THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

# Transfers of Information for Processing

**CANADIAN BAR ASSOCIATION**
**PRIVACY AND ACCESS LAW AND CHARITIES AND NOT-FOR-PROFIT LAW SECTIONS**

**August 2019**

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
**tel/tél**. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

## PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access Law and the Charities and Not-for-Profit Law Sections, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the Privacy and Access Law and Charities and Not-for-Profit Law Sections.

# TABLE OF CONTENTS

## Transfers of Information for Processing

# Transfers of Information for Processing

## I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law and Charities and Not-for-Profit Law Sections (CBA Sections) are pleased to comment on the Office of the Privacy Commissioner of Canada's (OPC) current consultation on transfers for processing, a reframed discussion document based on an earlier consultation on transborder transfers.

We are developing a separate submission on how a future law could address transborder data flows in our response to the current Innovation, Science and Economic Development Canada consultation on Digital Charter/PIPEDA. We do not respond to those issues in this submission.

## II. SHORTER TERM – CURRENT LAW

This submission addresses but does not directly follow the questions posed in the consultation document. Those questions focus too much on the issue of consent, when we believe the issues require broader consideration and discussion.

### A. Principle of Consent does not Apply

In our view, the principle of consent does not apply to transfers for processing that are subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). That view is consistent to the time when the Canadian Standards Association (CSA) *Code of Fair Information Practices* was developed as a national standard of Canada by a broad group of stakeholders. It was also when it was first contemplated to include the Code as a Schedule to PIPEDA, and when PIPEDA was subsequently drafted and passed by Parliament. It should not, in our view, be altered now.

#### 1. A transfer is a use, not a disclosure

In its 2009 guidance document, Guidelines on Processing Personal Data Across Borders,[1] the OPC correctly described a transfer, as referred to in the PIPEDA Accountability Principle (cl.

1 (Ottawa: 2009, Privacy Commissioner of Canada).

4.1 of Schedule 1), as a *use* by an organization's processing agent on behalf of the transferor. That should not be confused with a *disclosure* to a third party for the third party's own use. In the current consultation, the OPC suggests that the 2009 interpretation was incorrect and that a transfer is a disclosure even if the recipient organization obtains no rights in the data.

In our view, the proposed new interpretation is unsupported by accepted principles of statutory interpretation, specifically consideration of the context in which the relevant terms are used in PIPEDA and the intentions behind the relevant statutory provisions.[2] It is also inconsistent with the understood and accepted scheme of privacy protection reflected in PIPEDA and other Canadian private sector privacy laws, which originate in the rules in the OECD *Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data*[3] and the EU's 1995 *Data Protection Directive*, and carried forward in the *General Data Protection Regulation* (GDPR). Considered in context and using the plain wording of PIPEDA, transfers and disclosures are distinguishable, and are intentionally used separately and distinctively.

Principle 1, Accountability stipulates and clarifies that an organization is responsible for personal information under its control or possession, including information transferred to a third party for processing. In other words, that information remains within the control and possession of the organization, and that organization is responsible for ensuring that the third party processing the personal information on its behalf protects the information. The term "disclosure" is not used to describe a transfer for processing.

The OPC's 2009 guidance document states that transfers for processing are simply a "use", limited to the purposes for which the information was originally collected. This is similar to how other Canadian privacy statutes, discussed in depth below, address the topic and is consistent with the wording of Principle 1.

A disclosure of personal information under PIPEDA – and under other relevant Canadian privacy laws and international laws such as the GDPR – involves control and possession of information being moved or shared by the organization originally holding it (the "controller" under the GDPR) to or with another organization considered then to have also *collected* the

2 See, Ruth Sullivan, "Statutory Interpretation in the Supreme Court of Canada" (University of Ottawa).

3 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

information (the "controller" or successor "controller").[4] The second organization must have the individual data subject's consent to collect the information directly or indirectly through the disclosing organization having been given consent to disclose the information.[5] The purpose of the consent requirement is to enable the data subject to determine whether they accept the change of control and possession to the second organization. Once disclosed in this manner, the receiving organization (the new "controller" or "co-controller"), having collected the information, becomes subject to all the PIPEDA rules on use and disclosure of that information, as well as the accountability principle.[6] In contrast, a transfer of information for processing under a plain meaning and interpretation of the Accountability Principle does not change control or possession of the information. Control and possession remain within the organization transferring the information.[7]

A "use" of information is an activity by the organization primarily responsible for that information under the Accountability Principle. That principle states that the responsibility includes ensuring adequate protection for the information when the information is transferred to a third party for processing. The transfer is essentially a form of agency relationship where the "agent" does not acquire ownership or control but is simply authorized to perform certain services for the organization. This understanding of the relationship between the organization and its third party processor is supported by a plain reading of clause 4.1.3 of Principle 1. In addition, this characterization of the relationship between an organization and its contracted service providers, or agents, is consistent with

4 Depending on the circumstances, control and possession of the same information may continue also within the disclosing organization. In this case, both the disclosing and the receiving organizations are entitled to use the information for their own purposes.

5 This is other than in the limited situations where the disclosing organization is specifically authorized by PIPEDA to provide the personal information without the knowledge or consent of the data subject (for example, the instances delineated in s. 7(3) of PIPEDA).

6 In most such disclosure transactions, the disclosing entity does not seek to continue any control over the information once received by the receiving organization. However, in some instances where the discloser has a continuing interest in the integrity and security of the information, such as in the health sector where two-way information flows can occur, "data sharing agreements" may be entered into between the organizations, stipulating certain minimum protective standards for both organizations.

7 See also Perrin, Flaherty and Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, mentioned in the OPC document.

and reflected in other Canadian private sector privacy laws[8] and personal health information protection laws.[9] A transfer understood this way is distinct from a "disclosure" under PIPEDA, which implies the transfer of control, possession and responsibility, as described above.

The OPC supports its argument to consider a transfer as a disclosure by referring to the dictionary definition and other privacy legislation. However, rules of statutory interpretation[10] suggest that the meaning must be derived in the context in which terms are used, not by dictionary definitions read in isolation from that context.[11] Further, other privacy legislation does not provide clear guidance to conclude that, for PIPEDA purposes, a transfer should be considered a disclosure. As discussed below, a transfer is a "use" under most Canadian privacy laws. This is predominantly consistent with the understood application of the transfer for processing rule, as reflected in the OPC's 2009 guidance.[12]

## 2. Inter-jurisdictional Review

It is useful to survey other jurisdictions to determine whether a transfer in this context should be considered a "use" or a "disclosure", and whether consent is required in either situation.

