CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CARTERS CHARITY & NFP WEBINAR SERIES 2019

Wednesday, June 12, 2019

CRITICAL PRIVACY UPDATE FOR CHARITIES AND NFPS

By Esther Shainblum, B.A., LL.B., LL.M., CRM
eshainblum@carters.ca
1-866-388-9596

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Carters Charity & NFP Webinar Series 2019
Wednesday, June 12, 2019

Critical Privacy Update for Charities and NFPs

By Esther Shainblum, B.A., LL.B., LL.M., CRM

eshainblum@carters.ca
1-866-388-9596

Esther Shainblum, B.A., LL.B., LL.M., CRM – Ms. Shainblum practices at Carters Professional Corporation in the areas of charity and not for profit law, privacy law and health law. From 2005 to 2017 Ms. Shainblum was General Counsel and Chief Privacy Officer for Victorian Order of Nurses for Canada, a national, not-for-profit, charitable home and community care organization. Before joining VON Canada, Ms. Shainblum was the Senior Policy Advisor to the Ontario Minister of Health. Earlier in her career, Ms Shainblum practiced health law and corporate/commercial law at McMillan Binch and spent a number of years working in policy development at Queen's Park.

3

INTRODUCTION

- This presentation provides a high level overview of select privacy issues affecting charities
- Growing global emphasis on privacy and increasing stakeholder awareness and demands for protection of their personal information
- Expectations that charities and not-for-profits ("NFPs") must take into account when understanding their obligations around privacy, transparency and accountability

4

A. CASE LAW UPDATE

- Following is a brief discussion of some recent privacy-related rulings of interest to charities and NFPs

5

1. *R.* v. *Jarvis* - 2019 SCC 10

- High school teacher charged with voyeurism – secretly filmed students' breasts using pen camera
- Supreme Court of Canada held that the students had a reasonable expectation of privacy (REP) even in a public place (high school) and convicted the teacher of voyeurism
- SCC rejected narrow "all or nothing" interpretation of REP and adopted a broad interpretation - a person retains some expectation of privacy even in a public or semi public place
- Non-exhaustive list of nine factors to consider in determining if there is a REP

6

- Expands the range of settings and contexts in which individuals will arguably have a reasonable expectation of privacy
- Risks posed by new technologies – charities and NFPs must be vigilant, especially to protect privacy of minors and young persons
- Charities and NFPs should carefully screen and supervise employees/volunteers and ensure that privacy policies and protocols are regularly updated and reviewed

7

2. *Broutzas* v. *Rouge Valley Health System* 2018 ONSC 6315

- Patient contact information used to sell RESPs to parents of newborns
- No medical information was disclosed
- Proposed class action claimed tort of "intrusion on seclusion" – new privacy tort recognized in Ontario in 2012 in *Jones* v. *Tsige*
- Ontario Superior Court of Justice found no intrusion on seclusion - no significant invasion of personal privacy
- No REP in contact information, which is publicly available and is routinely and readily disclosed to strangers

www.charitylaw.ca www.carters.ca

8

3. *Jane Doe 72511* v. *Morgan* – 2018 ONSC 6607

- New tort of "public disclosure of private facts"
- Second "revenge porn" case in which this tort was recognized in Ontario – the first was set aside on a technicality
- Plaintiff's abusive ex-boyfriend posted a sexually explicit video of her on a pornographic website that was linked to ten other pornographic websites
- Her face was clearly visible and the video was viewed at least 60,000 times and downloaded an unknown number of times
- Ontario Superior Court of Justice – publication of an intimate image without consent is highly offensive and should give rise to a civil remedy – the best way is to adopt the tort of public disclosure of private facts in Ontario

www.charitylaw.ca www.carters.ca

9

- Elements of the tort :
  - the defendant publicized an aspect of the plaintiff's private life
  - the plaintiff did not consent to the publication
  - the matter publicized or its publication would be highly offensive to a reasonable person
  - the publication was not of legitimate concern to the public
- Held that the plaintiff had proved all the elements of the tort and awarded general damages, aggravated damages and punitive damages
- This tort now seems to be well-established in Ontario

