Centre for Information Policy Leadership
Hunton Andrews Kurth

17 May 2019

Comments by the Centre for Information Policy Leadership on the Office of the Privacy Commissioner of Canada's Consultation on Transborder Dataflows

On April 9, 2019, the Office of the Privacy Commissioner of Canada (OPC) published a public "Consultation on transborder dataflows",[1] seeking feedback from stakeholders by June 4, 2019 on a proposed revised approach to the rules pertaining to the governance of transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA). On April 23, the OPC issued a "Supplementary discussion document"[2] on its Consultation on transborder data flows. The Centre for Information Policy Leadership (CIPL)[3] welcomes the opportunity to submit the comments below.

Comments

The OPC states that its position on transborder transfers has evolved since its 2009 Guidelines for Processing Personal Data Across Borders (2009 Guidelines).[4] It now believes that individuals should be asked for their consent when their personal information will be transferred to foreign jurisdictions, even if only to be processed by third party service providers.

Currently, under the 2009 Guidelines, organizations that transfer personal data from Canada to a service provider in another jurisdiction do not have to obtain consent from individuals. However, they must ensure through contractual or other means that the data continues to be protected at a level that is comparable to the level at which it would be protected should it remain within the organization. Under this model, individual organizations are held accountable for what happens to the personal data they transfer and must ensure that their service providers deliver adequate protection regardless of where they are located.

This accountability-based model has served Canada well. It has cemented Canada's reputation as a pioneer and leader in promoting organizational accountability. It has also been widely regarded as a pragmatic and effective governance model for cross-border data transfers, demonstrating a compelling alternative to more cumbersome approaches that rely on a combination of transfer restrictions and various rationales and mechanisms to get around them.

---

[1] Consultation on transborder dataflows, Office of the Privacy Commissioner of Canada, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

[2] Supplementary discussion document – Consultation on transborder dataflows, Office of the Privacy Commissioner of Canada, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/sup_tbdf_201904/.

[3] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 75 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[4] Guidelines for Processing Personal Data Across Borders, Office of the Privacy Commissioner of Canada, January 2009, available at https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/ (Accessed on 15 May 2019 - please note that this page will be updated by the OPC following the conclusion of the present consultation).

While consent does not fit squarely into these more cumbersome models (as further discussed below), and it may make sense for consent to be a legal basis for transferring data in certain limited circumstances (such as those contemplated by the GDPR), laws should not require consent for all transfers as this will not contribute to better protections or empowerment of individuals with respect to their personal information. Instead, it will introduce an unnecessary obstacle to transborder data flows[5] without countervailing benefits. CIPL strongly recommends against the proposed changes to the OPC's 2009 Guidelines, for the reasons set forth in greater detail below.

I. The OPC's Rationale for Requiring Consent

The OPC points out that under PIPEDA, the consent requirement applies to all collection, use or disclosure of personal data. Since a cross-border transfer involves the "disclosure" of personal data to a third party in a foreign jurisdiction, the OPC argues that consent to cross-border transfers is required as a "matter of law". According to the OPC, nothing in PIPEDA exempts cross-border transfers from the consent requirement. The OPC also supports its argument for consent with the notion that "individuals would generally expect to know whether and where their personal information may be transferred or otherwise disclosed to an organization outside Canada".[6]

However, CIPL believes that:

(1) there is no mandate under PIPEDA to require consent for transfers, whether they be domestic or cross border (if there were, a public consultation on that point would not be warranted);

(2) transparency and consent are two distinct elements. Transparency with respect to cross-border transfers is already required under the 2009 Guidelines, and any lack of transparency should be addressed through separate means, rather than requiring consent;

(3) any problems with the existing accountability-based approach to transfers should be addressed by clarifying, enhancing and/or ensuring proper enforcement of this approach; and

(4) there are several clear factual, policy and legal reasons against this change in interpretation.

II. Reasons for Not Creating a Consent Requirement for Cross-border Transfers

1. Requiring consent does not add protections to individuals

It is not clear how a consent requirement will add any privacy protections to individuals. Firstly, the OPC notes that the current accountability requirements will continue, even where the individual has given his or her consent to the transfer. Under the current "accountability" approach, personal information already has to be protected at the Canadian level. A consent requirement adds nothing to that protection.

---

[5] For a study on the significant positive impact of cross-border data flows on global economic productivity, see "Digital Globalization: The New Era of Global Flows", McKinsey Global Institute, February 2016, available at https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows at page 76.

[6] *Supra* note 1.

