, it should be allowed to rely on the individual's implied consent. Such implied consent is obtained by including a clear indication in the organization's privacy policy that it relies on third parties located outside of Canada to process personal information and making that privacy policy readily available. Consent should be implied as long as the service provider only processes the information on behalf of the organization in control and not for its own purposes or for the purposes pursued by another third party.

      - **Explicit consent**: Explicit consent should only be obtained when information is transferred to a service provider that is granted the right to use same for its own purposes or for the purposes of another third party. Such explicit consent can be obtained in different ways, for example by way of a clear statement in the privacy policy and requiring individuals to positively confirm their agreement thereto or by any other contractual acceptance mechanism.

   b. **What should be the level of detail in the information given to the person affected? Do you agree that consent should be comprised of at least the following elements: (i) the purposes for which the responsible organization seeks to use the personal information, (ii) the fact that it uses third parties for processing but that it provides for a comparable degree of protection, (iii) when the third parties are outside of Canada, the countries where the personal information will be sent, (iv) the risk that the courts, law enforcement and national security authorities in those countries may access the personal information?**

      The information conveyed to individuals should only include key elements[12] that are relevant for individuals to make an informed decision about whether or not they want to interact with a given organization. Such information should include the purposes for which the organization seeks to use the information. The fact that it relies on third parties to process such information and

[12] On this issue, see item 1 of the OPC *Guidelines for meaningful consent*, May 2018.

requires those third parties to provide a comparable level of protection is already included in the law and does not need to be repeated, as this would lead to information overload for individuals and therefore not achieve any additional protection.

Many clients surveyed mentioned that such a requirement would be completely impractical in the cloud era, where information can be processed in multiple countries despite the fact that the processor is established in a given jurisdiction. It is also important to take into account that the processors relied upon by organizations may change frequently. We note that under the Quebec ARPPIPS, organizations have been required since 1993 to disclose the "place where the file will be kept"[13] and that this provision has never been enforced.

With respect to the information being accessible by courts, law enforcement and national security authorities in other countries, such an indication should be included in the privacy policy to ensure individuals understand the implications of their information being transferred abroad.

To avoid information overload and in accordance with the model adopted by PIPEDA, organizations should be required to comply with the *Guidelines for Obtaining Meaningful Consent* and be accountable for ensuring that they only transfer personal information to third party processors that can provide a level of security comparable to PIPEDA requirements.

c. Should the notice to the affected person name the third parties?

A requirement to name third party processors in a privacy notice would be unnecessary and impossible to implement in practice given the accountability placed on the organizations in control of the data, the number of processors involved and the frequency at which they may change. However, individuals should be advised of transfers to third parties who can use their personal information for their own purposes, i.e. those transfers that qualify as "disclosures" such as to organizations that may use information for their own online advertising purposes.

d. Should the notice contain other pieces of information?

No. The *Guidelines for Obtaining Meaningful Consent* require organizations to be sufficiently transparent and provide adequate notice to enable individuals to confidently make decisions about how and for what purpose their information is being used. These *Guidelines* ensure that organizations are transparent about the purposes for which they are using personal information and whether personal information will be transferred cross-border.

4. Since the 2009 Guidelines already require that consumers be informed of transborder transfers of personal information, and of the risk that local authorities will have access to information (preferably at the time it is collected), at a practical level, would elevating these elements to a legal requirement for meaningful consent significantly impact organizations? If so, how?

[13] An *Act respecting the protection of personal information in the public sector* (Quebec), c.P-39.1

Yes. For the reasons mentioned above, requiring organizations to obtain meaningful consent for processing-related transfers is impractical. Requiring consent implies that such consent can be withdrawn: therefore, this requirement in relation to transfers for processing would create confusion in the minds of individuals who may wrongly understand that they have an option to refuse such transfers when those are required by organizations as a condition of service.

As highlighted in the *Guidelines for Obtaining Meaningful Consent*, what is key is for individuals to have the option to say yes or no to secondary uses, i.e. uses that go beyond what is necessary to provide the product or service, whether those involve a transfer of information abroad or not.

Specifically, this elevated requirement would impact numerous industries, including business process outsourcing service providers (BPO Service Providers) who perform various administrative and ancillary tasks related to the operations of organizations in control (such as payroll, benefit administration, IT support): requiring meaningful consent from concerned individuals (such as employees or users) for the transborder transfer of their information to the service provider would be impractical and lead to them having to internalize those business processes and related resources in order to serve individuals who do not consent to the transfer. This will put organizations in an impossible position since they will not only be unable to transfer information to third parties for processing, but may not be able to provide these services since many do not have the internal resources, expertise, infrastructure and capabilities to do so. Not being able to use BPO Service Providers will also be highly detrimental to most organizations, who, unlike those BPO Service Providers, may not have the same means to invest in the necessary privacy and security safeguards for such processes.