10

4. OPC Report Of Finding On Equifax And Consultation On Cross-Border Transfers

- On April 9, 2019 the Office of the Privacy Commissioner of Canada ("OPC") released the report of its investigation of the 2017 data breach involving Equifax Canada Co. and its US parent.
- Surprising reversal of OPC's long-standing position on the transfer of personal information (PI) under The *Personal Information Protection and Electronic Documents Act* ("PIPEDA")
- OPC's 2009 Guidelines state that the cross-border transfer of PI for processing is a "use" requiring notice to consumers but not consent

11

- Had been well settled and relied upon by organizations in transferring PI to service providers and others
- In Equifax the OPC concluded that the transfer of personal information for processing is actually a "disclosure" of PI within the meaning of PIPEDA and that Equifax Canada should have obtained express consent
- The OPC stated that it views all transfers for processing as disclosures requiring consent, including transfers within Canada, trans-border transfers, and transfers to related entities

www.charitylaw.ca www.carters.ca

12

- OPC started a consultation on trans-border data flows as it "revisited" its policy position on this issue – was suspended due to Digital Charter but now restarted
- The OPC's "reframing" of the consultation on trans-border data flows seems to indicate a softening of its position as expressed in Equifax
- However, if it stands, this is a fundamental change that will have implications for charities/NFPs that are subject to PIPEDA (or that choose to comply with PIPEDA for the reasons discussed) including:
  - transfers of PI to a third party, including an affiliated entity, for processing or for other purposes, including trans-border transfers, would be considered to be a disclosure and consent, possibly express consent, would have to be obtained

www.charitylaw.ca www.carters.ca

13

  - the charity/NFP would have to provide clear information to stakeholders about the nature, purpose and consequences of the planned disclosure or cross-border disclosure, and its associated risks
  - the charity/NFP would remain accountable for the PI that was disclosed – would need robust written agreements with the third party including roles and responsibilities, reporting and oversight
- The OPC's new position would impose additional costs and obligations on organizations subject to PIPEDA

14

B. LEGISLATION

- Following is a brief discussion of recent privacy-related legislative initiatives

15

1. Mandatory Privacy Breach Reporting Under PIPEDA

- On November 1, 2018, new breach notification, reporting and recordkeeping obligations came into force under PIPEDA and accompanying regulations
- PIPEDA applies to every organization – including charities - in respect of the personal information that it collects, uses or discloses in the course of commercial activities
- Whether an activity is a "commercial activity" within PIPEDA will depend on the facts of each case – charities and NFPs should not assume they are exempt from PIPEDA

16

- Must report breaches to OPC and notify affected individual (and possibly third parties) when:
  - an organization experiences a **"breach of security safeguards"** involving PI 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 ("RROSH")
- "Breach of security safeguards" means loss of, unauthorized access to or unauthorized disclosure of PI
- "Significant harm" includes 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

17

- Relevant factors in determining whether a breach of security safeguards creates a RROSH include:
  - the sensitivity of the PI
  - the probability of misuse of the PI
  - any other prescribed factor (none so far)
- Obligations:
  - report the breach to the OPC;
  - notify the affected individual
  - notify any third party (*e.g.* the police, bank, credit reporting agency) that may be able to reduce or mitigate the harm
- Must retain records of all breaches for 24 months regardless of materiality
- Charities and NFPs should consider voluntary compliance given increasing stakeholder awareness and expectations around privacy, transparency and accountability

18

2. The General Data Protection Regulation ("GDPR")

- The GDPR came into force on May 25, 2018 and harmonizes data protection and privacy laws across all EU jurisdictions
- GDPR strengthens and enhances data protection rights for individuals and imposes strict requirements on organizations that handle "personal data"
- GDPR applies to any "processing" of personal data - any operation performed on personal data including collection, use, disclosure or storage
- Organizations to which the GDPR applies must comply or face severe penalties

19

a) Why should charities in Canada care about the GDPR?