*Europe*

The GDPR offers a uniform approach to "commissioned data processing", which is gathering, processing or use of personal data by a processor in accordance with the instructions of the controller based on a contract.[13] The relevant regulations for processing apply, if processing is connected to activities of any organization in the European Union (EU). It is sufficient if

8 The Alberta *Personal Information Protection Act* expressly includes the terminology, "transfers to a service provider" (s. 13.1 (1)) and has no mention of transfers to a service provider as disclosures not requiring consent, as in the BC PIPA. In other words, the Act considers transfers to service providers outside the scope of a "disclosure", not requiring any special consent exemption. While the BC PIPA does provide an exemption for disclosure, it can be argued that the exemption alone does not exclusively encompass transfers to service providers and that those transfers should be treated as under the Alberta PIPA.

9 See section below on Provincial Health Privacy Laws.

10 *Supra* note 2.

11 Contrary to the OPC document, there is no definition of the term "disclosure" in the *Privacy Act*; the reference in the footnote is to the Treasury Board *Directive on Privacy Practices.*

12 *Supra* note 1.

13 GDPR Processing.

either the controller or the processor operates an establishment in the EU, and processing takes place in the context of its activities.

The GDPR stipulates that notice to data subjects about the processing of their data must include information about the identity of the controller, what kind of data will be processed, how it will be used and the purpose of the processing operations.[14] It does not extend to providing information about contracted processors, or requiring consent to transfer of information to such processors. Similar to PIPEDA, controllers are required to enter into appropriately protective agreements with their processors and remain responsible for information while it is in the custody of processors.[15]

The GDPR provisions on contracting with processors do not address consent by the data subject and do not require it. In sum, the control and responsibility aspect of information held by the controller does not change – the contracted processor relationship is invisible to the data subject.

Under the GDPR rules on transfers of personal information for processing in a country outside the EU, the Commission must have determined that the third country, a territory or one or more specified sectors in that third country, ensures an adequate level of protection.[16] There is no requirement for consent to the transfer.[17]

*Provincial Health Privacy Laws*

Ontario's health privacy legislation, the *Personal Health Information Protection Act, 2004* (PHIPA) has been deemed substantially similar to PIPEDA.[18] The Ontario Information and Privacy Commissioner has recognized that "you can outsource services, but you cannot outsource accountability."[19] However, there is no legislative prohibition on outsourcing, including storing and accessing personal health information (PHI) outside Ontario.[20]

---

14 GDPR Consent.

15 Recital 81; Articles. 24, 28.

16 Transfers on the basis of an adequacy decision.

17 Consent may be basis for transfer under limited circumstances where adequacy status is not available: Article 49(1)(a).

18 Provincial legislation deemed substantially similar to PIPEDA.

19 Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report, June 27, 2012, at 6.

20 PHIPA s. 50(1).

This means that PHIPA does not restrict cross-border transfers of personal information for outsourcing purposes where the custodian remains accountable for the actions of its agent and is satisfied that appropriate administrative, physical and technical safeguards are in place – the primary vehicle being through contractual arrangements. If specific consent is not obtained from the data subject, PHIPA still permits disclosures of PHI to a person outside Ontario in certain situations, including when the person receiving the information performs functions comparable to those of certain persons to whom the disclosure in Ontario is permitted.[21]

The principles that ground and give function to the numerous PHI Acts across Canada are substantially similar, if not identical, to those principles that make up PIPEDA.[22] As with PIPEDA,[23] meaningful consent is a core element of privacy protection across PHI statutes, though Alberta's *Health Information Act* is unique in not requiring consent for legislatively authorized uses of PHI, while still requiring it for disclosures.[24] Currently, only Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia's PHI Acts have been deemed sufficiently similar to PIPEDA for PIPEDA to fully vacate those jurisdictions.[25] They can be used for a comparative analysis. Other Acts may also offer interpretive guidance, given general similarities to PIPEDA. An examination of provincial PHI Acts shows a clear distinction between transfers for processing, which are treated as a continued use of the information in question, and that information's disclosure.

In PHI Acts "[g]enerally, the processing and handling of [PHI] by agents or service providers is not considered 'disclosure'… provided certain conditions are met, principally restrictions on use and access".[26] An illustrative case is how these statutes deal with "agents" or "information managers". Each provincial PHI Act, excluding Ontario's PHIPA, authorizes information custodians to transfer PHI to an "information manager" for processing, storage, or other IT/information management services.[27] Contractual means must protect the PHI

21 PHIPA s. 50(1)(d).

22 *Personal Information Protection and Electronic Documents Act*, SC 2000, cl. 5 [PIPEDA].

23 Bob Zimmer, Chair, Report of the Standing Committee on Access to Information, Privacy and Ethics, *Towards privacy by design: review of the Personal Information Protection and Electronic Documents Act* (Ottawa: House of Commons, 2018) at 20.

24 Michael Power, *The Law of Privacy* (Markham: LexisNexis Canada, 2013) at s. 5.26 [Power].

25 Summary of privacy laws in Canada (last modified 31 Jan 2018).

26 Power, *supra* note 24, s. 7.44.

27 *Ibid*, s. 5.104.

from unauthorized access, disclosure, etc., and limit the PHI's use solely to purposes in the agreement between the custodian and information manager.[28] The parallels between these data protection requirements, which prevent such transfers from being considered disclosures, and those in clause 4.1.3 of Schedule 1 of PIPEDA are clear.[29]

This reading of transfers for processing is consistent with a definition of transfers as a continuation of use, where outsourcing data processing is still a use of that data, provided the originating organization retains significant control (contractually or otherwise) of the information.[30] The canonical view is that a transfer of information only becomes a disclosure when the third party receives the data permanently, to use indefinitely for its own purposes.[31] The presence of this distinction explains what would otherwise be a meaningless use of words in place of "disclosure" (such as "transfer" or "provide") in several PHI statutes.

The OPC's reframed discussion document cites New Brunswick's PHIPAA as legislation that "considers transfers for processing as disclosures".[32] We interpret this differently. That Act permits an information custodian to "provide personal health information to an information manager for the purpose of processing, storing or destroying the personal health information".[33] The word "provide" here contrasts with the Act's deliberate use of the word "disclose" elsewhere throughout, most notably in the sections dealing with consent (sections 18-19).[34] The modern approach to statutory interpretation, guided by the dictum that each word or section be read "harmoniously with the scheme of the Act", holds that the two words must signify different things because *expressio unius est exclusio alterius*, i.e. "the express mention of one thing excludes all others by necessary implication".[35] Further, the New Brunswick Act defines an "agent" as "an information manager… that acts for or on behalf of the custodian in respect of [PHI] for the purposes of the custodian and not for the agent's

28 *Ibid*.

