NORTON ROSE FULBRIGHT

Legal update

OPC reconsiders its approach to cross-border data transfers with the Equifax decision

April 2019
Data protection, privacy and cybersecurity

In a significant recent decision, the Office of the Privacy Commissioner of Canada (OPC) altered the regulatory landscape when moving personal information between affiliated companies and across Canada's border for data processing or storage purposes.

Any organization governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) will have to re-evaluate and likely adjust its approach to such cross-border data transfers, possibly affecting its outsourcing and cloud computing relationships with vendors and related companies. The OPC has also initiated a two-month consultation period with stakeholders concerning this important policy change.

In September 2017, Equifax Inc., the US parent company of Equifax Canada, announced an attacker had accessed the personal information of over 143 million individuals, including approximately 19,000 Canadians. This included social insurance numbers and other sensitive personally identifiable information. The attackers exploited a known vulnerability in May 2017 that Equifax Inc. had failed to patch, and operated undetected within Equifax Inc.'s systems for four months.

An OPC investigation determined the affected Canadians' personal information was collected by Equifax Inc. through obtaining direct-to-consumer products or fraud alerts from Equifax Canada. The security infrastructures of the two affiliated companies were found to be highly integrated. Several of the complainants to the OPC who suffered the loss of their personal information expressed surprise that their personal information was in the US to begin with. It was determined Equifax Inc. provided the underlying products and alerts and had collected such personal information directly itself or from Equifax Canada to do so.

OPC findings

The OPC undertook a wide-ranging investigation to address six related issues. It provided helpful guidance on appropriate practices regarding security safeguards for sensitive information (including system vulnerability management, oversight, network segregation and security standards adherence), personal information retention and destruction, and mitigation measures provided to affected individuals following a loss of personal information. But most importantly, the OPC examined Equifax Canada's and Equifax Inc.'s adherence to PIPEDA's obligations regarding accountability and consent.

Accountability

PIPEDA's core Principle 1 "Accountability" states an organization is responsible for the personal information under its control. PIPEDA's Section 4.1.3 expands on this to state that personal information in an organization's possession or custody includes that which has been transferred to a third party for processing. An organization must use contractual or other means to provide a comparable level of protection while the information is being processed by that third party.

The OPC first determined that even though an affiliated entity, Equifax Inc., is a third-party processor to Equifax Canada, Equifax Canada bore the responsibility to protect Canadians' personal information through appropriate means. For a variety of reasons, the OPC determined it failed to do so, most notably by not having in place an inter-corporate agreement with its affiliate Equifax Inc. concerning the products offered, relying instead on referencing in the privacy policy and terms of use agreement with its customers the possibility of some data processing being done by its affiliate.

Accordingly, at least for personal information crossing Canada's border, the OPC affirms the processes and written agreements that should exist between affiliated organizations regarding the transfer of personal information between them, and an organization should not expect that corporate relationships alone or mere references to them in notifications or online agreements with users, will satisfy those obligations.

Consent

The most consequential aspect of the OPC's report is its assessment of Equifax Canada's adherence to the key Principle 3 "Consent" that requires the individual's knowledge and consent for collecting, using or disclosing personal information, except in limited circumstances. Section 6.1 of PIPEDA elaborates that consent is only valid if it is reasonable to expect that the individual understood the nature, purpose and consequences of such collection, use or disclosure.

Pursuant to previous OPC decisions and prior practice, PIPEDA-governed organizations typically notify individuals, via policy statements or terms of use agreements, where data processing was, or could be, outsourced to a third party outside Canada.

The OPC summarized this directive in its "Processing Personal Data Across Borders: Guidelines" document, and confirmed "transfers" of personal information from an organization to another for processing was a "use" rather than a "disclosure," where no individual consent was required for such transfer in addition to the consent obtained at first "collection," so long as the purpose of the transfer was consistent with the original consent. This approach has facilitated cross-border outsourcing and cloud computing services for organizations. In fact, this was the approach taken by Equifax Canada.

However, for various reasons, the OPC determined the consent obtained by Equifax Canada was invalid in this case and only express consent to the data transfer and processing by an affiliated entity in the US, would be sufficient.

Critically, the OPC acknowledged that its previous guidance cited above would be reconsidered, and regarding data transfers for processing as a "use" of personal information not requiring fresh consent, may instead better be regarded as a "disclosure" not necessarily sheltered by the original consent. With such an approach, the OPC appears to signal that fresh express consent is required prior to an organization transferring personal information to another organization for processing, even if affiliated, across the Canadian border. Applying the consent principle in this context is the subject of the OPC's consultation now underway, given its significance to organizations and their service providers in our highly fluid and integrated digital economy.

Conclusion

All organizations subject to PIPEDA, prior to entering any arrangement that concerns the cross-border transfer of personal information for processing purposes, even to an affiliated entity, should:

- consider obtaining express consent from affected individuals prior to such transfer, following the OPC's guidance provided in the Equifax decision;

- enter into a written agreement with such third-party processor and adopt the numerous safeguards and other practices and processes described in the Equifax decision, and other documents issued by the OPC; and

- monitor the development of the OPC's consultation process to determine if more specific guidance is developed concerning such data transfer and individual consent requirements.

Tony A. Morris

For further information, please contact one of the following lawyers:

> Julie Himo	Montréal	+1 514.847.6017	julie.himo@nortonrosefulbright.com
> Robert L. Percival	Toronto	+1 416.216.4075	robert.percival@nortonrosefulbright.com
> John Cassell	Calgary	+1 403.267.8233	john.cassell@nortonrosefulbright.com
> Tony A. Morris	Calgary	+1 403.267.8187	tony.morris@nortonrosefulbright.com