- Extra-territoriality - GDPR applies to organizations that are not established in the EU if they:
  - process personal data of individuals in the EU to offer them goods or services (even if no fee is charged); or
  - monitor the behaviour of individuals in the EU
- Merely having a website accessible in the EU will not constitute "offering goods or services." It must be apparent that the organization "envisages offering services to data subjects" in the EU

20

- Under the new European Data Protection Board Guidelines (the "EDPB Guidelines"), in order for the application of the GDPR to be triggered
  - The key factor is whether the organization intends to "target" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour

- The EDPB Guidelines set out factors that indicate that goods or services are being offered, including:
  - Mentioning the EU or a member state by name
  - Giving EU addresses or telephone numbers
  - Using an EU domain name such as ".eu"
  - Mentioning EU customers
  - Using EU languages or currencies
  - Offering delivery of goods in EU member states

21

- If one or any combination of these factors is present with respect to a Canadian charity or NFP, the charity or NFP may be caught by the GDPR
- The second type of "targeting" activity triggering application of the GDPR is monitoring of data subject behaviour in the EU
- The behaviour monitored must relate to a data subject in the EU and must take place within the EU
- "Monitoring behaviour" includes tracking individuals on the internet to analyze or predict their personal preferences, behaviours and attitudes

22

- EDPB Guidelines provide that "monitoring" means 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
- EDPB Guidelines – use of the word "monitoring" implies having a specific purpose for the collection and re-use of data about an individual's behaviour within the EU
- EDPB Guidelines - not every online collection or analysis of personal data will automatically count as "monitoring"
  - there must be subsequent behavioural analysis or profiling involving that data, for it to constitute "monitoring"

23

- But - examples of monitoring activities given by the EDBP Guidelines include “online tracking through the use of cookies or other tracking techniques such as fingerprinting”
- Not clear whether using cookies on a website accessible to EU residents is enough to trigger the application of the GDPR, potentially capturing Canadian charities and NFPs
- Other examples of monitoring include targeting advertisements to consumers based on their browsing behavior, CCTV

24

b) Implications for Canadian charities

- If a Canadian charity is caught by the GDPR due to extra territoriality, it must designate a representative within the EU to oversee its GDPR compliance (and to facilitate enforcement?). Failure to do so is a breach of the GDPR, which could lead to penalties
- A Canadian charity or NFP may be exempted from this requirement if it can demonstrate that its data processing is “occasional”, does not include large scale processing of certain categories of particularly sensitive data, and is unlikely to pose a risk to the rights and freedoms of natural persons
- GDPR imposes other obligations on organizations and provides individuals with a number of rights that organizations must comply with

25

- If an organization is subject to the GDPR it should develop a compliance plan and must appoint a representative (unless exempted)
- Organizations that already comply with PIPEDA will be closer to compliance with GDPR but there will be gaps due to additional GDPR requirements that are not reflected in PIPEDA
- Failure to comply with GDPR can lead to fines of 4% of worldwide turnover or €20 million, whichever is higher
- If you think your charity or NPF may be subject to the GDPR, obtain legal advice

26

3. The Digital Charter

- On May 21, 2019 the Government of Canada launched its new Digital Charter
  - the foundation for modernizing Canada's privacy rules
- 10 Principles of the Digital Charter:
  - Universal Access
  - Safety and Security
  - Control and Consent
  - Transparency, Portability and Interoperability
  - Open and Modern Digital Government
  - A Level Playing Field
  - Data and Digital for Good
  - Strong Democracy Free from Hate and Violent Extremism
  - Strong Enforcement and Real Accountability

27

- The Government also released a Discussion Paper that includes plans to modernize PIPEDA including:
  - Alternatives or exceptions to consent, such as common uses of personal information for standard business activities
  - Explicit right to data mobility, like GDPR
  - Rights re online reputation, e.g. right to request deletion of information, like GDPR
  - Greater regulatory powers for the OPC and courts to enhance compliance with PIPEDA

28

  - Ongoing assessment in key areas such as:
    - Trans-border data flows – suspension of Equifax consultations
    - Application of PIPEDA to non commercial data collection activities – charities/NFPs?
  - New technologies
- The PIPEDA reforms introduced in the Discussion Paper are not binding but signal the likely direction of future legislation

