ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

June 24, 2019
Office of the Privacy Commissioner of Canada
30 Rue Victoria,
Gatineau, Québec, Canada
J8X 4H7

Re: Supplementary Discussion Document – Consultation on Transborder Dataflows

To Whom It May Concern,

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Office of the Privacy Commission of Canada (OPC) request for comment on its draft policy position on transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA).[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington D.C., committed to articulating and advancing a pro-productivity, pro-innovation, and pro-technology public policy agenda that spurs growth, prosperity, and progress.

Data is the lifeblood of the modern global economy. The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well.[2] To that end, ITIF welcomes the OPC's general approach to encourage data flows while still supporting privacy protections for Canadian citizens.

On April 9, 2019, the OPC launched a consultation on transborder data flows under PIPEDA, Canada's general data privacy law for private sector entities, to make changes to its 2009 guidance on this subject.[3] The supplementary document would keep most of the 2009 guidance intact, especially in important areas such as

[1] "Consultation on Transborder Dataflows – Reframed Discussion Document," Office of the Privacy Commission of Canada, April 23, 2019, accessed on June 24, 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.
[2] Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-crossborder-data-flows.pdf.
[3] "Guidelines for Processing Personal Data Across Borders," Office of the Privacy Commission of Canada, January 2009, accessed on June 24, 2019, https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

regulating data processing through the accountability principle. However, the guidance also requires organizations operating in Canada to gain affirmative consent prior to transferring data across borders. This requirement would not only fail to increase the privacy protections of Canadians already achieved through the accountability principle but would also significantly increase compliance costs and reduce data innovation in Canada. OPC should not be seduced by the misguided and costly fallacy that it is the location of data that matters when it comes to privacy. Indeed, there are other transparency mechanisms that OPC can initiate to achieve its goals without resorting to de-facto data localization policies. Getting this right is particularly important for Canada as it seeks to build its global reputation as a location of choice for artificial intelligence (AI) companies, because significant restrictions on cross-border data flows will most definitely harm the competitiveness of the Canadian AI industry.

These comments will address the OPC's accountability principle and its proposed consent requirements for transferring data abroad.

OPC CORRECT TO USE ACCOUNTABILITY PRINCIPLE RATHER THAN ADEQUACY STANDARD

The OPC has taken the right approach to cross-border data flows through its accountability principle. The OPC's 2009 guidelines stated that "in contrast to (the European Union's) state-to-state approach, Canada has, through PIPEDA, chosen an organization-to-organization approach that is not based on the concept of adequacy." Rather than adopt this adequacy standard used by the European Union and others, Canada's accountability principle states that organizations are responsible for the data in its possession or custody, including data transferred to a third-party, and organizations may use contracts or other means to provide an appropriate level of protection.

The accountability principle makes companies doing business in Canada responsible for their own actions and the actions of both their agents and business partners, regardless of where they are located. In other words, Canadian data protections rules apply to the data, regardless of where the data travels. This principle gives companies doing business in Canada a strong incentive to assist their business partners and affiliates outside Canada in adhering to its privacy protections, because the business subject to Canadian data protection law is held accountable for any privacy violations.

This type of approach to data privacy is one that is shared by other nations and international data protection frameworks. For example, the United States also does not have an "adequacy" standard. Instead, companies in the United States must make a risk-based decision about the necessary data protection measures and

safeguards they should implement when processing data outside the country, as they remain legally responsible for the data regardless of where it is processed. Moreover, this policy facilitates interoperability between nations with different data protection laws because data can flow between different nations. ITIF welcomes the OPC's approach to accountability, which reflects the realities of today's global digital economy.

OPC'S PROPOSED CONSENT RULES ARE THINLY-VEILED DATA LOCALIZATION MANDATES

The update to PIPEDA would require organizations subject to the law to obtain consent prior to disclosing personal information across a border.[4] Individuals would be given the opportunity to exercise their legal right to consent to international data flows, regardless of whether these are transfers for processing or other types of disclosures.

