

KEEPIN' IT "REAL": OPC FINDS THAT PIPEDA APPLIES TO FOREIGN-INCORPORATED BUSINESS

Posted on January 15, 2020

Categories: [Insights](#), [Publications](#)

The outcome of a recent Office of the Privacy Commissioner ("OPC") investigation confirms a number of important principles of Canadian privacy law, including that businesses incorporated outside of Canada are not necessarily immune from being required to comply.

The Facts

411 Numbers HK Limited ("411") operates websites allowing the public to search the full name, address or telephone number of individuals residing in Canada and various other countries. Incorporated in Hong Kong, 411's owner and sole employee lives in Quebec.

Because its services are free for users, 411 historically generated revenue through third party website advertising and charging removal fees to those seeking to delete their contact information from the directory. In addition to paying a fee, individuals who wanted to remove their personal information from the website were required to provide 411 with a copy of their passport, driver's license and a utility bill confirming their name and address.

The OPC received a number of complaints about 411, including from a Canadian judge who feared that the publication of his address and telephone number put his family at risk.

The Complaint

The complainant alleged that 411:

- collected, used and disclosed his personal information without his knowledge and consent by posting his information in its online directory;
- used his personal information for the improper purpose of generating revenue through its paid removal service;
- required him to provide more information than was necessary to have his personal information removed from the directory; and
- was unresponsive to his privacy-related inquiries.

411's Position

411 disputed the OPC's jurisdiction to investigate the complaint on the basis that the company was incorporated under Hong Kong law, its servers were located outside of Canada, and it did not procure the contact information listed in the directory from Canadian organizations.

411 also argued that, in any event, the information listed in the online directory was "publicly available", and therefore it was permitted to collect, use and disclose the personal information without individuals' consent.

The OPC's Findings

(a) A Real and Substantial Connection to Canada

PIPEDA [has been found to apply](#) to an organization based abroad where there is a "real and substantial" connection between its activities and Canada.

Relevant factors in determining whether a "real and substantial" connection to Canada exists can include whether a business markets its products or services to Canadians, whether it processes the personal information of Canadians, and whether any misuse or disclosure of personal information would have an impact on Canadians.

Here, the OPC found that, despite being formally incorporated in Hong Kong and having servers located abroad, the fact that 411's operations were carried out in Canada by the company's owner meant any revenues generated by the directory flowed to Canada. This established a real and substantial connection between 411's business and Canada, both in respect of 411's Canadian websites and its other country-specific websites. Accordingly, 411 was required to comply with PIPEDA.

(b) Non-Compliance With PIPEDA

After assuming jurisdiction over 411's activities, the OPC went on to find that 411 failed to comply with PIPEDA in several respects.

Organizations by and large require the knowledge and consent of an individual for the collection, use or disclosure of their personal information. Principled exceptions to this consent requirement exist, including with respect to "publicly available information", which is defined quite narrowly in the Regulations to PIPEDA^[1] as including only specific classes of personal information. Though the OPC partially accepted 411's argument that contact information listed in the directory of telecommunications companies did constitute "publicly available" information within the meaning of the Regulations, it found that this exception did not apply to unlisted telephone numbers.

411 obtained the contact information for its databases from three foreign-based companies without asking how these organizations obtained the personal information in question. The OPC found that 411 ought to have exercised due diligence to ensure that its databases did not include unlisted phone numbers, including by entering into agreements with its third-party suppliers to ensure that such information was not included in the listings obtained.

During the course of the OPC's investigation, 411 stopped charging individuals and requiring them to provide copies of identification in order to remove their personal information from the website. However, the OPC noted that it would have likely considered these practices offside of PIPEDA.

Finally, the OPC was particularly critical of 411's lack of accountability and openness with respect to the complaint and its obligations under Canadian privacy law generally, including its non-responsiveness to the OPC's investigation inquiries, failure to appoint a Chief Privacy Officer or other individual responsible for compliance with PIPEDA, and the posting of an inaccurate privacy policy on its website. The OPC found that this was contrary to several of PIPEDA's requirements, including that an organization designate at least one individual to oversee compliance with PIPEDA, and develop, implement and train staff on policies and procedures to receive and respond to complaints regarding the handling of personal information.

Takeaways for Your Business

An organization having its directing mind in Canada can be sufficient to establish a "real and substantial connection" such that the OPC will assume jurisdiction over a foreign-incorporated entity. Further, the physical location of a host server will not be determinative of whether the OPC assumes jurisdiction. Accordingly, businesses that market their products or services to Canadians, reside or do business in Canada, or use, process, store or otherwise handle the personal information of Canadians are advised to seek advice to understand whether PIPEDA's provisions may apply.

This investigation is also a reminder that an organization cannot shift responsibilities with respect to privacy compliance to its vendors or other third parties. Accordingly, careful vendor management policies and procedures, including appropriate contractual terms, should be negotiated and implemented.

Lastly, these findings emphasize that there is no time like the present to bring your organization into compliance with Canadian privacy laws. The failure to develop and implement an appropriate privacy compliance program – including policies and procedures for handling inquiries and complaints about privacy – not only runs afoul of PIPEDA, but also significantly increases the risk of civil liability flowing from a data breach or other claim or complaint regarding the organization's personal information handling practices.

by Kristen Pennington, Joseph Osborne, Student-at-Law

[1] Regulations Specifying Publicly Available Information, SOR/2001-7.[ps2id id='1' target='']

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2020