ONTARIO BAR ASSOCIATION'S INSTITUTE 2019

PRIVACY, LAND DEVELOPMENT, AND OTHER KEY UPDATES IN CHARITY AND NOT-FOR-PROFIT LAW

Toronto - February 5, 2019

PRIVACY ISSUES AFFECTING CHARITIES

Esther Shainblum
Carters Professional Corporation
eshainblum@carters.ca

PRIVACY ISSUES AFFECTING CHARITIES

PRIVACY ISSUES AFFECTING CHARITIES

February 5th, 2019

By Esther Shainblum*

A. INTRODUCTION

Recent developments in privacy law, both globally and in Canada, as well as increasing stakeholder expectations and demands for protection of their personal information, should change how Canadian charities understand and manage their obligations around privacy, transparency and accountability.

B. RECENT DEVELOPMENTS

1. GDPR

The European Union's ("EU") *Regulation 2016/679, General Data Protection Regulation* ("GDPR")[1] was implemented across the EU as of May 25, 2018. The GDPR harmonizes data protection and privacy laws across all EU jurisdictions. Of particular note, while the GDPR applies to organizations with a physical presence in the EU, it has also been given an extra-territorial scope, applying also to organizations that are not established in the EU if they process personal data of EU residents to offer them goods or services (whether or not a fee is charged) or to monitor their behaviour within the EU.[2] Therefore, in certain circumstances, organizations in Canada, including charities, may be subject to the GDPR.

The GDPR applies to "processing" of "personal data." "Personal data" is defined as "any information relating to an identified or identifiable natural person" and includes a broad range of identifiers, such as "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[3] "Processing" of data is also defined broadly and includes any operation performed on personal data, such as "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

* Esther Shainblum, B.A., LL.B., LL.M., CRM, of Carters Professional Corporation would like to thank Christina Shum, B.M.T., J.D, Student-at-Law, and Adriel N. Clayton, B.A. (Hons.), J.D., an associate at Carters Professional Corporation, for their assistance in preparing this paper.

[1] *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, L119, 4/5/2016, p. 1–88 ["GDPR"].

[2] *Ibid*, art 3.

[3] *Ibid*, art 4(1).

destruction."[4] The GDPR applies to "controllers", *i.e.* natural or legal persons, public authorities, agencies or other bodies that determine the purposes and means of the processing of personal data, as well as "processors", *i.e.* natural or legal persons, public authorities, agencies or other bodies that process personal data on behalf of the controller.[5]

The GDPR strengthens and enhances data protection rights for individuals and imposes strict requirements on organizations engaged in data processing. At a high level, the core principles of the GDPR require that personal data be:

- processed lawfully, fairly and in a transparent manner;
- collected and processed for specified, explicit and legitimate purposes;
- minimized, *i.e.* adequate, relevant and limited to what is necessary in relation to those purposes;
- accurate and kept up to date – inaccurate data must be erased or rectified without delay;
- stored for no longer than is necessary for the purposes; and
- processed in a manner that ensures appropriate security of the personal data.[6]

Organizations to which the GDPR applies must comply with these principles or risk incurring the potentially severe penalties available under it.

Organizations caught by the GDPR must also comply with the enhanced rights for individuals under the GDPR, including the right of access to personal data;[7] providing greater transparency about how data is processed;[8] ensuring data portability rights (*i.e.* the transfer of personal data from one organization to another);[9] the so-called "right to be forgotten" (advising individuals of and complying with their right to request access to and rectification or erasure of personal data);[10] the duty to inform individuals without undue delay of serious data breaches that are likely to result in a

[4] *Ibid*, art 4(2).
[5] *Ibid*, art 4(7)-(8).
[6] *Ibid*, art 5.
[7] *Ibid*, art 15.
[8] *Ibid*.
[9] *Ibid*, art 20.
[10] *Ibid*, art 13(2)(b).

high risk to the individual;[11] and ensuring that any consent obtained for the processing of individuals' personal information is "freely given, specific, informed and unambiguous."[12]

There are numerous other rules including the requirement to have a "data protection officer" who is responsible for data protection for businesses that process data on a large scale;[13] data protection requirements;[14] and breach notification requirements.[15]

a) Extra-territorial Scope of the GDPR

As alluded to above, even if not established in the EU, Canadian charities and not-for-profits may be caught by Article 3(2)(a) or (b) of the GDPR if they process personal data of EU residents to offer them goods or services or to monitor their behaviour within the EU[16]. Merely having a website that is accessible in the EU will not be enough to constitute "offering goods or services."[17] It must also be apparent that the organization "envisages services to data subjects" in more than one EU member state by, for example, mentioning users who are in the EU or using a language or a currency generally used in the EU with the possibility of ordering goods and services in that other language.[18]

The European Data Protection Board guidelines on the territorial scope of the GDPR[19] (the "EDPB Guidelines") shed some light on what constitutes "offering goods or services" within the meaning of the GDPR.

