MILLER THOMSON
AVOCATS | LAWYERS

FORWARD TOGETHER

CBA Privacy & Access Law Section

Update on Cross-border Personal Data Transfers

David Krebs, Counsel
Miller Thomson LLP
November 4, 2019

The Subject-Matter

- "Personal Information" "transfers" from Canada to other jurisdictions
- **We are talking about**: Transfers for "processing" – either to affiliates or other 3rd parties acting on behalf of the organization (and doing to the data what the organization contracted them to do)
- **NOT:** Transfers to other parties who then use information for their purposes will be a "disclosure;" not because it went to another jurisdiction, but because the use is a different one from the original purpose.
- Issue – what is the status of a cross- or trans-border transfer under the *Personal Information Protection and Electronic Documents Act* (with consistent use)?
- Starting point – 2009 Guidelines: "Transfer" is a "use," not a "disclosure"

What happened

- Equifax (April 9, 2019) – under the circumstances, “consent” required
- GDPR (May 25, 2018)
- Change in position announced by OPC in April ’19 – call for consultation/feedback
- Digital Charter (May 21, 2019)
- Reframed discussion (May ‘19)
- Consultation period ends (August ‘19)
- Closed (September 23, 2019) – result: status quo

The more things change…

- Upshot – after all the back and forth, things to stay the same as before (I guess…): a “transfer” remains a “use”
- Organizations don’t need to pivot or make any major changes to their policies and business arrangements
- But what have we learned?
  - OPC has decided to back down but did not really concede the academic argument
  - We have a clearer picture of what the OPC’s expectations are (eg what should be in an organization’s privacy policy)
  - The underlying arguments will not go away → potential changes to Canada’s privacy regime signaled in “Digital Strategy”
  - It was all very confusing…

Personal Information Transfers

- Under PIPEDA – by general definition, a “transfer” of data could, arguably, either be a “use” or a “disclosure.”
- A “use” and a “disclosure” are not treated equally under PIPEDA.
- **OPC’s 2009 position was articulated in a Guideline document (2009)**: *"Transfer" is a use by the organization. It is not to be confused with a disclosure.*
- *When an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected. A simple example is the transferring of personal information for the purpose of processing payments to customers. Or to use another example, an internet service provider may transfer personal information to a third party to ensure that technical support is available on a 24/7 basis. Increasingly, organizations outsource processes to third parties. In many cases, this involves the transfer of personal information. In the context of this document, when we refer to outsourcing, we are referring specifically to outsourcing that involves personal information.*
- *A transfer for processing is a "use" of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected,* ***additional consent for the transfer is not required****.”*
- Upshot – if a transfer (additional use) is for same purpose as was explained to individual at time of collection, no consent is required. **But** if information was disclosed, there would be a consent requirement.

April ’19: OPC’s Change in Position

- A high profile data breach involving a US company, Equifax Inc., and its Canadian subsidiary, Equifax Canada Co., along with the coming into force of the European Data Protection Regulation (“**GDPR**”), were driving forces behind the Office of the Privacy Commissioner of Canada’s (the “**OPC**”) decision to review and, potentially, significantly change the manner in which cross-border “transfers” of personal information would be treated under Canadian privacy law.
- Equifax transferred data to its US affiliate, which would be normally considered a “use” without the need for consent. BUT: OPC in in its decision decided that consent was required – triggering the need to alter its position on more general terms.
- April 9, 2019, the OPC signals that it would no longer view a “transfer” of personal information as a “use” but rather as a “disclosure” under Canada’s *Personal Information Protection and Electronic Documents Act* (“**PIPEDA**”), which could potentially impose significant restrictions and additional organizational obligations on cross-border data transfers.
- The OPC commenced a public consultation process on this issue, which was to conclude June 4, 2019.
- As an aside – to even larger extent than before, OPC borrowing concepts and terminology from European law.