29 PIPEDA, *supra* note 23, Sched 1, s. 4.1.3.

30 Ian Turnbull et al, *Privacy in the Workplace*, 2nd ed (Toronto: CCH, 2009) at 245-46 [Turnbull].

31 *Ibid* at 246.

32 Consultation on transfers for processing: Reframed discussion document (11 June 2019) at 4.

33 *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s. 52(2) [NB PHIPAA].

34 The French version of the statute makes the same distinction, using the verb 'communiquer' in place of 'disclose', and the verb 'fournir' in place of 'provide' in the same sections.

35 Craig Forcese et al, *Public Law: Cases, Commentary, and Analysis*, 3rd ed (Toronto: Emond Montgomery, 2015) at 523-25 [Forcese].

own purposes".[36] Because the agent cannot use the data for their own purposes, a transfer to them is not a disclosure by the traditional delineation based on use purpose.[37] In summary, the New Brunswick Act draws a clear distinction between disclosure of PHI and giving it to a third party for processing.

Ontario's PHIPA is even more explicit in distinguishing the two concepts. Under section 37(2):

> If subsection (1) authorizes a health information custodian to use personal health information for a purpose, the custodian may provide the information to an agent of the custodian who may use it for that purpose on behalf of the custodian.[38]

The Act is clear that "the providing of [PHI] between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information".[39] Here, again, a transfer is not a disclosure if the recipient does not use the information for their own purposes.

A counter argument might be that a transfer for processing/disclosure distinction ceases to apply once information crosses a border. New Brunswick's legislation is ambiguous on this point, but Newfoundland and Labrador's PHIA reaffirms the distinction in a cross-border context. It stipulates that information policies must be in place to protect the confidentiality of PHI "stored or used" in another jurisdiction "or that is to be disclosed… to a person in another jurisdiction",[40] while placing additional requirements on cross-border disclosures relative to storage or use.[41] Of course, PHI cannot be "stored or used" in another jurisdiction if it has not first been transferred across the border. PHIA also authorizes the Lieutenant-Governor in Council to make regulations "prescribing circumstances in which [PHI] may be stored, transferred, used or disclosed outside the province"[42] - wording that clearly indicates cross-border transfer is not automatically a disclosure. Manitoba gives similar authorization.[43]

---

36 NB PHIPAA, *supra* note 33, s 1.

37 Turnbull, *supra* note 30 at 244-45.

38 *Personal Health Information Protection Act*, SO 2004, c. 3, Sched A, s. 37(2) [ON PHIPA].

39 ON PHIPA, *ibid.* s. 6(1).

40 *Personal Health Information Act*, SN 2008, c P-7.01, s 13(2)(c) [NL PHIA].

41 *Ibid*, s. 47(1).

42 *Ibid*, s. 90(1)(n).

43 *Personal Health Information Act*, SM 1997, c 51, s 66(1) [MB PHIA].

Further support for a transfer for processing/disclosure distinction based on the temporariness/permanence of the transfer is in Newfoundland and Labrador's PHIA, New Brunswick's PHIPAA, and Alberta's HIA. Each allows an information custodian to disclose data without the individual's consent when they transfer records to a successor as a result of them ceasing to provide health services in their geographic area.[44] These provisions consider a transfer to be a disclosure when it is permanent, here in the case where a successor is permanently taking over from the original custodian.

Ontario's PHIPA has a similar provision but draws the distinction along a slightly different axis. It holds transfer to be a continuation of the type of use, while disclosure takes place when information is transferred to another party for its own use. It defines a transfer of PHI to a custodian's potential successor, "for the purpose of allowing the potential successor to assess and evaluate the operations of the custodian", as a "disclosure".[45] Information is merely "transferred", however, when the custodian transfers PHI "to the custodian's successor" (i.e. their now confirmed successor), who will use the information to perform the former custodian's duties.[46] When information is transferred for the purpose of being put to the same use, it is not a disclosure, provided safeguards are in place. The transfer becomes a disclosure only when it is to an individual or entity that will potentially put it to a new use.

Notably, Alberta's HIA requires consent for certain disclosures but never for authorized *uses*, some of which, by their nature, require a prior transfer of PHI. As with most PHI Acts, "use" is defined to include "reproducing the information",[47] and the list of permitted uses a custodian may make of individually-identifying PHI includes "determining or verifying the eligibility of an individual to receive a health service"; "providing for health services provider education"; and "for internal management purposes".[48] These purposes cannot likely be achieved without a transfer of PHI to a third party for processing, yet the Act clearly groups them under the category of "use". These purposes are not found in the section that exempts certain disclosures from a consent requirement (section 35(1)).

---

44 NL PHIA, *supra* note 40, s. 39(1)(j); NB PHIPAA *supra* note 33, s. 38(1)(j); *Health Information Act*, RSA 2000, c H-5, s 35(1)(q)(i) [AB HIA].

45 ON PHIPA, *supra* note 38, s. 42(1).

46 *Ibid*, s. 42(2).

47 AB HIA, *supra* note 44, s. 1.

48 *Ibid*, s. 27(1).

Again, the PHI Acts of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia were deemed substantially similar to PIPEDA, so PIPEDA no longer applies in those provinces for health information (while of course still applying to cross-border transfers of PHI).[49] A scan of these and other PHI statutes shows that transfers for processing are treated as "uses" within the scheme of the Acts, in accordance with the OPC's prior recognition of a disclosure/transfer distinction. Reading an Act in its entire context entails looking at other statutes and the principles underlying them,[50] lending support to a reading of PIPEDA as making a similar distinction. Reinterpreting PIPEDA to erase this distinction would require a reinterpretation of the provincial Acts to accord with PIPEDA—with the possibility that they may be deemed no longer substantially similar. That could potentially force amendments to provincial legislation, or even result in reconsideration of the application of PIPEDA to those jurisdictions.

*Provincial Privacy Laws*

In British Columbia, the approach to outsourcing and disclosures outside Canada depends on whether the data controller is a public or private sector organization. All public bodies subject to the *Freedom of Information and Protection of Privacy Act* (FOIPA) are prohibited from the disclosure, storage or access of personal information outside Canada unless they have the consent of the individual[51] or the transfer is in the context of an outsourcing relationship and is necessary for the public body to perform its duties (and, where the disclosure is outside of Canada, such disclosure is necessary because the individual service provider is temporarily travelling outside Canada).[52]

However, private sector organizations subject to the province's *Personal Information Protection Act* (PIPA) do not appear to face a similar restriction and may transfer personal information outside Canada. Guidance from the British Columbia Commissioner indicates that transparency is critical and the organization should set out in its privacy policy to whom personal information is transferred outside the organization and why it is transferred.[53]

49 Summary of Privacy Laws, *supra* note 25.

50 Forcese, *supra* note 35 at 523.

51 FOIPA s. 33.1(1)(b).

52 FOIPA s. 33.1(1)(e.1).

53 In the clouds and beyond! Navigating access and storage outside of Canada.

In Alberta, the *Personal Information Protection Act* (PIPA) is deemed to be substantially similar to PIPEDA. It expressly provides that a private organization is responsible for personal information in its custody or under its control and that, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, for those services, responsible for that person's compliance with PIPA.[54] The Act requires notification when using a service provider outside Canada to collect information or transfer information to a provider; the organization must before or at the time of collecting or transferring the information notify the individual in writing or orally.[55] However, the disclosure provisions do not expressly require consent to transfer or disclose information to the service provider.