The EDPB Guidelines confirm that, while Article 3(2) of the GDPR applies to the personal data of data subjects who are in the EU, regardless of their citizenship, residence or other legal status,[20]

[11] *Ibid*, art 34.
[12] *Ibid*, arts 6(1)(a) and 4(11).
[13] *Ibid*, ch IV, s 4.
[14] *Ibid*, art 25.
[15] *Ibid*, arts 33-34.
[16] *Ibid*, art 3(2)(a) and (b)
[17] *Ibid*, recital 23.
[18] *Ibid*, recital 23.
[19] European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation" (adopted on 16 November 2018), online: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf>. ["EDPB Guidelines"].
[20] *Ibid* at 13.

there must be an element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour, in order for the GDPR to apply.[21]

The EDPB Guidelines set out a number of factors that may, alone or in combination with one another, indicate that goods or services are being offered to a data subject in the EU including:

- The EU or at least one Member State is mentioned by name;
- Marketing and advertisement campaigns have been directed at an EU audience;
- EU addresses or telephone numbers are mentioned;
- An EU domain name such as ".eu" is used;
- There are travel instructions from one or more EU Member States;
- EU customers are mentioned;
- EU languages or currencies are used;
- The delivery of goods in EU Member States is offered.[22]

If one or any combination of these factors is present, organizations in Canada, including charities, may be subject to the GDPR.

The second type of activity triggering the application of Article 3(2) is the monitoring of data subject behaviour in the EU. "Monitoring behaviour" includes tracking individuals on the internet to analyze or predict their personal preferences, behaviours and attitudes.[23]

---

[21] *Ibid* at 12. The EDPB Guidelines provide the following example at page 14 - A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market. The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR.
[22] *Ibid* at 15-16.
[23] GDPR, *supra* note 1, recital 24.

According to the EDPB Guidelines, in order for the GDPR to apply, the monitoring must relate to a data subject in the EU and the monitored behaviour must take place within the territory of the EU.[24] The EDPB Guidelines state that "monitoring" does not exclusively mean tracking a person on the internet, but can also include tracking through other types of network or technology, such as wearable and other smart devices.[25] They also provide that not every online collection or analysis of personal data of individuals in the EU will automatically count as "monitoring" within the meaning of Article 3(2), and that there must be subsequent behavioural analysis or profiling involving that data, for it to constitute "monitoring."[26]

The EDPB Guidelines go on to list examples of monitoring activities including "online tracking through the use of cookies or other tracking techniques such as fingerprinting."[27] Including this activity in the list of "monitoring" indicates that using cookies on a website that is accessible to EU residents will be enough to trigger the application of the GDPR, potentially capturing a broad range of Canadian charities.

Other examples of monitoring that are listed include targeting advertisements to consumers based on their browsing behavior; closed circuit TV and various online activities related to an individual's health status or diet.[28]

If a Canadian charity is caught by the GDPR due to Article 3(2), it is required to designate a representative within the EU who is mandated to ensure its compliance with the GDPR.[29] Failure to appoint a representative or failure to make the identity of the representative available to data subjects would be a breach of the GDPR, exposing it to the significant penalties available.[30] The Canadian charity would be able to avoid the obligation to appoint a representative if it can demonstrate that its data processing is "occasional", does not include, on a large scale, processing of certain

[24] EDPB Guidelines, *supra* note 19 at 17.
[25] *Ibid* at 17-18.
[26] *Ibid* at 18.
[27] *Ibid.*
[28] *Ibid*.
[29] GDPR, *supra* note 1, art 27.
[30] EDPB Guidelines, *supra* note 19 at 19.

categories of particularly sensitive data, and does not pose a risk to the rights and freedoms of natural persons.[31]

