After Equifax: Canadian business and GDPR-era privacy regulation

AUTHORS

 Molly Reynolds

 Lara Guest

 Shalom Cumbo-Steinmetz

Around 19,000 Canadians were among the over 143 million individuals whose personal information was compromised in the 2017 Equifax privacy breach.

How did Canadian regulators respond to this large and high-profile breach? The Office of the Privacy Commissioner of Canada (OPC) released a report detailing its investigation into Equifax, finding that the credit agency had failed to meet its privacy obligations. The report also marks a significant change in the OPC's position on privacy requirements for Canadian companies with domestic or international practices. It's a move that could not only align Canadian privacy regulation closer to the regulatory framework set out in Europe's GDPR, but render Canada's regime more unfriendly to business transfers of data.

OPC investigation

The OPC determined that the affected personal information of Canadians was collected by Equifax Inc. from Canadian consumers who purchased or received direct-to-consumer products or fraud alerts from Equifax Canada. Equifax Canada's security infrastructure was highly integrated with that of Equifax Inc.

The investigation was broad: the OPC looked at the adequacy of safeguards by Equifax Inc. and Equifax Canada, whether Equifax Canada had adequate accountability for Canadian data processed by Equifax Inc., whether Equifax Canada had obtained valid consent for this processing, and the companies' data destruction practices. The report concluded that both Equifax Inc. and Equifax Canada contravened PIPEDA in a number of respects and recommended improvements.

Importantly, the OPC found the transfer of data from Equifax Canada to Equifax Inc. to be inconsistent with the organizations' obligation to obtain meaningful consent from individuals before disclosing their personal information to a third party. For consent to be valid, individuals must be given clear information about the disclosure, including when the third party is located in another country, and the associated risks.

Data handling

The OPC's evolving position on data transfers shows it is interpreting Canada's privacy law in a manner consistent with Europe's privacy rules, despite no legislative amendments having been proposed to formally align *Personal Information Protection and Electronic Documents Act* (PIPEDA) with General Data Protection Regulation (GDPR).

The findings of the report will have a number of impacts on companies. It means companies now must obtain meaningful consent to disclose personal information to third parties. This includes clearly explaining the nature and purpose of the transfer, whether the recipient processor is located outside Canada, and any alternatives that would allow the customer to continue receiving services without transferring data internationally.

This doesn't mean cross-border data transfers are necessarily prohibited. Rather, depending on the sensitivity of the information, the transparency of the transfer outside Canada, and the availability of domestic alternatives, companies may need to provide a higher level of disclosure to obtain valid consent.

There is now also a regulatory expectation that data transfers among corporate affiliates should be treated like third-party disclosures. Most significantly, this may involve more detailed data processing agreements that impose rigorous privacy and security obligations on the recipient organization—even when the entities are related and subject to comparable internal policies.

Cross-border transfers

While the OPC's decision focused on the transfer of data from Canada to the United States, it will affect all cross-border transfers of information, whether to third parties or within the corporate organizational structure.

Organizations that process personal information about individuals in Canada in other countries have long been advised to include a notice of this practice in their privacy policies, and a statement that the privacy laws in those jurisdictions may differ from those in Canada. This decision indicates the standard will now be higher to obtain meaningful consent to process or store personal data outside Canada.

The existence of a cross-border transfer of information will be a factor the OPC now considers in assessing the validity of consent for the company's handling of the personal information. This is because individuals may not reasonably expect their information to be transferred to another country to provide services they have purchased from a Canadian company. Where the information is sensitive, individuals may also have heightened concerns about the transfer and storage of their personal information in particular countries, such as the United States. Accordingly, organizations should ensure that cross-border transfers of data, risks associated with the transfer, and alternatives to such transfers are clearly communicated to individuals so they can provide valid consent.

This change in position on part of the OPC may have a significant impact on Canadian businesses' data practices. Recognizing this, the OPC has launched a formal consultation process before issuing revised guidance on cross-border data transfers.

Intercompany transfers

Beyond cross-border issues, the OPC's revised position will also impact companies' domestic transfers of personal information for processing purposes. Although transfers of information to vendors (such as payment processors or marketing agencies) will be treated as disclosures rather than uses, the impact may be more significant in relation to intercompany transfers. A transfer of personal information to a corporate affiliate for processing purposes, for example, may have been less stringently documented than vendor arrangements under the previous view that this constitutes an internal use of data.

Even where all affiliates are located in Canada, where the services to be provided by a company will require data processing by a different legal entity, this transfer will be a factor in assessing the level of disclosure and consent required.

The OPC's focus on intercompany transfers suggests another step toward interpreting PIPEDA in line with the GDPR. In particular, we may see data processing agreements reminiscent of EU standard contractual clauses become more routinely used for transfers between Canadian corporate affiliates in order to document the privacy and security obligations of the counterparties.

Canadian businesses will know more as the OPC releases more information about their evolving approach to interpreting Canadian privacy legislation; whether we will continue to see the influence of the GDPR reflected in our own regulatory framework remains to be seen. The OPC's response to Equifax is one more reminder to Canadian businesses of how increasingly critical it is to develop, maintain and evolve privacy (and privacy breach) practices that are not only sound in regulatory compliance, but that are capable of being agile and responsive to changes from regulators or in best practices.