Secondly, an individual who does not consent to transfers that are inherent in the transaction or the organization's business model is left with the choice of not doing business with that organization. As the OPC notes, "organizations are free to design their operations to include flows of personal information across borders, but they must respect individuals' right to make that choice for themselves as part of the consent process". Thus, "individuals cannot dictate to an organization that it must design its operations in such a way that their personal information must stay in Canada [. . .], but organizations cannot dictate to individuals that their personal information will cross borders unless, with meaningful information, they consent to this". Significantly, the OPC concludes that "whether this affects [the individual's] decision to enter into a business relationship with an organization or to forego a product or service should be left to the discretion of the individual".

This result is substantially the same as under the 2009 Guidelines, which essentially provide that (a) the fact of a cross-border transfer must be disclosed to individuals and (b) once an individual has chosen to proceed with doing business with the organization, he or she does "not have an additional right to refuse to have their information transferred". In short, it appears that both under the 2009 Guidelines and the current proposal, the individual can chose not to proceed with the transaction based on the information that his or her personal data may be transferred to a foreign jurisdiction, but he or she cannot prevent the transfer from happening and still obtain the product or service. In addition to the general absence of a privacy enhancing choice in this schema, there is the potential for actively undermining privacy protections because cross-border transfers to cloud providers whose core business is to provide a secure environment may actually result in better security than is available domestically. Accordingly, an explicit consent requirement does not increase an individual's privacy protections.

2. Any existing problems could be addressed by strengthening organizational accountability

It is also not clear from the original consultation document or the supplementary discussion document whether the OPC is reacting to any specific observed insufficiencies of the current accountability-based approach. If there are specific insufficiencies, these insufficiencies should be clearly identified and explained. This, in turn, would enable strengthening the current accountability-based approach. Such strengthening may include (a) clarifying the existing accountability requirements that are designed to ensure continued comparable protection in transfer contexts (for instance transparency,[7] data security, due diligence in selecting processors and service providers, clarifying and enhancing contractual commitments relating to comparable privacy and security such as by requiring consistency with the EU standard contractual clauses and reliance on certifications (such as APEC Cross-Border Privacy Rules)), (b) instituting policies and incentives that would increase organizational accountability among Canadian organizations, and (c) enforcement of the relevant accountability measures.[8]

[7] It seems that the OPC's proposal is conflating transparency with consent in its present consultation in that the principal purpose of the new consent requirement would be to demonstrate that individuals have been made aware of the cross-border transfers. To the extent there is evidence for flaws in the current approach to transparency on this point, the remedy would appear to involve clarifying the transparency requirements.

[8] See CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society," 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability," 23 July 2018, available at

3. Requiring explicit consent would be burdensome both for individuals and businesses, confuse individuals and reduce privacy protections

The problems associated with over-reliance on consent are widely known and discussed in detail elsewhere[9] and don't have to be elaborated here. Given these problems and the resulting consent fatigue among individuals, adding yet another consent requirement where none is needed will further aggravate the problems. Under the 2009 Guidelines, individuals already receive information about the fact of cross-border transfers and already are able to stop any transactions with the business if they do not want their personal information transferred. The only new element would be to make consent explicit in some contexts, but without any difference in outcome for the individual. To the extent there is a marginal benefit associated with this change, it is outweighed by significant downsides, including the following:

- Asking for consent for all cross-border transfers is confusing to individuals. Requiring this type of consent could mislead people to think that there might be something inherently risky or wrong with such transfers. Given the realities of the modern global digital economy where such transfers are commonplace, routine and necessary, this is the wrong message to send to individuals. The OPC itself even notes in the section on "What Should Individuals Expect" in the 2009 Guidelines that individuals should "[r]ecognize that transborder flows of information are a fact of life and are very common". It is likely that in the 10 years since then, individuals' awareness of global interconnectedness and data flows has only increased.

- Asking for consent obfuscates the fact that an organization already has a separate and clear legal obligation to protect the personal data essentially at the Canadian level regardless of whether it remains in Canada or moves to another jurisdiction.

- Given how much personal data is routinely transferred across borders in the modern digital and global economy, being asked to consent to every transfer dramatically increases the number of consent requests. This would further burden individuals and have the effect of diluting and undermining the effectiveness of consent in situations where it would be meaningful.

- Requiring consent for all transfers may result in the unintended consequence of lowering organizations' vigilance vis-à-vis the transferred personal data. For example, it could create the impression that an organization's obligation ends with having obtained consent rather than having complied with the necessary accountability requirements to ensure ongoing comparable protections. In effect, it creates an illusory defense for less than accountable organizations.

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

[9] CIPL White Paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; and CIPL comments on the Article 29 Working Party Guidelines on Consent, 29 January 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf.