Administrative fines can be imposed for any infringement of the GDPR. While fines are supposed to be "effective, proportionate and dissuasive",[32] certain infringements are subject to fines of up to €10 million or up to 2% of the total worldwide annual turnover for the undertaking for the previous financial year, whichever is higher.[33] Other more serious infringements, such as non-compliance with the core principles described earlier in this article, are subject to fines of up to €20 million or up to 4% of the total worldwide annual turnover for the undertaking for the previous financial year, whichever is higher.[34]

2. Mandatory Breach Reporting Under PIPEDA

On November 1, 2018, the *Digital Privacy Act*[35] came into force. It established mandatory data breach reporting and recordkeeping requirements under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[36] through the addition of new Division 1.1, "Breaches of Security Safeguards" to PIPEDA, and was accompanied by *Breach of Security Safeguards Regulations* (the "Regulations"),[37] providing additional details about these obligations.

Organizations that experience certain types of data breaches are now required to report them to the Office of the Privacy Commissioner of Canada ("OPC") and to notify the affected individuals as well as, in some cases, third party organizations.

a) Key Concepts Under PIPEDA

By way of background, PIPEDA is based on the ten fair information principles that are set out in Schedule 1 to the legislation, which include:

[31] GDPR, *supra* note 1, art 27(2)(a)
[32] *Ibid*, art 83.
[33] *Ibid*.
[34] *Ibid*.
[35] SC 2015, c 32.
[36] SC 2000, c. 5 ["*PIPEDA*"].
[37] SOR/2018-64 ["*Regulations*"].

- identifying the purposes for which personal information is collected at or before the time of the collection;

- requiring the knowledge and consent of the individual for the collection, use, or disclosure of personal information;

- limiting the collection of personal information to that which is necessary for the purposes identified;

- not using personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law;

- using security safeguards appropriate to the sensitivity of the personal information;

- informing individuals about the existence, use and disclosure of their personal information, giving them access to it and allowing them to challenge its accuracy and completeness.[38]

"Personal information" is defined under PIPEDA as "information about an identifiable individual"[39] and has been given a broad and expansive interpretation, capturing virtually any type of information about, or that can be used to identify, an individual.[40]

b) What Triggers the Notification and Reporting Obligations:

The notification and reporting obligations build on the ten fair information principles under PIPEDA and are triggered when an organization experiences a "breach of security safeguards" involving

[38] To assist organizations with complying with PIPEDA and its fair information principles, the OPC has published topical guidance documents elaborating upon the requirements under PIPEDA. See, for example, Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (May 24, 2018), online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805> ["Consent Guidance"] and Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805> ["Data Guidance"].

[39] *PIPEDA*, *supra* note 36, s 2(1)

[40] Office of the Privacy Commissioner of Canada, "Personal Information", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/>.

personal information under its control, if it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual.

Section 2(1) of PIPEDA defines a "breach of security safeguards" as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of or a failure to establish the types of security safeguards organizations should have to protect personal information. In a nutshell, PIPEDA requires organizations to have in place physical, organizational and technical security safeguards appropriate to the sensitivity of the information.[41]

Subsection 10.1(7) of PIPEDA defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Subsection 10.1(8) of PIPEDA sets out a number of factors that are relevant to determining whether a breach of security safeguards creates a "real risk of significant harm" to an individual, including:

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused; and
- any other prescribed factor.

The open-ended language of this provision suggests that organizations are not precluded from considering other factors when determining whether a breach creates a "real risk of significant harm."

c) Reporting and Notification Requirements

If an organization experiences a "breach of security safeguards" involving personal information under its control and it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual ("Serious Breach"), the following obligations are triggered:

[41] PIPEDA, *supra* note 36, Schedule 1, s 4.7.3.

- it must report the Serious Breach to the OPC;

- it must notify the affected individual of the Serious Breach;

- it must notify any other organization, a government institution or a part of a government institution of the Serious Breach (such as, for example, the police, a bank or a credit reporting agency), if it believes that the other organization may be able to reduce the risk of harm or mitigate that harm, or if other prescribed conditions are satisfied. The Regulations do not currently identify any prescribed conditions.

