CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 422

MAY 31, 2018

EDITOR: TERRANCE S. CARTER

NEW ONLINE GUIDELINES FROM THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

By Esther Shainblum*

A. INTRODUCTION

On May 24, 2018, the Office of the Privacy Commissioner of Canada ("OPC") published two new guidance documents designed to help organizations comply with their privacy obligations in an online environment:[1] the "Guidelines for obtaining meaningful consent" (the "Consent Guidance"),[2] and the "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" (the "Data Guidance").[3] This *Charity & NFP Law Bulletin* provides an overview of both documents, which the OPC states are intended to improve the consent model under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

B. CONSENT GUIDANCE

The Consent Guidance, which was issued jointly with the offices of the Information and Privacy Commissioners in Alberta and British Columbia, is intended to "breathe life" into the principle of meaningful consent, an essential element of Canadian private sector privacy legislation, which is often rendered illusory by advances in technology and the use of "lengthy, legalistic privacy policies". In this

---

* Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office. The author would like to thank Luis Chacin, LL.B., M.B.A., LL.M., Student-at-Law, for his assistance in preparing this Bulletin.

[1] Office of the Privacy Commissioner of Canada, News Release (May 24, 2018), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180524/.

[2] Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaning consent" (May 24, 2018), online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

[3] Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.

regard, the Consent Guidance sets out the following seven principles – a combination of legal requirements and best practices - that should guide organizations in developing and improving their consent processes.

1. Organizations must avoid information overload. They must inform individuals about key elements of their privacy management practices in a comprehensive and understandable manner. This information must be made available to individuals at the moment they are making decisions, such as whether or not to make a purchase or to download an app. Organizations must place additional emphasis on the following four elements: (i) what personal information is being collected, (ii) with whom is it being shared, (iii) for what purposes is the personal information being collected, used or disclosed, and (iv) what are the risks of harm and other consequences of the collection, use or disclosure to which the individual is consenting, including any residual risks of harm remaining after the organization has applied mitigation measures.

2. Organizations should allow individuals to control the amount and the timing of detail they receive about the privacy practices of the organization. The level of detail required may vary by individual and by situation. Key information may be summarized up front and increasing levels of detail made easily available in a layered format or by other means that support individual control. This information should remain available to be accessed by individuals at their discretion, as consent choices can be reconsidered at any time.

3. Organizations must provide individuals with clear and accessible choices to say "yes" or "no" to the collection, use or disclosure of personal information that goes beyond a "condition of service" (which is a collection, use or disclosure of personal information that is integral to and necessary for the provision of a product or service). Organizations should be transparent and prepared to explain why a collection, use or disclosure is a condition of service. Individuals must be given a choice with respect to all collections, uses or disclosures that are not conditions of service. These choices must be explained clearly and made easily accessible and consent must be obtained in the appropriate form, *i.e.* express or implied.

4. Organizations should be innovative and creative, adopting consent processes that are appropriate to the context and interface used, such as "just-in-time" notices and tools that interact with the individual

while filling out an online form, as opposed to simply importing a paper-based form to obtain online consent.

5. As consent is valid only to the extent that individuals understand what they are consenting to, organizations must consider the consumer's perspective to ensure that their consent processes are understandable, user friendly and easily accessible from all devices, including digital health technologies, smart phones, tablets, gaming devices, as well as desktops and laptops. Organizations must use clear explanations, appropriate levels of language and comprehensible means of displaying information, and may wish to take additional steps such as consulting with users or pilot testing to ensure that they are doing all of this effectively.

6. Organizations should make consent a dynamic and ongoing process, recognizing that informed consent is an ongoing process. Organizations may wish to provide interactive and dynamic ways to answer users' questions through various means such as by telephone, through regularly updated FAQs or by using smart technologies such as chatbots. Organizations should consider periodically reminding users of their consent choices and those available to them but must obtain consent to any significant changes to their privacy practices, such as using personal information for a purpose not originally contemplated or disclosing information to a new third party.

7. Organizations should be ready to demonstrate their compliance with these principles, especially that their consent processes are sufficiently understandable to permit them to obtain meaningful consent.

The Consent Guidance goes on to deal with a number of other consent-related issues including:

- Determining the appropriate form of consent for any collection, use or disclosure of personal information. While taking the position that consent should generally be express, the Consent Guidance states that implied consent can be used in strictly defined circumstances, depending on the sensitivity of the information, the reasonable expectations of the individual and whether the collection, use or disclosure creates a meaningful residual risk of significant harm.

- The notion of "risk of harm" which underlies the concepts of both sensitivity and reasonable expectations. The Consent Guidance states that express consent would be required where there is a

meaningful risk that a residual risk of harm will materialize and be significant. In a situation in which there is a likely or probable risk of significant harm, the purpose would be considered offside PIPEDA.