29

4. Mandatory Privacy Breach Statistics Reporting Under PHIPA

- Under s. 12(2) of PHIPA health information custodians ("HICs") were always required to notify the affected individual of the breach at the first reasonable opportunity and advise them of their right to make a complaint to the Information and Privacy Commissioner ("IPC")
- However, new rules requiring a HIC to notify the IPC of certain types of privacy breaches came into effect on October 1, 2017

30

- HICs are now required to report to the IPC regarding seven categories of privacy breaches, including Personal Health Information (PHI) used or disclosed without authority or stolen or significant breach e.g. sensitive, large volume, PHI of many individuals, more than one HIC
- The new rules are set out in s. 12(3) of the *Personal Health Information Protection Act* ("PHIPA") and Sections 6.3 and 6.4 of Ontario Regulation 329/04 to PHIPA

31

- The regulation also requires each HIC to track privacy breach statistics starting January 1, 2018 and to report annually to the IPC on the number of times PHI in its custody or control was stolen, lost, used or disclosed without authority in the previous calendar year
- The reporting requirement commenced March 1, 2019 and continues annually thereafter
- The IPC has a guidance document that provides more detail to HICs on the type of information to be tracked and reported

32

C. PIPEDA AND CHARITIES AND NFPs

- Charities and NFPs should be complying with PIPEDA
- The following discussion intended to lay the groundwork for understanding why

33

1. Commercial Activity

- PIPEDA applies to any organization that collects, uses, or discloses PI in the course of commercial activities (s. 2(1))
- The nature of the organization (as for-profit or charity) does not determine whether PIPEDA applies
- If a particular activity is determined to be a "commercial activity", then charities and NFPs could be caught within the scope of PIPEDA

34

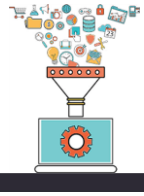
- OPC - "whether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act"
- Whether an organization is collecting, using or disclosing PI in the course of a commercial activity will vary depending on the facts of each case
- OPC found that a non-profit daycare organization was caught by PIPEDA
  - payment for child care services was seen as a commercial activity

35

- OPC found that the non-profit Law School Admission Council was engaged in commercial activity
  - OPC stated that there is no exemption for non-profit or member-oriented organizations
- Charities are increasingly turning to sale of goods and services methods to earn revenue
  - increasing likelihood that revenue-generating activities may be caught by PIPEDA
- It is becoming increasingly complex for a charity or NFP (or the OPC or a court) to determine whether an activity falls within the scope of PIPEDA

36

- No bright-line test that can be applied to determine whether an activity is commercial in nature.
- Whether an activity constitutes a commercial activity will vary with the facts of each case
- Uncertainty in predicting whether PIPEDA compliance is required
- Most prudent for charities and NFPs to assume that the OPC or a court might find that they are engaged in commercial activity and that they are subject to PIPEDA



37

- Further, charities and NFPs in certain provinces may be subject to provincial legislation that has been declared to be substantially similar to PIPEDA, such as:
  - British Columbia *Personal Information Protection Act* ("BC PIPA") applies to charities
  - Alberta *Personal Information Protection Act* ("Alberta PIPA") applies to religious societies, housing cooperatives, unincorporated associations, federally incorporated not-for-profits, and organizations incorporated by private Acts
  - Quebec private sector privacy act is not limited to commercial activities

38

- Charities and NFPs should consider compliance with PIPEDA, whether required or not
- Charities and NFPs should be complying with PIPEDA's underlying "fair information principles"
- By complying voluntarily with PIPEDA, charities and NFPs can also avoid accidentally breaching PIPEDA requirements if their activities turn out to be commercial - avoiding possible fines and penalties

39

2. Public Policy

- No convincing public policy justification for excluding charities and NFPs from privacy law requirements
- *GDPR* applies to charities, as does BC PIPA, and many charities are also subject to Alberta PIPA
- Many health information custodians under the Ontario *Personal Health Information Protection Act, 2014* (PHIPA) and its counterparts in other provinces are charities and NFPs
- Charities and NFPs can and do comply with privacy legislation throughout Canada and elsewhere

www.charitylaw.ca www.carters.ca

40

3. Stakeholder Expectations

- There are increasing stakeholder awareness and expectations around privacy, transparency and accountability
- Majority of Canadians make financial donations to charities or NFPs
- Majority of Canadians prefer to donate online
- The privacy interests of many Canadians will turn on the nature of the privacy protections, safeguards and protocols that Canadian charities have in place
- Consumers 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

www.charitylaw.ca www.carters.ca

41

- In the 2018 Global Trends in Giving Report, 92 percent of donors said it was important for charities to protect their financial and contact information from data breaches
- By aligning with PIPEDA, charities and NFPs can maintain the trust and confidence of their donors, clients and other stakeholders, and minimize the risk of reputational damage