The report to the OPC must be written and provided "as soon as feasible"[42] after the organization has determined that a Serious Breach has occurred.[43] However, the organization may submit updates to the OPC regarding the details in the report if it becomes aware of new information after the report has been submitted.[44] While the Regulations are flexible in that the report to the OPC may be sent "by any secure means of communication,"[45] there are certain minimum content requirements prescribed by the Regulations including a description of the personal information breached, the number of individuals affected, the steps taken to reduce or mitigate the risk of harm and to notify the affected individuals of the breach,[46] and the name and contact information of a person who can speak to the OPC about the breach on behalf of the organization.[47]

Notification to the affected individual must be conspicuous[48] and given "as soon as feasible" to the individual after the organization has determined that the Serious Breach has occurred.[49] There is substantial overlap between the information that must be provided to the OPC and to the affected individuals. Additionally, the notification must provide the individual with steps that he or she may take to reduce the risk of harm or to mitigate harm caused.[50]

---

[42] *Regulations*, *supra* note 37, s 2(1).
[43] *PIPEDA*, *supra* note 36, s 10.1(2).
[44] *Regulations*, *supra* note 37, s 2(2).
[45] *Ibid,* s 2(3).
[46] *Ibid,* ss 2(1)(c)-(f).
[47] *Ibid,* s 2(1)(g).
[48] *PIPEDA*, *supra* note 36, s 10.1(5).
[49] *Ibid,* ss 10.1(2), 10.1(6), s 10.2(2).
[50] *Ibid, s* 3(e).

Under the Regulations, notification must generally be given directly to the individual. However the means of communication is flexible in that an organization may notify the affected individual in person, by phone, mail, or email, or in "any other form of communication that a reasonable person would consider appropriate in the circumstances."[51]

The Regulations also provide for exceptions where direct notification is not required. An organization may provide indirect notification to the affected individual if direct notification would likely cause further harm to the individual, undue hardship to the organization, or if the organization does not have the contact information of the individual.[52] Nevertheless, if notification is given indirectly, it must be given by public communication or a "similar measure that could reasonably be expected to reach the affected individuals."[53]

d) Recordkeeping Requirements

An organization must keep records of every breach involving personal information under its control, regardless of whether or not it is a Serious Breach.[54] Furthermore, in compliance with the regulations, organizations must retain these records for a minimum period of 24 months, starting from the day the organization determines that a breach has occurred.[55] These records must contain "any information that enables the Commissioner to verify compliance" with the OPC reporting and notification to individual requirements under PIPEDA.[56] Further, the organization must provide the OPC with a copy of, or access to, these records upon the OPC's request.[57]

e) Failure to Comply with Requirements

Failure to comply with the notification, reporting, and recordkeeping requirements may result in substantial consequences. A person who knowingly violates the mandatory breach requirements under PIPEDA and the regulations, or obstructs the OPC or its delegate in its investigation of a

[51] *Regulations*, *supra* note 37, s 4.
[52] *Ibid,* ss 5(1)(a)-(c).
[53] *Ibid,* s 5(2).
[54] *PIPEDA*, *supra* note 36, s 10.3(1).
[55] *Regulations*, *supra* note 37, s 6(1).
[56] *Ibid,* s 6(2).
[57] *PIPEDA*, *supra* note 36, s 10.3(2).

complaint or its audit, may be liable to a fine of up to $100,000 for indictable offences or $10,000 for offences that are punishable on summary conviction.[58]

The OPC also may enter into a compliance agreement with an organization and has the authority to include any terms necessary to ensure the organization's compliance.[59] In the event that an organization does not follow the agreement, the OPC may also seek a mandatory order from the Federal Court to require compliance. Entering into a compliance agreement with the OPC does not protect the organization from prosecution for an offence, nor does it protect the organization from potential legal action by an individual.[60]

f) OPC Guidance

The OPC published a guidance, finalized on October 29, 2018, to supplement the legislative and regulatory provisions (the "OPC Guidance").[61]

The Guidance recommends that organizations develop a framework for assessing the "real risk of significant harm", including determining the "sensitivity" of personal information as well as who accessed it (known or unknown entities), whether it was lost, inappropriately disclosed or stolen, whether it has been recovered, whether there was evidence of malicious intent, and whether the personal information was encrypted, anonymized or otherwise not easily accessible.

The Guidance also provides clarity on the minimum content that the OPC expects to see in organizations' records of data breaches, including, if the breach was not reported to the OPC, a brief explanation of why the breach was determined not to pose a "real risk of significant harm."

The Guidance includes a draft breach report form designed to make it easier for organizations to report a Serious Breach to the OPC.