OPC's position cont: Consent

- **Transfer requires consent**. "A company that is **disclosing** personal information across a border, including for processing, must obtain consent. Individuals must be given the opportunity to exercise their legal right to consent to disclosures across borders, regardless of **whether these are transfers for processing or other types of disclosures**."
- **Form of Consent**. Under PIPEDA, the **form of consent** required depends on the sensitivity of the information at issue and the individual's reasonable expectations in the circumstances. Underlying the contextual analysis of both sensitivity and reasonable expectations is the risk of harm to the individual. **Where there is a meaningful risk that a residual risk of harm will materialize and will be significant**, consent should be express, not implied.

- **Reasonable expectation**. It is the OPC's view that **individuals would reasonably expect** to be notified if their information was to be disclosed outside of Canada and be subject to the legal regime of another country. 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**.

- **Choices**: Individuals must be informed of any options available to them if they do not wish to have their personal information disclosed across borders. **As we state in our consent guidance, organizations must make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service**. Depending on the circumstances, 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. Nonetheless, by being provided with clear and adequate information about the nature, purpose and consequence of any disclosure of their personal information across borders, individuals will be able to make an informed decision about whether to consent to the disclosure and therefore do business with the organization

Potential Fallout

- Current web privacy policies and other aspects of current privacy programs in general may no longer be adequate to comply with the new approach.
- Procedures and consent mechanisms may need to be altered or implemented to obtain the consent required when engaging in trans-border data transfers to third party service providers as well as to affiliated companies located outside of Canada.
- Supplier and other agreements (e.g. data processing agreements) may require review.
- The additional consent requirements for cross-border data transfers may create unintended trade consequences: the additional consent requirements may be viewed as a non-tariff barrier to trade, given that such additional consent requirements could be regarded as more onerous than those actually required to adhere to local privacy policies.

Reframed Discussion in May, 2019

- Government announces Digital Charter including potential changes to privacy framework.
- OPC had to reframe the discussion
- Meanwhile – negative feedback from business community (and academics as well)
- The OPC is seeking stakeholder input in two main categories, one being with respect to a **future law** and the other with respect to the **present law** and how it should be interpreted. Feedback requested:
- **Additional enforcement powers**: For instance, should a future law require "demonstrable accountability" and give the OPC the ability to "approve standard contractual clauses before they are implemented and, once they are adopted, proactively review their implementation to ensure a comparable level of protection?"
- **Scope of consent**: Questions include whether consent should be implicit or explicit, what level of detail should be required, whether this should include naming third parties, and whether any other information would need to be included.
- **International trade agreements**: Feedback as to whether any of these potential changes would run contrary to Canada's obligations under these agreements.

Lots of Smoke…little fire…

- On September 23, 2019, the Federal Privacy Commissioner ("**OPC"**) confirmed that transborder transfers of personal data will remain a "use" of personal information under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and will not be treated as a "disclosure," which means that the 2009 ***Guidelines for processing personal data across borders*** ("**2009 Guidance**") will remain the governing guidance document in this area.
- "In our view, existing privacy protections are clearly insufficient and we will be making recommendations to strengthen the protections in a future law."
- In making its decision, the Commissioner cited pragmatism and the overwhelmingly critical submissions it received from stakeholders on the topic. The announcement further noted as a reason for this conclusion that PIPEDA will likely be reformed and any changes arising out of this current consultation would likely not be implemented until after such new legislation is in force.

Learnings for Key Elements of a Privacy Policy

- to **be transparent** about personal information handling practices;
- advising customers their **personal information may be sent to another jurisdiction** and that while the information is in another jurisdiction it **may be accessed** by the courts, law enforcement and national security authorities;
- **clarifying the type** of personal information being collected;
- **identifying the parties with whom** personal information is being shared;
- naming the **purposes** underlying all personal information processing; and
- stating any **residual meaningful risk of harm** or other consequences.

- For now, no need to name parties or amend policies when new 3rd parties/jurisdictions are added.

Looking ahead

- How to protect Canadian Personal Information abroad?
- Canadian *GDPR?*
- Model Clauses? Adequacy regimes? Certifications? Something else?

Questions?

FORWARD TOGETHER

MILLER THOMSON

AVOCATS | LAWYERS

MILLERTHOMSON.COM