42

4. Litigation

- Risks associated with privacy breaches and violations including the risk of court action, class action litigation, court awarded damages and reputational injury
- Canadian courts showing an increasing willingness to protect privacy interests
- Privacy-related class action litigation on the rise in Canada - *e.g.* multi million dollar Winnipeg Royal Ballet class action brought by former students for intimate photos taken by instructor and posted online

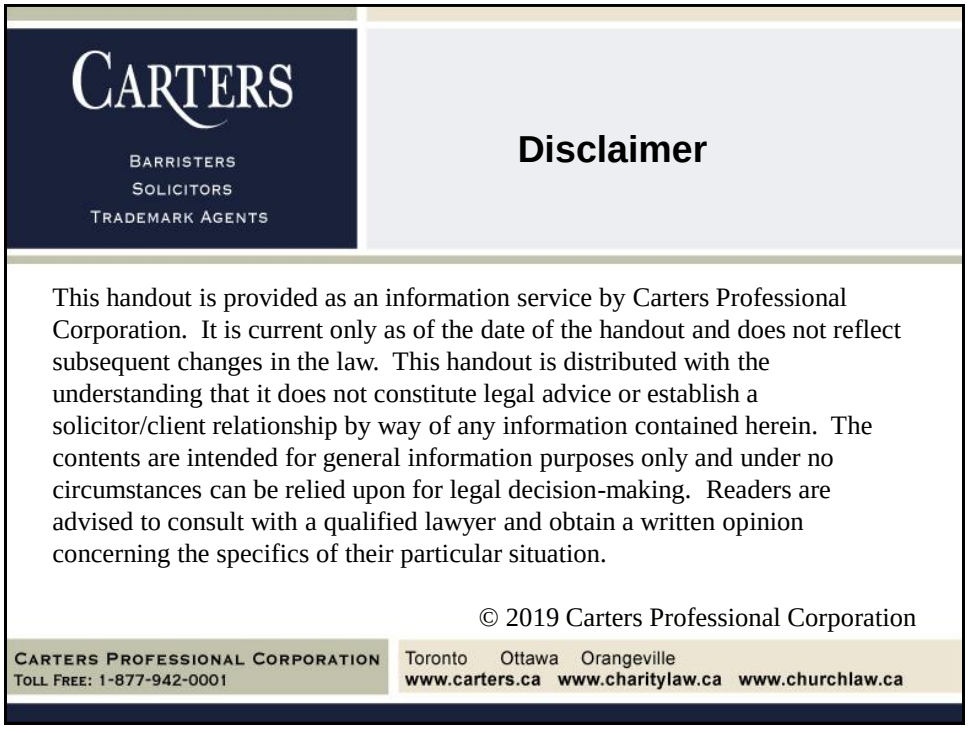
43

- Floodgates have been opened for new privacy-based lawsuits
- The rise of class action lawsuits to remedy privacy breaches poses an existential risk to all organizations
- The standards set out in PIPEDA will shape stakeholder expectations, and possibly court expectations, regarding how an organization should collect, use, disclose and safeguard PI

44

CONCLUSION

- Privacy is an increasingly interesting and volatile area
- Even issues once thought to be well settled are in flux
- Donors and other stakeholders have increasing expectations regarding the use and protection of their personal information by charities
- GDPR could pose a significant risk due to its extra-territorial effect
- The stakes are high - possible reputational damage, loss of stakeholder confidence and possible fines and penalties


CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS
Disclaimer
This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.
© 2019 Carters Professional Corporation
CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001
Toronto Ottawa Orangeville
www.carters.ca www.charitylaw.ca www.churchlaw.ca