---

[58] *Ibid,* s 28.
[59] *Ibid,* s 17.1(1)-(2).
[60] *Ibid,* s 17.1(4).
[61] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.

C. DOES PRIVACY LAW APPLY TO CHARITIES?

PIPEDA applies to any private sector organization that collects, uses, or discloses personal information in the course of commercial activities.[62]

Most if not all Canadian charities believe that the "commercial activities" trigger automatically places them outside of the scope of PIPEDA. However, while PIPEDA clearly applies to commercial entities, it is not their status as a commercial entity that has made them subject to PIPEDA. Rather, it is the nature of the specific activities undertaken by an organization that may attract the requirements of PIPEDA. If a particular activity is determined to be a "commercial activity", then even charities could be caught within the scope of PIPEDA. The term "commercial activities" is defined in section 2 of the Act 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.[63]

The OPC itself 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".[64]

Charities and not-for-profit organizations are not automatically exempt from PIPEDA. The fact that an organization is non-profit for purposes of taxation does not determine whether or not its collection, use or disclosure of personal information is carried out in the course of commercial activity.[65] Whether an organization can be said to collect, use or disclose personal information in the course of a commercial activity will vary depending on the facts of each case.[66]

---

[62] Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Charitable and Non-Profit Organizations", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/> ["PIPEDA Application"].
[63] *PIPEDA*, *supra* note 36, s 2. See also Office of the Privacy Commissioner of Canada, "Commercial Activity", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronicdocuments-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/>.
[64] PIPEDA Application, *supra* note 62.
[65] *Ibid.*
[66] *Ibid*.

In one case, the OPC found that a non-profit daycare organization was caught by PIPEDA because payment for child care services was seen as a commercial activity.[67] In another case, the non-profit Law School Admission Council, which administers law school entrance exams, was found to be engaged in commercial activity. The OPC stated that the organization's status as a non-profit, non-stock, membership-based organization was not determinative and that there is no exemption for non-profit or member-oriented organizations.[68]

Further, charities and not-for-profits in certain provinces may be subject to provincial legislation that has been declared to be substantially similar to PIPEDA. Pursuant to paragraph 26(2)(b) of PIPEDA, if a province has enacted privacy legislation that is "substantially similar" to PIPEDA, an organization operating in that province will be exempted from PIPEDA and will be subject to the substantially similar legislation instead. Alberta and British Columbia, in particular, have passed substantially similar private sector privacy legislation and therefore that legislation operates in those provinces in respect of all personal information, although PIPEDA continues to operate in those provinces in respect of personal information that crosses provincial boundaries.[69]

The British Columbia *Personal Information Protection Act* ("BC PIPA") is BC's private sector privacy legislation and applies with respect to the collection, use or disclosure of personal information within the province's borders. Subject to certain limitations, BC PIPA applies to "every organization" and, as such, applies to corporations, unincorporated associations, co-operative associations, societies, churches and other religious organizations, charities and sports clubs.[70]

The Alberta *Personal Information Protection Act* ("AB PIPA") is Alberta's private sector privacy legislation and applies with respect to the collection, use or disclosure of personal information within Alberta's borders. Under the AB PIPA regime, some types of non-profit organizations are fully subject to the legislation while others are only subject to it in respect of information collected, used

[67] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-309", online: Government of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-309/>.
[68] Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2008-389" online: Government of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/389_rep_080529/>.
[69] *PIPEDA*, *supra* note 36, s 26(2)(b).
[70] *Personal Information Protection Act*, SBC 2003, c 63, s 3(1) ["BC PIPA"]. For further information, see also Office of the Information & Privacy Commissioner for British Columbia, "A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations" (October 2015) online: Government of British Columbia <https://www.oipc.bc.ca/guidance-documents/1438>.

or disclosed for commercial activity.[71] Religious societies, housing cooperatives, unincorporated associations, federally incorporated not-for-profit organizations, and organizations incorporated by private Acts are fully subject to AB PIPA and have the same obligations in respect of privacy as do other organizations in Alberta.[72]

Charities and not-for-profits in those provinces may therefore be subject to the substantially similar provincial legislation.

D. PRIVACY LITIGATION

Violations of privacy can now give rise to damage awards, tort claims and class action litigation in the courts, and Canadian courts are showing an increasing willingness to protect privacy interests.

In *Jones v Tsige*,[73] the Ontario Court of Appeal recognized a new common law tort of "intrusion upon seclusion."