- A new consent requirement for transfers would also impose significant burdens on organizations that would have to implement the mechanisms and procedures associated with it and could cause substantial cost and disruption to businesses. In addition, a consent requirement could create disincentives for businesses in Canada – particularly smaller ones – migrating to cloud and other online services. It could force major overhauls of how and where an organization processes personal data, which can have far-reaching impacts, particularly for multinational organizations of all sizes whose global affiliates often combine their processing activities in one jurisdiction, or for smaller Canadian affiliates of larger global companies who typically process their personal information outside of Canada. Businesses whose normal processes rely on transfers to providers in foreign jurisdictions would now face unpredictable and unnecessary failures to consent by Canadian individuals, forcing these businesses to either repatriate entire data sets to Canada (which frequently will be impossible where they are sharing one third party service provider with their international affiliates) or lose Canadian customers and the benefit of using Canadian personal information. This will result in significant negative effects on productivity, efficiency and any number of additional advantages associated with processing operations outside of Canada, including better information security in many cases. Ultimately, this is certain to undermine the global competitiveness of Canadian businesses.

4. The EU General Data Protection Regulation does not provide for consent in the context of cross-border transfers

Even the EU General Data Protection Regulation (GDPR) enables information transfers without relying on individual consent, save in very narrow circumstances. The OPC's proposal is inconsistent with the GDPR and would also be an outlier among transfer regimes globally.

Under the GDPR, data may be transferred to a third country, or a territory or a sector within a country, or an international organization, that has been found to be "adequate" by the EU Commission. Alternatively, the GDPR provides for a number of "appropriate safeguards" which, if applied by an organization, legitimize cross-border information transfers, some of which correspond to the steps a Canadian organization currently would have to take to ensure the ongoing protection of information at a "comparable" level when it is transferred to another country.

Only in cases where the transfer is not pursuant to an adequacy finding, or where there are no appropriate safeguards available, and the individual has been informed of the possible risks of the transfer in light of the absence of adequacy or safeguards, does the GDPR allow for explicit consent as a basis for transfer. Indeed, the European Data Protection Board (EDPB) has noted that it expects companies to interpret the derogations (including consent) from the general transfer mechanisms narrowly.[10] Accordingly, consent is rarely used as a transfer basis under the GDPR. Thus, the GDPR models an approach that does not rely on consent as a legitimizing tool for cross-border transfers that are subject to other safeguards to ensure ongoing comparable protection for personal information. However, a scenario in which no appropriate safeguards are available is not the ostensible scenario for which the OPC seeks to introduce consent. Rather, the OPC seeks to introduce consent comprehensively with respect to all transfer contexts, putting it at odds with the GDPR.

[10] See EDPB Guidelines on Derogations of Article 49 of the GDPR, 25 May 2018, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf at page 4.

5. Requiring consent is inconsistent with the APEC Privacy Framework and the APEC Cross-Border Privacy Rules

Canada is part of APEC, has helped develop and endorsed the APEC Privacy Framework (Framework), and has helped develop and joined the APEC Cross-Border Privacy Rules (CBPR) system. In addition, the OPC is a participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA), whose principal purpose is to enable backstop enforcement of the CBPR by Privacy Enforcement Authorities in the participating APEC economies.

One of the core objectives of the APEC Privacy Framework is to ensure the free flow of data in the Asia-Pacific region and to promote "effective privacy protections that avoid barriers to information flows".[11] The Framework specifically calls out the role of the CBPR in furthering both privacy and maintaining information flows among APEC economies and with their trading partners, as well as in encouraging organizational accountability with respect to personal information.[12] Indeed, one of the foundational premises of the Framework was to create "conditions, in which information can flow safely and accountably, for instance through the use of the CBPR system". According to the Framework, the CBPR system was created so that "individuals may trust that the privacy of their personal information is protected" no matter where it flows.[13]

An APEC Privacy Framework[14] section specifically on cross-border transfers provides as follows:

> *69. A member economy should refrain from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.*
>
> *70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.*

Further, it is noteworthy (but not surprising) that the program requirements of the CBPR do not provide for choice or individual consent with respect to cross-border data transfers. Such an option would be

[11] See, for example, APEC Privacy Framework at Foreword and Preamble, paragraph 4, available at https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.
[12] *Id*. at Preamble, section 8.
[13] *Id*. at Part IV, B, III, paragraphs 65 and 67.
[14] *Id*. at Part IV, B, IV paragraphs 69 and 70.

inconsistent with APEC's and the CBPR's premise of providing accountability-based protections to the information regardless of geographic location.[15]

The OPC's proposal to introduce a consent requirement, therefore, is inconsistent with the goals of the Framework and the specific purpose and requirements of the CBPR: to make geographic location of personal information irrelevant because protections should flow with the information regardless of where it goes. Given that under the OPC's current transfer framework sufficient protections and appropriate measures already exist (and could be improved if they didn't), and given that a consent requirement addresses no additional risks nor adds protections, such additional obstacle to cross-border transfers is clearly not proportionate.