In Saskatchewan, the *Freedom of Information and Protection of Privacy Act* (FOIP) permits a public sector organization to provide personal information to an information management service provider for various information management or information technology services, such as processing, storing and archiving, pursuant to an agreement.[56] The disclosure sections do not expressly require consent to transfer or disclose information to a service provider, so long as the information is disclosed for the purpose for which it was obtained or compiled, or for a use consistent with that purpose.[57]

In Manitoba, the *Freedom of Information and Protection of Privacy Act* (FIPPA) permits a public sector organization to provide personal information to an information manager for prescribed purposes, namely information management or information technology services, similar to Saskatchewan.[58] The information may only be used by the information manager for the same activities and purposes that the public body may itself undertake.[59] The public body and the information manager must have an agreement in place[60] and the personal information is deemed to remain in the custody and control of the public body.[61]

54 PIPA s. 5(2).

55 PIPA s. 13.1(1).

56 FOIP s. 24.2.

57 FOIP s. 29(2)(a).

58 FIPPA s. 44.1(1).

59 FIPPA s. 44.1(2).

60 FIPPA s. 44.1(3).

61 FIPPA s. 44.1(5).

In Quebec, the *Act respecting the protection of personal information in the private sector*,[62] which has been deemed substantially similar to PIPEDA, applies to every organization (enterprise) that collects, uses and discloses personal information (disclosure is referred to as "communication") about a "natural person" (i.e., not legal entities). It is not limited to the collection, use and disclosure of personal information as part of a commercial activity**.** Personal information may not be communicated to a third party or used for purposes not relevant to the object of the file, unless the person concerned has consented to the communication or use, or the communication or use is allowed by the Act.[63] Further, in carrying out the activities of the enterprise, any party who has been contracted by the enterprise may have access to personal information without the consent of the person *only if the information is needed for the performance of their duties or carrying out other mandates or contracts.*[64]

Personal information can be communicated to a third party outside Quebec only if the *enterprise* is *satisfied* that:

> (1) the information will be used for purposes that are relevant to the object of the file or communicated to a third person with the consent of the persons concerned except in cases as permitted by the Act; and
>
> (2) in the case of marketing lists, the persons involved are able to opt out of the commercial use.[65]

Nova Scotia's *Freedom of Information and Protection of Privacy Act* (FOIPOP) does not appear to expressly impose obligations related to the disclosure or transfer of personal information to service providers or a third party. However, Nova Scotia has specific legislation, the *Personal Information International Disclosure Protection Act* (PIIDPA), aimed at protecting personal information from unauthorized disclosure outside Canada. PIIDPA gives additional protections for personal information collected, used, or disclosed by public bodies and service providers who act on behalf of the public body and makes it illegal to disclose, store or allow personal information to be accessed from locations outside Canada, unless the individual the information is about has consented to it being stored in or accessed from

---

62 The Act *respecting the protection of personal information in the private sector* provides detailed rules of application for Articles 3, 35-41 of the *Civil Code of Quebec* and therefore needs to be read with the Code to have a comprehensive understanding of the organizations compliance obligations.

63 *Act respecting the protection of personal information in the private sector* s.13.

64 *Act respecting the protection of personal information in the private sector* s.20.

65 *Act respecting the protection of personal information in the private sector* s.17.

outside Canada, or if the information's storage/access outside Canada has been authorized by the head of a public body (who has deemed the storage/access necessary to meet the operational needs of the organization).[66] In the case of a service provider, a person retained under a contract to perform services for a public body, providing storage, access or disclosure of personal information outside Canada, the provider can only collect and use personal information necessary to fulfill its obligation as a service provider.[67] The province's health privacy legislation, deemed substantially similar to PIPEDA,[68] requires consent for out-of-province disclosures, subject to certain exemptions, though it is unclear whether the Act considers all out-of-province transfers as disclosures.[69] Many health information custodians in Nova Scotia proceed on the basis that a transfer for processing out of the province is not a "disclosure".

In New Brunswick, the *Right to Information and Protection of Privacy Act* (RTIPPA), seems to permit public sector organizations to transfer personal information without consent to a provider where it has a written agreement with the provider "… for the protection of the personal information against risks including unauthorized access, use, disclosure or destruction."[70] That said, the province's *Personal Health Information Privacy and Access Act* (PHIPAA), deemed substantially similar to PIPEDA, does require express consent when disclosing personal health information to a person outside New Brunswick, though also ambiguous as to whether out-of-province transfers are automatically considered disclosures.[71] Still, many health information custodians in New Brunswick proceed on the basis that a transfer for processing out of province is not a "disclosure".

In Prince Edward Island, *Freedom of Information and Protection of Privacy Act* (FOIPOP) applies to public bodies. FOIPOP does not appear to expressly provide obligations related to the disclosure or transfer of personal information to service providers or a third party.

66 PIIDPA s.5.

67 PIIDPA s. 5(4).

68 Provincial legislation deemed substantially similar to PIPEDA.

69 *Personal Health Information Act* section 44(1).

70 RTIPPA s. 46(2).

71 PHIPAA s. 19(1)(d).

Newfoundland and Labrador's *Access to Information and Protection of Privacy Act* requires only that records containing personal information are transferred securely.[72] Its *Personal Health Information Act*, deemed substantially similar to PIPEDA,[73] requires consent for disclosures outside the province subject to certain exceptions. A cross-border transfer of information is not automatically considered a disclosure.[74]

## 3. The Equifax Case and Report of Findings

The current discussion seems largely to be driven by the investigation into Equifax Canada and its US affiliate, Equifax Inc. and the resulting report of findings (*Equifax Report of Findings*).[75] That case presented unique facts, uncommon in the usual circumstances of transfer of personal information. Because of the connection between that case and this discussion, it is important to consider the case in the context of transfers for processing. In our view:

(1) the case is not about cross-border transfer of data; and

(2) the data privacy gap at the core of the *Equifax Report of Findings* is not the result of a transfer of the data cross-border, but of the fact that consumers were misled into believing Equifax Canada was in control when that was not actually the case.