In *Doe 464533 v N.D.*,[74] the Ontario Superior Court of Justice recognized another new tort - "public disclosure of private facts", although this decision was subsequently overturned on a technicality, creating some confusion about the state of the law.

Privacy-related class action litigation is also on the rise in Canada. In addition to the high profile, well known class actions against major retailers, financial institutions and social media providers,[75] a multi-million dollar class action lawsuit was brought against the Winnipeg Royal Ballet, a registered charity, in July 2018 by former students who allege that they were coerced by a teacher employed by the Ballet to pose for sexualized photos that he later posted online.

---

[71] *Personal Information Protection Act*, SA 2003, c P-6.5, s 56 ["AB PIPA"].
[72] Office of the Information and Privacy Commissioner, "Review of the Personal Information Protection Act" online: Government of Canada <https://www.oipc.ab.ca/media/686362/PIPA_Review_Submission_Web_Feb2016.pdf> at 5.
[73] 2012 ONCA 32.
[74] 2016 ONSC 541.
[75] For example, over the last two years, class action lawsuits have been launched in Canada against Walmart Canada Inc., Equifax Canada Co., and Facebook Inc., over privacy breaches.

On a smaller scale, in 2017, the Ontario Superior Court of Justice Small Claims Court awarded a plaintiff the sum of $4000 in damages after she was filmed jogging in a park and her image was used for commercial purposes without her knowledge or consent.[76]

These decisions highlight the fact that the floodgates have been opened for new privacy-based lawsuits. In particular, the rise of class action lawsuits to remedy privacy breaches poses an existential risk to all organizations, including charities, that collect, hold, use or disclose personal information.

E. CHARITIES AND CHILDREN

Charities that serve or deal with children are exposed to a particular privacy risk. As noted above, a key concept in privacy law is consent to the collection, use or disclosure of personal information.

Organizations face a problem with obtaining valid consent from children. As pointed out by the OPC, "it can be challenging (or even not possible) to obtain meaningful consent from youth, and in particular younger children."[77] The OPC has stated that the personal information of children and youth is particularly sensitive, especially the younger they are.[78] In fact, the OPC has taken the position that, in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians.[79] With respect to youth aged 13 to 18, the OPC's position is that their consent will only be meaningful if organizations have taken into account their level of maturity and have adapted their consent processes accordingly.[80] Consents signed by youth between 13 and 18 may therefore not be effective and the courts may hesitate to enforce them.

For example, one major issue is the use by many charities of photographs of identifiable children – considered to be personal information under PIPEDA – to promote their programs or to share with parents and other stakeholders. It is standard practice among schools, religious organizations and

[76] *Vanderveen v Waterbridge Media Inc*., [2017] OJ No 6034 (ON SCSM).
[77] Office of the Privacy Commissioner of Canada, "Collecting from kids? Ten tips for services aimed at children and youth", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/02_05_d_62_tips/>.
[78] Office of the Privacy Commissioner of Canada, "Privacy and Kids", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/>.
[79] Office of the Privacy Commissioner of Canada, "2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act", online: Government of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1>.
[80] *Ibid*

other entities to request the consent from the child's parent or guardian when using and posting online photographs of children. However, there is no clarity yet as to whether a waiver signed by a parent is binding on a minor.[81] If it is challenged, a court may not enforce the waiver/consent or may only enforce portions of it.

Charities that post children's photos online are also exposed to the risk that such images will be misused by sexual predators. In February, 2016 France's national police force warned that posting photos of children online could jeopardize their privacy and security, expose them to sexual predators and lead to social or psychological problems later in life.[82] Online sexualized images of a child become a permanent, indestructible record, leading to an ongoing violation of that child.

Posting images of children and youth could expose children to potential misuse of their images and a charity to potential lawsuits, or class action lawsuits, years later.