- Children and youth. The Consent Guidance acknowledges that the capacity to consent varies from individual to individual and that the OPC's counterparts in Alberta, British Columbia and Quebec do not set a specific age threshold for consent. However, consistent with the OPC's previously enunciated stance on this issue, the Consent Guidance takes the position that, except in exceptional circumstances, children under the age of 13 are unable to meaningfully consent to the collection, use and disclosure of personal information and that consent must be obtained from their parents or guardians. The Consent Guidance states that, in order to be able to obtain meaningful consent from minors over the threshold age, organizations must reasonably take into account their level of maturity and adapt their consent processes accordingly. Further, organizations should "stand ready to demonstrate on demand that their chosen process leads to meaningful and valid consent."

- Organizations must use personal information for purposes that a reasonable person would consider appropriate. They must also comply with their other obligations under privacy law. Having consent is not a "free pass" for organizations to collect and use personal information for whatever purpose they choose.

The Consent Guidance will be applied starting on January 1, 2019.

C. DATA GUIDANCE

The Data Guidance provides the guiding principles for the interpretation of subsection 5(3) of PIPEDA, which reads as follows:

> (3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

The Data Guidance frames subsection 5(3) as a "critical gateway" that either permits or prohibits the collection, use or disclosure of personal information depending on the organization's purposes for doing so, and which protects individuals from inappropriate data practices.

Looking first at how the courts have interpreted subsection 5(3), the Data Guidance identifies a series of guiding principles as follows:

1. The application of subsection 5(3) requires a balancing of interests between the rights of individuals to privacy with the need of organizations to collect, use or disclose personal information.

2. This balancing of interests must be viewed through the eyes of a reasonable person.

3. Subsection 5(3) is an overarching requirement that is superimposed on the organization's other obligations. All collection, use and disclosure is limited to purposes that a reasonable person would consider appropriate in the circumstances.

4. Even with consent, an organization must still show that a reasonable person would consider its purposes to be appropriate. However, even if the purposes meet that test under subsection 5(3), the organization must still meet its other obligations under PIPEDA.

Turning next to the issue of how to determine whether an organization's purposes are appropriate "in the circumstances", as required by subsection 5(3), the Data Guidance advises that this analysis must be carried out in a "contextual manner", looking at the surrounding facts, and that what is "appropriate" will vary according to the circumstances of each case. The Data Guidance goes on to outline the factors that the courts have taken into account in determining whether an organization's purposes are in compliance with subsection 5(3):

- The degree of sensitivity of the personal information at issue;

- Whether the organization's purpose represents a legitimate need / bona fide business interest;

- Whether the collection, use and disclosure would be effective in meeting the organization's need;

- Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and

- Whether the loss of privacy is proportional to the benefits.

Based on these past findings and a series of consultations with stakeholders, the Data Guidance then identifies six "No-Go Zones" or data practices that would generally be considered inappropriate by a reasonable person and that the OPC considers to be offside PIPEDA:

1. Collection, use or disclosure that is otherwise unlawful. Organizations' activities must comply with all legal and regulatory requirements and the collection, use and disclosure of personal information cannot be for purposes that contravene federal or provincial laws.

2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law. Use of big data analytics or other profiling or categorization that could lead to discrimination on prohibited grounds would not be considered to be appropriate under subsection 5(3).

3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual. Significant harm includes bodily and reputational harm, financial loss, property loss and identity theft, and is not seen as an appropriate known or probable cost for products or services.

4. Publishing sensitive personal information online with the intended purpose of charging individuals for its removal. Blackmail is not an appropriate purpose.

5. Requiring passwords to social media accounts for the purpose of employee screening. Seeking to access highly sensitive personal information that is not relevant or necessary for an employer's legitimate business purposes would not be considered appropriate by a reasonable person.

6. Surveillance by an organization through audio or video functionality of the individual's own device. This activity is seen as highly invasive and grossly disproportionate to the business objective, whether carried out covertly or with consent.

The Data Guidance concludes with a reminder that the determination of what is appropriate is a flexible and variable concept and that the list of No-Go Zones is not static and will be revisited and updated periodically over time. The Data Guidance will be applied starting on July 1, 2018.

D. CONCLUSION

As the OPC prepares to apply the Data Guidance starting on July 1, 2018 and the Consent Guidance starting on January 1, 2019, charities and not-for-profits collecting, using or disclosing personal information through digital means should review and revise their privacy policies and consent processes in order to ensure compliance with these OPC guidance documents. Further, they should be ready to revisit them on an ongoing basis as technological advancements and best practices continue to evolve and reshape the expectations of regulators such as the OPC.