The recent OPC guidelines on meaningful consent require that an organization enable individuals to quickly review key information "right up front" as they are engaging said organization, including:

(1) details of the personal information being collected

(2) the third parties with whom personal information is shared

(3) the purposes for which personal information is collected, used or disclosed, and

(4) any residual meaningful risk (more than a minimal or mere possibility) of harm (including reputational harm) and other consequences arising from the collection, use and disclosure of personal information.

Neither Equifax Canada nor its affiliate Equifax Inc. were open about the flow of personal information. Consumers requesting products from Equifax Canada were first "engaged" by Equifax Inc., via the portal or the telephone line, and Equifax Inc. never sought appropriate

72 ATIPPA s. 64(c).

73 *Supra* note 68.

74 PHIA s.47.

75 Equifax Report of Findings.

consent to collect their personal information. The unclear information offered on the process led to lack of clarity on the use and disclosure of the personal information, including which organization handled the personal information and which organization was responsible for it.

The *Equifax Report of Findings* explained that the breach occurred concerning products purchased by Canadians. These products were delivered by Equifax Inc. and made available via a portal hosted by Equifax Inc. (paras. 61, 62). Even the phone lines related to the products were managed by Equifax Inc. Information was collected and stored by Equifax Inc., the US affiliate, in the US. "Equifax Canada subsequently discloses personal information to Equifax Inc. (...), as needed to fulfill the consumer's order." It appears from these facts that the collection was performed by Equifax Inc. and Equifax Canada complemented the personal information with additional information after initial data sets were collected and stored. Equifax Inc. and Equifax Canada were not transparent about this framework to their Canadian consumers. In their publicly available *Privacy Policy* at the time, the organization designated as accountable for the collection and use was Equifax Canada, when the collection derived from direct to consumer products was performed by Equifax Inc. Perhaps more crucially, and contrary to the applicable Privacy Policy, Equifax Canada did not meet the requirements of the Accountability Principle.

At paras. 89-94, the OPC notes a failure by Equifax Canada to monitor for compliance or to ensure the presence of adequate safeguards. This case was not about transborder transfers or outsourcing. This case was about a lack of meaningful consent (who was the actual party to which consent was being given) and a failure of accountability.

Consequently, with the Equifax facts, the most significant privacy issue lies not in the transfer of data. Rather, the issues are ones of accountability, transparency and consent: the delivery of products for which personal information was collected and handled was under the control of Equifax Inc.

In most cases, cross-border data transfers (including outsourcing and cloud computing with vendors) do not fit the data flow scenario of the *Equifax Report of Findings*. Changing the privacy landscape for transfers of personal information between affiliates and across borders based on a distinct and unusual set of circumstances uncharacteristic of typical transfer-for-processing arrangements is inadvisable, in our view.

## B. If a Disclosure, what Consent is Required?

If consent is required for the use of outsourcing arrangements or for transborder transfers of personal information (which we do not support), then organizations should be able to rely on implied consent, except in narrowly defined cases. Exceptional cases would include situations where the organization has lost control over the information transferred to the third party. For example:

- If an organization transfers personal information to a third party for the third party's own use in accordance with the third party's privacy notice and business practices.
- If there has been a manifest failure in fulfilling the accountability principle (clause 4.1, Principle 1 of Schedule 1 to PIPEDA). An example appears to be the *Equifax Report of Findings*. In this class of cases, implied consent fails because the outsourcing organization no longer has effective control over the personal information. In effect, the real and substantial consequence for the organization's failure to maintain effective control is the loss of the ability to rely on implied consent.
- If the organization has adopted misleading practices to encourage individuals to believe that their information will only be used internally by the organization or kept in Canada. Again, the real and substantial consequence for the organization engaging in deceptive practices is not only a breach of section 6.1 for collection and use of the personal information generally but also transfer of personal information specifically.

In this way, organizations fulfilling the accountability requirements are free to structure their business processes in the manner they see fit, which is consistent with and gives life to the purpose statement of PIPEDA (section 3).

### 1. Implied Consent

In *Royal Bank of Canada v. Trang,*[76] a unanimous Supreme Court of Canada adopted an objective test for determining whether implied consent is appropriate. Importantly, implied consent does not rely on particular disclosures by the organization. Instead, consent is implied based on a "reasonable person" test.

The Supreme Court noted that Schedule 1, clause 4.3.6 of PIPEDA acknowledges that consent can be implied when information is less sensitive (para. 34). However, it emphasized that even information that would ordinarily be considered sensitive – that is, financial information – must be assessed in the total context to determine the actual degree of sensitivity for the purposes of assessing whether implied consent is appropriate: "the degree

76 2016 SCC 50.

of sensitivity of specific financial information is a contextual determination" (para. 36).

In addition to considering the sensitivity of the information, the Supreme Court noted that clause 4.3.5 directs the organization to consider the reasonable expectations of the individual when determining the form of consent (at para. 35). The Supreme Court stated that when considering reasonable expectations, "the whole context is important" (para. 43). The Supreme Court specifically stated that privacy interests must not be unduly prioritized over legitimate business concerns (at para. 43), which is consistent with the purpose clause of PIPEDA (section 3, emphasis added):

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information *and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances*.

The purpose clause is significant. The Supreme Court has held that due regard for a purpose statement must be given, since it offers context for the entire Act.[77] In *Oceanex Inc. v. Canada (Transport)*,[78] the Federal Court noted that a purpose statement carries the authority and weight of duly enacted law. While the Court was interpreting the *Canada Transportation Act* in that case, its endorsement of Ruth Sullivan's statement of the binding nature of a purpose clause is applicable to the task of interpreting PIPEDA (at para. 334, emphasis added):

> 14.39 Purpose statements may reveal the purpose of legislation either by describing the goals to be achieved or by setting out governing principles, norms or policies. Unlike preambles purpose statements come after the enacting clause of the statute and are part of why it is enacted into law. *This makes them binding in the sense that they carry the authority and weight of duly enacted law.* However, like definitions and application provisions, purpose statements do not apply directly to facts but rather give direction on how the substantive provisions of the legislation – that do apply to facts – are to be interpreted.

In *Trang*, the Supreme Court concluded that there had been implicit consent to disclosure, as a "reasonable mortgagor in their position would be aware that the financial details of their mortgage were publicly registered on title, and that default on the RBC debt could result in a judgment empowering the sheriff to seize and sell the mortgaged property" (at para. 47).

77 *Council of Canadians with Disabilities v. Via Rail Canada Inc.*, 2007 SCC 15 at para. 287.

78 2018 FC 250.