F. CYBER RISK

Charities are also exposed to various privacy breach, data breach and other cyber risk scenarios. The majority of Canadians prefer to donate online with their debit or credit card,[83] and charities have the same types of information as for-profit entities have – such as employee information, credit card numbers, donor information, and private health information,[84] placing them at risk of being targeted by hackers and cyber attackers. Often short of funds, charities may have inadequate security safeguards in place. In June 2017, a UK charity was fined after a cyber-attack because it had failed to implement appropriate technical and organizational measures to protect personal data on its network, allowing sensitive financial data to be accessed by the hackers.[85]

---

[81] See *Dewitt* v. *Strang* 2016 NBQB 28, that may lead to a definitive ruling on the enforceability of parental waivers.
[82] Amart Toor, "French police tell parents to stop posting Facebook photos of their kids", online: The Verge <https://www.theverge.com/2016/3/2/11145184/france-facebook-kids-photos-privacy>.
[83] You better watch out: How charities and donors can be more cyber-secure this holiday season You better watch out: How charities and donors can be more cyber-secure this holiday season, December 11, 2018, https://business.financialpost.com/sponsored/business-sponsored/you-better-watch-out-how-charities-and-donors-can-be-more-cyber-secure-this-holiday-season
[84] Charity Village, Cyber Security and Privacy Risk, Vulnerability in the non-profit and charitable sector, https://charityvillage.com/cms/content/topic/cyber_security_and_privacy_risk_vulnerability_in_the_nonprofit_and_charitable_sector/last/141#.XE5mc2frsdU
[85] The British and Foreign Bible Society was issued a monetary penalty notice and fined £100,000 in accordance with s. 55A of the UK's Data Protection Act 1998 after a 2016 cyber-attack compromised its computer network. For the monetary penalty notice, see Information Commissioner's Office, "Monetary Penalty Notice", online: Government of the United Kingdom <https://ico.org.uk/media/action-weve-taken/mpns/2259142/bible-society-mpn-20180531.pdf>.

Charities are also vulnerable to "snooping", inappropriate use of social media or loss of equipment by staff or volunteers, all of which can expose them to data breaches, large or small, as well as claims for breach of privacy.

According to the Ponemon Institute, LLC, which published the results of its annual study of the financial impact of data breaches on organization in its "2018 Cost of a Data Breach Study: Global Overview" in July 2018, the cost of data breaches on an organization's bottom line has continued to rise, and more consumer records are lost or stolen each year. Canada had one of the highest average per capita cost of data breach, after the United States.[86] Canada also had the highest direct costs per compromised record, which includes expenses such as forensic expert costs, legal costs, and identity protection services for victims. Canada was also in second place regarding the indirect per capita cost of a data breach, which includes the costs of using organizational resources for breach-related activities as well as the loss of goodwill and customer churn.[87] In the charitable sector, where the use of donor money is heavily scrutinized and can build or destroy the reputation of an organization, these costs could jeopardize the continued existence of a charity.

In addition to ensuring that they have adequate safeguards and protections in place, charities should consider obtaining cyber insurance to cover some of the costs of a data breach or cyber-attack.

G. WHY CHARITIES SHOULD COMPLY WITH PIPEDA

1. Commercial Activity v. Tax Status

As discussed above, PIPEDA does not generally apply to charities and not-for-profits because most of the activities that charities and not-for-profits regularly engage in do not qualify as "commercial activities." Examples of activities that generally do not fall under the category of commercial activity include the collection of membership fees, fundraising, organizing club events, compiling lists of member information, and mailing out newsletters.[88]

Charities and not-for-profits are also increasingly turning to methods other than donations, grants, or government funding to earn revenue, increasing the likelihood that such revenue-generating

[86] Ponemon Institute LLC, "2018 Cost of a Data Breach Study: Global Overview", online: <https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf> at 13 ["Ponemon Study"].
[87] *Ibid* at 30.
[88] PIPEDA Application, *supra* note 62.

activities may be 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% of their total revenue by 2016, totalling $22.6 billion.[89] It is therefore becoming increasingly complex for a charity (or the OPC or a court) to determine whether an activity falls within the scope of PIPEDA.

There is no bright-line test that can be applied to determine whether an activity is commercial in nature. As we have seen, whether an activity constitutes a commercial activity will vary with the facts of each case. It would be most prudent for charities to assume that, regardless of their tax status, the OPC or a court might find that they are engaged in commercial activity and that they are subject to PIPEDA. This means that charities should obtain consent and abide by the other "fair information principles" when collecting, using or disclosing personal information.[90] By complying voluntarily with PIPEDA, charities and not-for-profits can also avoid accidentally breaching PIPEDA requirements if certain of their activities are later held to be commercial in nature, thereby also avoiding possible fines and penalties under the legislation.