Canadian companies engaged in e-commerce activities often rely on offshore fulfillment centres with a chain of shipping partners to get the goods to the consumer. The path of information sharing in that limited instance is not always known ahead of time, so theoretically requiring meaningful consent at each stage (to the extent it requires identification of the carrier) would add several pinch points for the cross-border flow of commerce. The elevated requirements would not apply to foreign e-commerce retailers and would disadvantage the Canadian economy as a result.

5. **If the elements identified in question 6(b) were required conditions for meaningful consent under a new OPC statement of principle, what steps should the OPC take to address the needs of organizations to collect, use, and disclose personal information?**

The OPC should create an exemption to such requirement for transfers made to affiliates and third party service providers who are merely processing personal information on behalf of an organization in control, since the organization in control will remain the entity accountable for PIPEDA compliance towards the OPC and concerned individuals. The OPC could require organizations to include a separate section in their privacy policies notifying individuals about transborder transfers. For example, the title of the relevant section could include the words “cross-border transfer” in order to ensure adequate transparency for consumers that are interested to know about the cross-border transfer of their information, so that they can quickly and easily access this information.

6. **What elements should be included in obtaining consent for transfers for processing that are not transborder?**

No consent should be required for transfers for processing data in accordance with the purposes for which consent was provided, whether these transfers are transborder or not.

7. **Do you think the proposed interpretation of PIPEDA is consistent with Canada's obligations under its international trade agreements? If not, why would the result be different from the current situation, where the elements identified in question 6(b) must disclosed as part of the openness principle?**

A consent requirement would be contrary to Canada's international obligations. Specifically, the United States-Mexico-Canada Agreement (USMCA), which was signed on November 30, 2019 to replace NAFTA, generally prohibits restricting cross-border transfers of personal information between the U.S., Canada and Mexico. It only allows such restrictions if they are necessary to achieve a "legitimate public policy objective".[14] The Canadian government has taken the position that data localization requirements are only acceptable for data held by the government or on its behalf by third parties under contract and has never supported any other restriction.

The interpretive presumption of conformity calls on administrative officials and courts to interpret domestic law in a manner that respects Canada's international legal obligations.[15] Accordingly, the OPC must interpret PIPEDA in compliance with USMCA's principle of prohibiting data localization, subject to the Federal government identifying that such requirements are necessary with regards to credit information to achieve a legitimate public policy objective. As of the date of this submission, no such intention by the Federal government has been issued or announced.

This interpretation is supported by Article 19.8 (6) USMCA, which specifically states that the parties "recognize that the APEC Cross-Border Privacy Rules system - to which both Canada and the US are parties - is a valid mechanism to facilitate cross-border information transfers while protecting personal information." It may therefore be possible for Canada to require compliance with the APEC CBPR system for cross-border data transfers. At this point however, such requirement has not been issued.

As such, we respectfully submit that a requirement to obtain consent regarding transfers for processing would constitute a violation of Canada's obligations under the USMCA.

8. **Any other comments or feedback you think may be helpful.**

---

[14] Article 19.11, USMCA: "1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person. 2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.5 5. A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party."

[15] Canadian Foundation for Children, Youth and the Law v. Canada (A.G.), 2004 SCC 4, [2004] 1 S.C.R 76, 234 D.L.R. (4th) 257 at para.31 holding that "(…) Statutes should be construed to comply with Canada's international obligations"; cited by Armand de Mestral, Evan Fox-Decent, Rethinking the Relationship between International and Domestic Law, 53 McGill L.J. 573 (2008)

The OPC's revised position amounts to imposing data localization requirements on private sector organizations that are not found in PIPEDA. It is worth noting that such data localization requirements would go beyond what is provided for in the European General Data Protection Regulation (GDPR), which is considered as being the most stringent piece of privacy legislation in the world.

Under the GDPR, once individuals enter into an agreement that involves the processing of their personal data, a transfer of such data to a recipient located outside of an adequate jurisdiction or to an organization located in the U.S. that is not certified under the Privacy Shield framework is only lawful if appropriate safeguards are in place.[16] Such safeguards include entering into an agreement that incorporates standard contractual clauses between the data exporter and the data importer that will ensure an adequate protection of the data. The concerned individuals are only required to provide their explicit consent to the cross-border transfer and be advised of the possible risks of such transfer where adequate safeguards are not in place.[17]

Accordingly, a data transfer agreement between the organization in control and its processor that would impose strict privacy and security obligations on the processor would appear to be sufficiently protective of individuals' rights, even by European standards. Nothing in the legal and economical Canadian ecosystem would justify imposing a more stringent requirement to organizations offering products and services to Canadians.

***

Authors:

Eloïse Gratton
National Co-Leader, Privacy and Data Protection
EGratton@blg.com

Elisa Henry
National Co-Leader, Privacy and Data Protection
EHenry@blg.com

[16] GDPR, art. 46

[17] GDRP, art. 49.1(a)