## 2. Outsourcing does not require Express Consent

It would not be reasonable to require express consent if the outsourcing organization is meeting its accountability obligations, which require maintaining control and using contractual or other means to ensure a comparable level of protection while the information is being processed by a third party.

This does not change even if the information is sensitive. In a true outsourcing arrangement, an organization maintains effective control over personal information being transferred to the third-party supplier and appropriate contractual or other mechanisms are in place to ensure the information is protected. These contractual mechanisms include protections against the third party using the personal information for its own purposes for which the outsourcing organization has not obtained consent. Unless there is something unique about the context of processing, there is no meaningful difference between the organization processing the data itself and the third party processing it on the organization's behalf. Indeed, in some contexts, the third party may have technological capabilities that offer greater protection for the personal information than the organization can on its own.

In assessing the reasonable expectations of the individual, it is important to consider the accountability principle as well as the globalized economy. A reasonable person would understand that organizations that are outsourcing are required to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party (clause 4.1.3) and the organization remains responsible for personal information even when it is transferred to the third party (clause 4.1.3). As noted above, clause 4.1.3 specifically treats the transfer to the third party for processing as being an extension of the "possession or custody" of the outsourcing organization, rather than a true "disclosure".

PIPEDA repeatedly references the need to obtain consent if information is used or disclosed for purposes other than those for which it was collected (clause 4.5, as an example). Consent is not required where the use is the same but the method of processing changes. Nowhere does PIPEDA give individuals a right to dictate business processes. Indeed, any interpretation of PIPEDA that would lead to that result is inconsistent with PIPEDA's purpose statement.

The Federal Court of Appeal in *Toronto Real Estate Board v. Commissioner of Competition*[79] recently reinforced the point that PIPEDA gives individuals control over *purposes* and not over *methods* of processing (at para 165, emphasis added):

> [165] *PIPEDA only requires new consent where information is used for a new purpose, not where it is distributed via new methods.* The introduction of VOWs is not a new purpose–the purpose remains to provide residential real estate services and the Use and Distribution of Information clause contemplates the uses in question. The argument that the consents were insufficient–because they did not contemplate use of the internet in the manner targeted by the VOW Policy–does not accord with the unequivocal language of the consent.

When an organization obtains consent from an individual to collect information for a given purpose, it does not matter whether the primary organization uses a processor to fulfil the purpose on its behalf. The purpose for which the consent was obtained remains the same and the primary organization remains accountable for ensuring that the information is used or disclosed solely in fulfilment of that purpose and in compliance with its obligations under PIPEDA.

A reasonable person would also understand that Canada participates in a global economy with the full policy support of the federal government. Recently, the federal government introduced the *Canada-United States-Mexico Agreement Implementation Act* to facilitate the Canada-U.S-Mexico Agreement. This agreement includes provisions to remove and prevent barriers to cross-border trade in services and electronic commerce. Canada is also a party to the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, which similarly seeks to prevent and reduce barriers in these areas, among others. These are only two examples of the many international trade agreements that Canada has entered into.

Far from being merely government policy, the cross-border trade in services is a reality for a substantial proportion of Canadian businesses. In 2014, Statistics Canada reported on outsourcing trends to other countries between 2010 to 2012, before the current large scale adoption of cloud services: 20.6% of surveyed businesses outsourced business functions across borders. Interestingly, small and medium sized organizations were leading the pack with significantly higher rates of outsourcing than large businesses. These rates can be expected to have dramatically increased since the advent and mass adoption of cloud computing technologies. The Deloitte Global Outsourcing Survey for 2018 reported that 93%

79 2017 FCA 236.

of survey respondents reported that their organizations are considering or have already adopted cloud services. Not only are these cloud-based services outsourcing IT infrastructure, they frequently involve transfers across borders by design, even if that transfer is limited to business continuity purposes.

This is the economic reality in which Canadian businesses, employees, and consumers operate, with the support and promotion of the federal government. This economic reality forms a backdrop as part of the total context for determining the reasonable expectations of individuals who provide their information to an organization.

Based on the Supreme Court's approach to determining whether implied consent is appropriate, if organizations are required to obtain consent for the transfer of personal information to a third party for processing, they should be able to rely on implied consent for ordinary business outsourcing, including when personal information crosses borders. Although we support the continued application of the 2009 Guidelines, which require transparency in privacy notices, no specific notice is required to rely on implied consent for ordinary business outsourcing.

Where the organization is not outsourcing but disclosing personal information for the third party's own uses or where the organization has failed to maintain effective control in accordance with the accountability principle, these would be considered disclosures requiring consent. In these cases, the third party is not an extension of the outsourcing organization. The outsourcing organization cannot be said to still "possess" or have "custody" of the personal information, much less have effective control. In those situations, a reasonable person may expect a greater level of notice and possibly a request for additional consent.

### 3. Avoidance of Absurdity

As emphasized above, it is important to apply well-established principles of statutory interpretation to PIPEDA. The overriding principle is that "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament".[80] Courts avoid interpretations that result in absurdity or a lack of logical coherence.

80 *Bell ExpressVu Limited Partnership v. Rex*, 2002 SCC 42 at para. 26.

The approach taken by the OPC must be logically consistent with section 7.2 and avoid an absurd result in which disclosures in circumstances where the organization no longer retains control over the personal information are treated less strictly by Parliament than transfers for processing are treated by the OPC. Section 7.2 governs scenarios in which personal information may be used and disclosed without the knowledge or consent of the individual for purposes related to a prospective business transaction (section 7.2(1)) and a completed business transaction (section 7.2(2)). In the former scenario, the receiving party's right to use and disclose the information is limited to purposes related to the transaction. The individual has not, of course, provided any explicit consent to that use or disclosure. In the latter scenario, once the transaction is completed, both parties are free to use or disclose the personal information for their own purposes, though in keeping with the purposes for which the personal information was originally collected, permitted to be used or disclosed. If the receiving party wishes to expand the uses for which it has consent, it is free to do so by requesting consent from the individuals involved.

Crucially, there is no requirement for consent to disclosure of information for the third party's own use in the section 7.2(2) scenario. The only requirement is that one of the parties to the transaction notify the individual(s) whose information was disclosed within a reasonable time after the transaction is completed.

It would be illogical if a transfer for processing where the transferring organization maintains effective control over the personal information would require consent – particularly explicit consent – while a wholesale transfer of that information in a business transaction would require mere notice.

## 4. Consistency with International Norms

Reliance on implied consent as a legal basis for outsourcing use of the personal information is also consistent with international norms. The GDPR sets a high standard for consent, which must be "freely given" (Art. 4). Recital 42 states that "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." Expanding on the notion of "freely given" in its *Guide to the General Data Protection Regulation*, the UK Information Commissioner's Office (ICO) advises at page 63 that:

> Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate.