However, the location where data is stored and processed has no bearing on the security or privacy of data. Because virtually all companies doing business in Canada have "legal nexus," they are firmly within the OPC's jurisdiction. For example, an international hotel chain that has hotels in Canada is subject to the nation's privacy laws and regulations. As such, the business must comply with those rules whether it stores and processes the data in Canada or abroad. Companies simply cannot escape from complying with PIPEDA by transferring data overseas. Indeed, the law specifically requires organizations to use contractual or other means to "provide a comparable level of protection while the information is being processed by the third party."[5]

Therefore, the change to require consent to transfer data across borders would not improve Canadian's privacy because organizations are equally accountable for the data stored abroad as the data stored domestically.[6] As described above, domestic laws limiting disclosure by third parties apply to Canadian companies, no matter where they store their data. If a company uses a foreign service provider which improperly discloses personal data then that company can and should be held responsible under PIPEDA, and it can in turn pursue action against its foreign service provider to recoup any losses. This forces organizations that collect and share data to consider the challenges that they face in enforcing claims against a foreign service when selecting that service. Therefore, while including this consent mechanism to restrict international data flows may initially sound reasonable on paper, in practice it would not have any effect on the actual privacy protections of individuals' personal data.

---

[4] "Consultation on Transborder Dataflows," Office of the Privacy Commission of Canada.
[5] The Personal Information Protection and Electronic Documents Act, Office of the Privacy Commissioner of Canada, updated February 5, 2019, accessed June 24, 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.
[6] Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

Instead, this policy would, in effect, create de facto data-residency requirements by discouraging companies from sending data beyond Canadian borders, a concept known broadly as "data localization," because only companies storing or processing data abroad would need to obtain consent.[7] As such, this policy represent a barrier to global digital trade by making cross-border data flows more expensive and thus artificially favoring Canadian businesses over foreign ones.

Increasingly, most industries and firms rely on cross-border data flows as part of their core operations and business model.[8] By limiting where organizations can store data, OPC would stand in the way of that positive development and also impose costs on businesses operating in Canada.[9] For example, companies might have to relocate data storage and processing centers to Canada or build duplicate ones domestically. They might also choose to use Canadian cloud computing service providers, even if these providers are more expensive than foreign competitors. These expenses would affect all businesses in Canada, making them less globally competitive. Such barriers also prevent companies from transferring data that is needed for day-to-day activities, which means companies may have to pay for duplicative services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring data-protection officers, or putting in place software and systems to get individuals' or the government's approval to transfer data.[10] Moreover, by limiting consolidation of data across establishments located in multiple nations, this policy limits firms' ability to use data to support research and development and deliver other innovative goods and services.[11]

Rather than restrict data slows, the OPC should rewrite the rule to simply require the disclosure of countries in which an organization stores its data. This is an effective tool for empowering Canadians to understand how their data is protected and what countries it is stored in. This knowledge can enable those citizens to "vote-with-their-feet" by opting not to use a service if they are disinclined to support industries or worry

---

[7] Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," (Information Technology and Innovation Foundation, September 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf

[8] Daniel Castro and Alan McQuinn, " Cross-Border Data Flows Enable Growth in All Industries," (Information Technology and Innovation Foundation, February 24, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries.

[9] Nigel Cory. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

[10] Nigel Corey, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored" (Information Technology and Innovation Foundation, April 1, 2019), https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where.

[11] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), 19-22, http://www2.itif.org/2018-trust-privacy.pdf.

about government control in a specific country. As the OPC noted, "whether this affects their 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."[12] This transparency component can satisfy individuals' right to know where their information is stored, while the accountability principle can satisfy equal privacy protection under PIPEDA—regardless of where information is stored—keeping compliance costs low without erecting trade barriers.

CONCLUSION

The OPC has a history of supporting transnational data flows, which significantly benefit the Canadian economy. While the regulator is in a position to better inform users about how and where their information is being stored, creating barriers to the geolocation of that data will not benefit Canadian privacy, and will instead create undue costs that will be passed along to Canadian consumers. OPC should reassess its position on transborder data flows.

Sincerely,

Robert D. Atkinson
President and Founder, Information Technology and Innovation Foundation

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation

[12] "Consultation on Transborder Dataflows," Office of the Privacy Commission of Canada.