While the Framework and the CBPR explicitly do not prohibit domestic privacy protections that go above and beyond what is provided by APEC, implementing a new requirement so at odds with the very premise of the APEC Privacy Framework and the CBPR warrants careful consideration. Our recommendation would be to strengthen the current accountability-based protections for transferred data, including through active implementation and promotion of the CBPR in Canada, rather than introducing a new consent requirement. Part of the promise of the CBPR is to harmonize privacy and data protection practices across the APEC region. This will be one of the principal benefits and incentives for organizations that certify to the CBPR. Any unnecessary national deviation, therefore, has the potential to directly undermine this harmonization benefit and, thus, the relevance and effectiveness of the CBPR in the long run.

6. Requiring consent is inconsistent with the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows

The OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows[16] provides as follows:

> *PART FOUR. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS*
>
> *16. A data controller remains accountable for personal data under its control without regard to the location of the data.*
>
> *17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including*

[15] There is one limited exception to this. The Framework's accountability principle (Part III, principle IX, para. 32 plus Commentary) provides that where personal information in a domestic or international transfer cannot be protected through exercise of due diligence or other reasonable steps, an organization should obtain consent "to assure that the information is being protected consistent with these principles". However, this would not be the context under the CBPR or, importantly, under Canada's current requirement of transferring personal data subject to the appropriate accountability measures that ensure continued protection at the appropriate level. (It is also not clear how consent would assure the information is protected where the transferring organization has no way to protect the information itself).

[16] OECD Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), available at http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

> *effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.*
>
> *18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.*

The OPC's 2009 Guidelines provide for an accountability-based transfer regime that squarely meets the OECD principles set forth in paragraphs 16 and 17 above. However, the OPC's proposal to add a consent requirement is inconsistent with the principles set forth in paragraph 18. Given that the existing accountability-based protections for any transferred personal data will remain in place under the new policy, and given that the proposed consent requirement does not protect individuals from any additional risks that cannot be addressed by the required accountability measures, this new obstacle to cross-border transfers is disproportionate to any risks presented.

7. Requiring consent would undermine Canada's commitments in relevant trade agreements

a. USMCA

On September 30, 2018, the United States, Mexico and Canada (the Parties) announced a new trade agreement (the USMCA). If passed by the Parties' legislatures, the USMCA would, among other things, require the Parties' privacy frameworks to consider 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.[17] It would also formally recognize the APEC CBPRs within the respective legal systems of the Parties.[18] Further, it provides that the Parties should promote "compatibility" between their legal regimes, including through the CBPR.[19] It also states that the Parties "recognize the importance of [. . .] ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented".[20]

CIPL believes that the OPC's proposal to introduce a consent requirement for cross-border transfers runs at cross-purposes with the USMCA in at least two ways:

- it would reduce "compatibility" between the CBPR and Canada's privacy framework in that it creates an additional inconsistency between the two (see discussion above on pages 6 and 7); and
- it would introduce an unnecessary obstacle to cross-border flows of personal information that is neither necessary nor proportionate to any risk presented, given that the personal data that is going to be transferred continues to be protected by the same accountability measures as before and asking for consent adds no additional protections to individuals.

[17] See Article 19.8(2) of the United States-Mexico-Canada Agreement (USMCA), signed 30 November 2018, available at https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.
[18] *Id*. at Article 19.8(6).
[19] *Id*.
[20] *Id*. at Article 19.8(3).

b. Comprehensive and Progressive Agreement for Trans-Pacific Partnership

This agreement, also known as TPP-11,[21] came into effect on December 30, 2018. Its electronic commerce chapter[22] includes commitments that protect the free flow of information across borders and minimize data localization requirements, while protecting Canada's right to protect data for compelling public policy purposes. Similar to the cases of the APEC Privacy Framework, the CBPR and the USMCA, the proposal to add a consent requirement in the cross-border transfer context could run at cross-purposes with commitments set forth in the TPP-11.

c. EU-Canada Comprehensive Economic and Trade Agreement

The EU-Canada Comprehensive Economic and Trade Agreement (CETA)[23] provides in Article 16.4 that "[e]ach Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection relevant of international organisations of which both Parties are a member". As described above, imposing a general consent requirement for transferring personal information across borders would be out of step with such international standards of data protection.

Conclusion

CIPL is grateful for the opportunity to comment on the Office of the Privacy Commissioner of Canada's "Consultation on transborder dataflows" and the "Supplementary discussion document". We look forward to further opportunities for dialogue on cross-border data flows or other privacy and data protection matters.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

[21] Comprehensive and Progressive Agreement for Trans-Pacific Partnership, available at https://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/text-texte/cptpp-ptpgp.aspx?lang=eng.
[22] Consolidated TPP Text – Chapter 14 – Electronic Commerce, available at https://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.
[23] EU-Canada Comprehensive Economic and Trade Agreement, available at http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/.