CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 445

APRIL 25, 2019

EDITOR: TERRANCE S. CARTER
ASSISTANT EDITORS: NANCY E. CLARIDGE,
RYAN M. PRENDERGAST AND ADRIEL N. CLAYTON

OPC SIGNALS POLICY CHANGE FOR DATA TRANSFERS ACROSS BORDERS

By Esther Shainblum*

A. INTRODUCTION

On April 9, 2019, the Office of the Privacy Commissioner of Canada ("OPC") released the report of its investigation of the 2017 data breach involving Equifax Canada Co. ("Equifax Canada") and its US-based parent company, Equifax Inc. (the "Report").[1] The Report signals a sea change on the part of the OPC with respect to cross-border transfers of personal information – a change that could have significant potential implications for charities and not-for-profits.

The Report also identifies a number of contraventions of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[2] on the part of both Equifax Canada and Equifax Inc. This *Charity & NFP Law Bulletin* provides an overview of the Report and the potential impact on charities and not-for-profits.

B. BACKGROUND

As reported in the September 2017 *Charity & NFP Law Update*, a massive data hacking at Equifax Inc., the credit rating and monitoring company, compromised the personal information of about 143 million

* Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office.

[1] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2019-001, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information* (9 April 2019), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001 ["Report"]. See also Esther Shainblum, "Equifax Breach Demonstrates What Not to Do", *Charity & NFP Law Update* (September 2017), online: http://www.carters.ca/pub/update/charity/17/sep17.pdf#es3.

[2] SC 2000, c 5.

Americans and about 19,000 Canadians.[3] The personal information of Canadians accessed by the hackers included names, addresses, dates of birth and social insurance numbers,[4] placing these individuals at risk of identity theft. The hackers had exploited a flaw in Equifax's computer system – a flaw that Equifax knew about but had not corrected – to gain access to consumers' personal information between May and July 2017. Although Equifax Inc. learned about the breach on July 29, 2017, it did not make it public until September 7, 2017.[5]

The breach and its handling led to complaints filed with the OPC on a number of grounds, including the fact that Canadian consumers did not expect their personal information to be in the US.[6]

C. ISSUES REVIEWED IN THE REPORT

In the Report, the OPC examined a number of issues relating to whether Equifax Inc. and Equifax Canada had complied with various requirements of PIPEDA, including:

- whether the personal information of Canadians held by Equifax Inc. was protected by safeguards appropriate to the sensitivity of the information;

- whether the personal information of Canadians held by Equifax Canada was protected by safeguards appropriate to the sensitivity of the information;

- whether Equifax Canada demonstrated adequate accountability for protecting personal information of Canadians;

- whether there was adequate consent by Canadians for the collection of their personal information by Equifax Inc. and for the disclosure of their personal information to Equifax Inc. by Equifax Canada; and

[3] Esther Shainblum, "Equifax Breach Demonstrates What Not to Do", *Charity & NFP Law Update* (September 2017), online: http://www.carters.ca/pub/update/charity/17/sep17.pdf#es3
[4] Report, *supra* note 1 at paras 1-6, 21, 24.
[5] *Ibid.*
[6] *Ibid* at para 4.

- whether the mitigation measures offered by Equifax Canada were adequate to protect the Canadians affected by the breach from unauthorized use.

In its findings, the OPC examined the two entities' information security practices, policies and activities and determined that both Equifax Inc. and Equifax Canada had contravened these PIPEDA principles. The Report identified a number of deficiencies in both Equifax Inc. and Equifax Canada's privacy and security practices and stated that Equifax Canada suffered from "serious and systemic" issues that it knew about but failed to correct in a timely way.[7]

D. CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

Perhaps the key development emerging from the Report is the OPC's new position on cross-border transfers of personal information. Although the OPC had previously characterized the cross-border transfer of personal information for processing as a "use" requiring notice to consumers but not consent[8], the Report completely alters that position. The OPC concluded that the transfers of personal information from Equifax Canada to Equifax Inc. constituted the "disclosure" of personal information within the meaning of PIPEDA and that Equifax Canada should have obtained express consent.[9]

Acknowledging that this position is a departure from its previous guidances, the OPC found that Equifax Canada had acted in good faith in failing to obtain express consent for its disclosures to Equifax Inc.[10]

The Report also states that individuals should be given choices with respect to the collection, use and disclosure of their personal information, such as, in this case, the choice not to sign up or to obtain free credit reporting by mail, thereby avoiding the collection by and disclosure to Equifax Inc.[11]

The specific context of the Equifax breach should be noted:

---

[7] *Ibid* at para 147.
[8] *Ibid* at para 111. See also Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (last modified 27 January 2009), online: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127; and Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (last modified 27 January 2009), online: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/
[9] Report, *supra* note 1 at paras 101, 107, 110.
[10] *Ibid* at para 111.
[11] *Ibid* at para 109.