2. Public Policy

In addition to the risk that certain activities of charities and not-for-profits might be seen as commercial in nature, thus bringing them within the scope of PIPEDA, it is difficult to come up with a convincing justification for excluding charities and not-for-profits from the requirements of privacy law.

The GDPR applies to charities and not-for-profits, as does BC PIPA, and many charities and not-for-profits are also subject to AB PIPA. Many health information custodians under the Ontario *Personal Health Information Protection Act, 2014*[91] and its counterparts in other provinces are charities. Charities and not-for-profits can and do comply with privacy legislation throughout Canada and elsewhere.

Furthermore, the reach of charities and not-for-profits is extensive in Canada. According to Statistics Canada's "volunteering and charitable giving in Canada" report, 82% of Canadians made financial

[89] Canada Helps, "The 2018 Giving Report", online: <https://www.canadahelps.org/en/the-giving-report/> ["The Giving Report"].
[90] Charities should also be complying with the Consent Guidance and Data Guidance, *supra* note 38.
[91] SO 2004, c 3.

donations to a charitable or non-profit organization in 2013.[92] While some of these donations may not have involved the transmission of any personal information, the likelihood is that many donors, who would like to receive charitable donation receipts, would have been required to provide personal information to the charity. The number of online donors has also been steadily increasing.[93] According to the Financial Post, 62% of Canadians prefer to donate online with their debit or credit card.[94] Therefore, the privacy interests of many Canadians will turn on the nature of the privacy protections, safeguards and protocols that Canadian charities have in place. The fact that PIPEDA only applies to organizations to the extent that they are engaged in commercial activities does not reflect the reality that many charities across Canada are in control of a great deal of personal information, particularly relating to donors, clients and volunteers.

3. Stakeholder Expectations

There are increasing stakeholder awareness and expectations around privacy, transparency and accountability. Consumers, whether online purchasers or donors, do not expect different standards of protection to apply depending on whether they are providing their credit card number to a charity or to an online retailer. With the growing awareness of the risks of providing online information and fairly frequent news of data breaches, charities and not-for-profits must take care to ensure that they do not lose the confidence and trust of their donors. Donors, clients 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 per cent of donors said it was important for charities to protect their financial and contact information from data breaches.[95]

Charities and not-for-profits should take these expectations into account when developing and adopting their privacy practices. As discussed earlier in this paper, there are also greater risks associated with privacy breaches and violations these days, including the risk of court action, class action litigation, court awarded damages and reputational injury.

---

[92] Martin Turcotte, "Volunteering and charitable giving in Canada" (January 30, 2015), online: Statistics Canada <https://www150.statcan.gc.ca/n1/en/pub/89-652-x/89-652-x2015001-eng.pdf?st=9pFaMU2R> at 23.
[93] The Giving Report, *supra* note 89 at 13
[94] Danielle Lee, "You better watch out: How charities and donors can be more cyber-secure this holiday season", *Financial Post* (11 December 2018) online: <https://business.financialpost.com/sponsored/business-sponsored/you-better-watch-out-how-charities-and-donors-can-be-more-cyber-secure-this-holiday-season>.
[95] Giving Report, "2018 Global Trends in Giving Report", online: <https://givingreport.ngo/>.

By moving toward alignment with PIPEDA, charities and not-for-profit organizations can maintain the trust and confidence of their donors, clients and other stakeholders, and minimize the risk of reputational damage.

Charities and not-for-profits should bear in mind that the standards set out in PIPEDA will shape stakeholder expectations, and possibly court expectations, regarding how an organization should handle the collection, use, disclosure, and safeguarding of personal information. As such, in order to effectively manage legal and reputational liability with respect to misuse of personal information, charities and not-for-profits should seriously consider PIPEDA requirements as a basis for building and implementing their privacy policies.

H. CONCLUSION

The GDPR may affect Canadian charities to the extent that they process personal data of EU residents to offer them goods or services or to monitor their behaviour within the EU. Having cookies on a website accessible to the EU may be sufficient to bring a charity within the scope of the GDPR. Charities that may be subject to the GDPR should immediately take steps to obtain legal advice and comply with the GDPR to avoid significant penalties.

With the growing emphasis on proper handling of privacy information as well as stakeholder awareness of privacy issues, charities and not-for-profits are facing increasing risk with respect to privacy matters. As such, charities and not-for-profits should consider voluntary compliance with PIPEDA. Doing so will help to manage legal and reputational liability, and maintain stakeholder confidence in the organization.