Unlike PIPEDA, the GDPR does not have a concept of implied consent. Other legal bases for processing fill the void. For example, organizations may rely on legitimate interests or necessity in the performance of a contract (Art. 6). These grounds fill in the gap that would otherwise exist in the GDPR in the absence of the Canadian concept of implied consent.

Although explicit consent can be a legal basis for transborder transfers, explicit consent is not required under the GDPR. Instead, an organization can rely on grounds equivalent to those for implied consent – such as legitimate interests or performance of a contract – provided the organization employs mechanisms such as standard contractual clauses or binding corporate rules that maintain accountability, or transfers the personal information to a jurisdiction declared by the European Commission as adequate.

As the OPC acknowledged in its original consultation document, *Consultation on Transborder Dataflows*, "a transfer for processing may well be integral to the delivery of a service", stating that "in such cases, organizations are not obligated to provide an alternative." An interpretation of PIPEDA that would require explicit consent would lead to the absurd result that consent is required for situations in which explicit consent is not seen as appropriate in other jurisdictions, because it cannot be meaningful. The OPC should not depart from the generally accepted international framework that permits outsourcing and transborder transfers based on grounds similar to implied consent (as interpreted by the Supreme Court).

## C. If Express Consent is Required, is the Change Retroactive?

The OPC should avoid applying its new interpretation requiring express consent to personal information already collected from individuals, including in any application to the Federal Court under section 14 or appearance under section 15 of PIPEDA.

In any proceeding before the Federal Court brought by a complainant following a Report of Findings by the OPC, the complainant may wish to rely on the excuse of officially induced error. In the criminal law context, the Supreme Court of Canada has held in *Lévis (City) v. Tétrault*[81] that constituent elements of the excuse of officially induced error involve:

(1) that an error of law or of mixed law and fact was made;

(2) that the person who committed the act considered the legal consequences of his or her actions;

81 2006 SCC 12 (at para. 26).

(3) that the advice obtained came from an appropriate official;

(4) that the advice was reasonable;

(5) that the advice was erroneous; and

(6) that the person relied on the advice in committing the act.

While this test applies in the criminal law context, it is relevant to guide an examination of the consequences if the OPC were to change its policy position to require explicit consent. As the ombudsperson tasked with addressing complaints by individuals and offering guidance, the Commissioner is an appropriate official to advise on the interpretation. The Federal Court would likely examine the OPC's advice, past and present, on this topic. It seems inappropriate before the Federal Court for the Commissioner to act contrary to the office's own history of guidance by arguing that organizations should not have relied on it.

As the OPC acknowledged in the *Equifax Report of Findings*, organizations have relied on its longstanding guidance that transfers of personal information to third parties for processing constitutes a "use" and not a "disclosure" of personal information. This guidance was well-considered by previous Commissioners. Deeming the OPC's previous interpretations now to be incorrect suggests that organizations had been induced into erroneous business practices by the OPC itself. While organizations may be expected, over time, to change their practices in line with new guidance, the OPC should avoid finding fault with organizations that relied on its previous guidance on a fundamental issue relating to outsourcing arrangements.

This issue of retroactivity would not arise if the OPC finds that implied consent is appropriate for outsourcing arrangements except in those circumstances outlined in the previous section. It would not be reasonable for an organization to be protected by the OPC's 2009 guidance if it disclosed personal information without consent to a third party for the third party's own use, lost effective control over the information due to a failure of accountability, or otherwise deceived the individual.

## D. Organizations that Voluntarily Follow the CSA Model Code or PIPEDA

The OPC should consider the impact of a significant policy change on organizations that may not be directly subject to Canadian privacy law. This includes the non-profit sector, many members of which voluntarily follow the CSA Model Code or assure stakeholders that personal information will be protected in the same manner as under PIPEDA.

The evolution of privacy law, both globally and in Canada, as well as increasing stakeholder expectations for protection of their personal information, are changing how Canadian charities manage their obligations around privacy, transparency and accountability.

PIPEDA applies to any private sector organization that collects, uses, or discloses personal information in the course of commercial activities.[82] There is a common perception that the "commercial activities" requirement places Canadian charities and not-for-profit entities outside the scope of PIPEDA. However, while PIPEDA applies to commercial entities, it is not their status as a commercial entity that makes them subject to PIPEDA. Rather, the nature of the specific activities of an organization may attract the PIPEDA requirements. If an activity is determined to be a "commercial activity", charities and not-for-profits would be caught in the scope of PIPEDA. "Commercial activity" is defined in section 2 of PIPEDA as:

> any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.[83]

In other words, charities and not-for-profit organizations are not automatically exempt from PIPEDA. The fact that an organization is non-profit for taxation purposes does not determine whether its collection, use or disclosure of personal information is carried out in the course of commercial activity.[84] The OPC has stated that "[w]hether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act".[85]

Whether an organization can be said to collect, use or disclose personal information in the course of a commercial activity will depend on the facts of each case.[86] In one case, the OPC found that a non-profit daycare organization fell under PIPEDA because payment for child care services was a commercial activity.[87] In another case, the non-profit Law School Admission Council was found to engage in commercial activity. The OPC stated that the

82 The Application of PIPEDA to Charitable and Non-Profit Organizations [PIPEDA Application].

83 *PIPEDA, supra* note 22, s. 2. See also Office of the Privacy Commissioner of Canada, Commercial Activity.

84 *Ibid.*

85 PIPEDA Application, *supra* note 77.

86 *Ibid*.

87 Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2005-309.

organization's status as a non-profit, non-stock, membership-based organization was not determinative and there is no exemption for non-profit or member-oriented organizations.[88]

In addition, charities and not-for-profits increasingly use methods other than donations, grants or government funding to earn revenue, increasing the likelihood that their activities may be "commercial activities" caught by PIPEDA. According to *The Giving Report 2018*, the sale of goods and services by charities increased from 7.9% of their total revenue in 2010 to 8.6% by 2016, totaling $22.6 billion.[89] It is becoming more difficult to determine whether a charity's activity falls in the scope of PIPEDA.

There is no bright-line test that can be applied to determine whether an activity is commercial in nature. The OPC has stated that whether an activity constitutes a commercial activity depends on the facts of each case. For this reason, many lawyers in the charity and not-for-profit area advise their clients to assume that, regardless of their tax status, they may be engaged in commercial activity in the meaning of PIPEDA, may be subject to PIPEDA and so should comply with it. As a result, many charities and not-for-profits choose to obtain consent and abide by the other "fair information principles" in the CSA Model Code for the Protection of Personal Information (the CSA Model Code), Schedule 1 to PIPEDA, when collecting, using or disclosing personal information.