- The OPC determined that Equifax Inc. was a third party with respect to Equifax Canada based on a number of considerations, including the fact that Equifax Canada represented itself as a separate entity in its online Privacy Policy and Terms of Use available at the time of the breach.[12]

- The OPC noted in the Report that Canadians purchasing direct-to-consumer products would have been unaware that their personal information was being collected by and disclosed to a third party outside of Canada. Equifax Canada's webpages, its Privacy Policy and its Terms of Use all presented to Canadians that the direct-to-consumer products were being provided by Equifax Canada,[13] when in fact their information was being collected by Equifax Inc. and additional personal information was subsequently being disclosed by Equifax Canada to Equifax Inc. in the United States.[14] Further, in light of those representations, an individual would not reasonably expect their personal information to be collected by or disclosed to Equifax Inc.;[15]

- Large volumes of extremely sensitive information were being collected and disclosed. The OPC pointed out that more robust forms of consent are required for more sensitive information.[16]

However, notwithstanding these fairly unique details, there is no indication in the Report that the OPC's new position turns on the specific context of the case – namely the particular sensitivity of the information and individuals' reasonable expectations. On the contrary, the OPC actually characterizes its new position as an "evolution from previous findings and guidance"[17] and, in its consultation document, discussed below, states that:

> the OPC's view is that transfers for processing, including cross border transfers, require consent as they involve the disclosure of personal information from one organization to another. Naturally, other disclosures between organizations that are not in a controller/processor relationship, including cross border disclosures, also require consent.[18]

[12] *Ibid* at paras 58, 99.
[13] *Ibid* at paras 61 – 63, 65, 66, 68.
[14] *Ibid* at para 108.
[15] *Ibid* at para 107.
[16] *Ibid*.
[17] *Ibid* at n 13.
[18] Office of the Privacy Commissioner of Canada, *Consultation on transborder dataflows* (last modified 29 April 2019) online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/

E. CONSULTATION ON PROCESSING PERSONAL DATA ACROSS BORDERS

The OPC has announced that it is committed to consulting with stakeholders on this change to its position on cross-border transfers of personal information. In its consultation document, the OPC reiterates its position that consent to data transfers is required and that individuals should be able to choose, under PIPEDA, whether their personal information will be disclosed outside Canada.[19] The consultation document outlines various points upon which it is requesting feedback and input from interested parties.[20] The consultation will be open until June 4, 2019.

F. IMPLICATIONS FOR CHARITIES AND NOT-FOR-PROFITS

If the OPC's position as expressed in the Report stands in its present form, it will have significant implications for charities and not-for-profits that are subject to PIPEDA (or that choose to comply with PIPEDA for the reasons outlined in our other publications), including:

- transfers of personal information from a charity or not-for-profit to a third party for processing or for other purposes, including trans-border transfers, would be considered to be a disclosure and consent, possibly express consent, would have to be obtained;

- transfers of personal information from a charity or not-for-profit to an affiliated entity for processing or for other purposes, including trans-border transfers, would be considered to be a disclosure and consent, possibly express consent, would have to be obtained;

- the charity or not-for-profit would have to provide clear information to stakeholders about the nature, purpose and consequences of the planned disclosure or cross-border disclosure, and its associated risks;

- the charity or not-for-profit would have to inform individuals of the options available to them if they do not wish to have their personal information disclosed to the third party;

[19] *Ibid*.
[20] Additional information on the consultation, including a list of questions for stakeholders, is available at: Office of the Privacy Commissioner of Canada, *Supplementary discussion document – Consultation on transborder dataflows* (last modified 23 April 2019) online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/sup_tbdf_201904/

- individuals could elect not to consent to the disclosure and the charity or not-for-profit would have to accommodate their refusal or revocation of consent; and

- the charity or not-for-profit would remain accountable for the personal information that has been disclosed and must have robust written agreements with the third party that set out the roles and responsibilities of each party as well as reporting and oversight arrangements to ensure compliance.

The OPC's new position may therefore impose additional costs as well as rather onerous requirements on organizations subject to PIPEDA.

G. CONCLUSION

Charities and not-for-profits that are subject to PIPEDA, or that choose to comply with PIPEDA, should closely monitor the progress of this issue, as well as the consultation process and may even wish to make a submission to the OPC consultation. Charities and not-for-profits that may use third party processors or that may transfer or disclose personal information to processors or to other third party organizations within or outside of Canada, should re-examine both their privacy policies as well as their respective agreements with those third parties in order to ensure that appropriate accountability, consent and oversight structures are in place.