The increasing sophistication of the charitable sector is another reason for charities and not-for-profit organizations to comply with PIPEDA and the CSA Model Code. Canada's charitable sector employs more than two million Canadians and accounts for 8% of Canada's GDP.[90] According to Statistics Canada's *Volunteering and Charitable Giving in Canada report*, 82% of Canadians made financial donations to a charitable or non-profit organization in 2013.[91] The number of online donors has been steadily increasing.[92] According to the Financial Post, 62% of Canadians prefer to donate online with a debit or credit card.[93] Charities have the same

88 Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2008-389.

89 Canada Helps, The 2018 Giving Report.

90 John Lorinc, Canada's Charitable Sector: What to Expect in 2019 (January 7, 2019).

91 Martin Turcotte, Volunteering and charitable giving in Canada (January 30, 2015), at 23.

92 *The Giving Report*, *supra* note 89 at 13.

93 Danielle Lee, You better watch out: How charities and donors can be more cyber-secure this holiday season, *Financial Post* (11 December 2018).

types of information as for-profit entities, including employee information, credit card numbers, donor information and private health information.[94]

Donors, clients, volunteers, employees and other stakeholders expect charities and not-for-profits to safeguard their personal information, protect it from misuse and be transparent and accountable for how it is used. In the 2018 *Global Trends in Giving Report*, 92% of donors said it was important for charities to protect their financial and contact information from data breaches.[95] Consumers, whether online purchasers or donors, do not expect different standards of protection to apply when giving their credit card number to a charity or an online retailer.

Further, in common with the for-profit sector, charities and not-for-profits also face the risks associated with privacy breaches and violations, including the risk of court action, class action litigation, court awarded damages and reputational injury.

In the charitable and not-for-profit sector, where money is tight and use of donor funds is heavily scrutinized, the costs and reputational damage associated with a perceived failure to protect stakeholder personal information could jeopardize the continued existence of a charity or not-for-profit. Given the risks involved, many charities and not-for-profits choose to comply with PIPEDA and the CSA Model Code to maintain the trust of their donors and other stakeholders and they will meet the likely expectations of the OPC or a court if there is a complaint or court action concerning their privacy practices.

## 1. Implications for Charities and Not-for-Profits of Elevating Disclosure Requirements

Requiring express consent for outsourcing or even transborder transfers will have significant implications for charities and not-for-profits who are either subject to PIPEDA or choose to comply with PIPEDA and the CSA Model Code for the reasons outlined above. By reversing its well-settled position that a transfer for processing is a "use" of information and not a "disclosure",[96] and by requiring meaningful consent, and possibly even express

94 Charity Village, Cyber Security and Privacy Risk, Vulnerability in the non-profit and charitable sector.

95 Giving Report, 2018 Global Trends in Giving Report.

96 See, OPC, Guidelines for processing personal data across borders.

consent, to such transfers, the OPC would impose additional costs and onerous requirements on a sector needing "to do more with less" and facing a steady decline in charitable giving.[97]

Many charities and not-for-profits rely heavily on third parties. In the course of their normal operations, *most* charities and not-for-profit organizations transfer personal information to third party service providers for processing or for other purposes like information technology and system administration, cloud computer service, administration and back office services, fundraising, telemarketing, direct mail services, donor relations, payment processors, payroll processors and after hours calls management.

Some charities and not-for-profits may lack the capacity or expertise to deliver these services internally while others may enter into collaborative arrangements to share resources with other organizations for cost savings and efficiencies. These arrangements allow charities and not-for-profits to save money so that they can devote more resources to fulfilling their charitable and not-for-profit purposes. Many charities, particularly those that work internationally, enter into agency or service arrangements with third parties that deliver services on the ground under the charity's direction and control. Some transfers are to affiliated entities, such as international umbrella or parent organizations that give administrative, management or other services and support.

Practice under the 2009 Guidelines meant that charities and not-for-profit organizations would typically give notice to individuals, through privacy policies or service agreements, that their personal information might be transferred to service providers or affiliates for processing. If the personal information was used for the purposes for which it was originally collected, no individual consent was required and charities and not-for-profits could operate seamlessly and without barriers.

If the *Equifax Report of Findings* and the resulting position of the OPC stands, charities and not-for-profits, most of whom already struggle to meet increasing demands with dwindling resources, would be hamstrung by the requirement to obtain meaningful consent, possibly even express consent, to these "disclosures". This would consume resources that could otherwise be deployed for charitable or not-for-profit purposes, cause delays and curtail a charity's ability to fulfill its mandate, especially in the international context.

97 Lorinc *supra* note 90.

Requiring consent would also interfere with the operational choices for charities and not-for-profits. It might require charities and non-profits to give individuals information about their options if they chose not to have their personal information disclosed to third parties. This requirement would be confusing and unworkable for most charities and not-for-profits, which typically lack resources and capacity to provide other options. Individuals should not have the right to selectively opt out of having their personal information transferred to or processed by a third party if the accountability principle is adhered to.

In short, charities and not-for-profits complying with PIPEDA and the CSA Model Code would be adversely impacted if the existing rules were elevated to a requirement that meaningful consent, and possibly even express consent be obtained for transfers of personal information for processing or to affiliated entities, whether or not transborder.

The new requirements would consume scarce resources that could be deployed for core organizational activities and could adversely affect an organization's ability to achieve its charitable or not-for-profit purposes and mission. Many charities and not-for-profits rely on their ability to work with third parties and affiliated entities to achieve their purposes or to support their administrative or operational functions. By creating barriers to the flow of information required by these organizations to carry out their missions, the new requirements could have a damaging effect on Canada's charitable and not-for-profit sector.

## III. CONCLUSION

The CBA Sections are dedicated to the rule of law, and believe that:

(a) transfers for processing where the accountability principle is fully given effect are not "disclosures" for PIPEDA purposes

(b) PIPEDA does not require consent for such transfers for processing, and

(c) the unique facts of the Equifax case do not necessitate reinterpreting PIPEDA.

Many organizations in Canada operate across provincial/territorial and international boundaries. Consistency in the legal regimes affecting the collection, use and disclosure of personal information is desirable. Following the 2009 Guidelines, there was a broad, clearly documented consensus on how transfers for processing should be managed, and that those transfers can be adequately managed under the accountability principle without adverse impact on individuals or organizations. A significant change in the OPC's position could eliminate that consistency and introduce uncertainty in the law. The proposed change would

be inconsistent with the express wording and the framework of PIPEDA and undermine the confidence that organizations and individuals can have in OPC Guidelines more generally.

If the OPC believes it to be desirable for consent to be obtained for transfers for processing or cross-border transfers, we believe that change should occur through the federal Parliamentary process.