PIPEDA – HOW TO OBTAIN "MEANINGFUL" CONSENT, AND WHEN CONSENT IS NOT ENOUGH

Posted on May 30, 2018

Categories: Insights, Publications

On May 24, 2018, the Office of the Privacy Commissioner of Canada (the "OPC") released its finalized consent guidelines, as well as guidance on certain "no-go zones" under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

PIPEDA provides that the "knowledge and consent" of an individual are required for the collection, use, or disclosure (collectively "**Processing**") of his/her personal information,[1] and also that "consent is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."[2] The "**Guidelines for obtaining meaningful consent**", which the OPC issued jointly with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner of British Columbia, set out both mandatory and suggested steps for organizations to obtain "meaningful" consent.

In addition, section 5(3) of PIPEDA provides that an organization is only permitted to collect, use or disclose personal information for purposes that a reasonable person would consider to be appropriate in the circumstances.[3] This reasonableness requirement is separate and apart from the consent requirements under PIPEDA, which means that an organization may be in contravention of PIPEDA even if it obtains consent for unreasonable Processing of personal information. The OPC's "**Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)**" sets out five "no-go" zones that it would generally consider to be contrary to the PIPEDA reasonableness requirement.

Set out below is a high level overview of the OPC's two new guidance documents, as well as key steps organizations should take to avoid enforcement action.

Guidelines for Obtaining Meaningful Consent – *To be applied by the OPC beginning on January 1, 2019*

On a number of occasions the OPC has expressed concerns about organizations relying upon long and legalistic privacy policies as the basis for Processing personal information. The Guidelines for Obtaining Meaningful Consent ("**Consent Guidelines**") are intended to "breathe life" into the ways in which consent is

obtained, by providing organizations with seven guiding principles that the OPC expects organizations to follow.

Overall, these principles are intended to provide businesses with the flexibility to design their own consent processes, provided that they create simple, readable privacy notices and policies that their consumers can understand.

The seven guiding principles are as follows:[4]

1.Emphasize key elements

Information about Processing of personal information must be readily available in complete form, but organizations should also avoid information overload. Therefore, individuals must be able to quickly review key elements impacting their privacy decisions, up front, including:

1. What personal information is being collected. This must be defined with "sufficient precision."
2. With which parties personal information is being shared, including the types of information being shared. In particular, organizations should specify any disclosures to a third party that may use the information for its own purpose.
3. The purpose of the data Processing. "Sufficient detail" must be provided, and purposes that are integral to the service should be distinguished from ancillary purposes.
4. Any risk of harm or other potential consequences to the individual. This includes only "meaningful risks" of significant harm, which are residual risks that fall below the balance of probabilities (but are more than a mere possibility), after the organization makes reasonable mitigation efforts. 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."

The OPC has indicated that emphasizing the above four points is a mandatory requirement to meet the consent requirements of PIPEDA.

2. Allow individuals to control the level of detail they get and when

Different individuals will require different amounts of information in order to make consent decisions. Privacy information should be layered so consumers can review it quickly, but obtain more information if they wish to do so. Also, the information should remain available to individuals throughout their relationship with the organization, and they should have the opportunity to re-consider their consent choices.

3. Provide individuals with clear options to say 'yes' or 'no'

Individuals can only be required to provide personal information that is essential to the product or service being offered. If the personal information is not essential, individuals must be able to easily opt-out. If the personal information is integral to the product or service, the organization must explain why this is the case.

4. Be innovative and creative

Organizations should take advantage of digital capabilities in order to create dynamic, user-friendly consent processes that are appropriate to the user interface. Organizations might consider adopting "just-in-time" notices, interactive tools (e.g., videos, infographics), and customized mobile interfaces.

5. Consider the consumer's perspective

Consent processes must be user-friendly and customized to the organization's target audience. This may involve seeking user input, pilot testing consent processes, consulting with privacy experts or regulators, and/or following an established best practice.

6. Make consent a dynamic and ongoing process

Obtaining consent should be an ongoing process, as organizations innovate, evolve and grow. Organizations must obtain users' consent before introducing significant changes to their privacy policy (e.g., using personal information for new purposes, or new disclosures of personal information for ancillary purposes). Organizations should address privacy questions through FAQs, chatbots and other technologies.

7. Be accountable: Stand ready to demonstrate compliance

Organizations must be able demonstrate that their consent process is understandable to their target audience. Pointing to a sentence "buried" in a privacy policy will not be sufficient.

In addition to these seven "guiding principles," the Consent Guidelines describe some additional considerations applicable to obtaining valid consent, including:

- In determining the appropriate form of consent, the sensitivity of the information and the reasonable expectations of individuals must be taken into account.
- Organizations generally must obtain express consent if the information is sensitive, or if the Processing of the information is outside the individual's reasonable expectations or gives rise to a meaningful residual risk of significant harm.
- For children under the age of 13, consent must be obtained from a parent or guardian in most circumstances.[5]
- Even with consent, organizations cannot Process information for a purpose that a reasonable person would consider to be inappropriate.

- If an individual withdraws their consent, the organization must stop collecting further data and should delete existing personal information where possible.
- "Consent is not a silver bullet". PIPEDA contains other obligations, such as those related to accountability, collection limitation, accuracy and safeguards.

Finally, in response to input received from stakeholders on the draft consent guidelines that were released last year, the OPC provided a "checklist" of things that organizations "must do" versus those that they "should do" for compliance with PIPEDA. This checklist indicates whether the OPC believes that each of the above points is mandatory for legal compliance, versus a recommendation on best practices.

Key Steps for Organizations

The OPC has indicated that the reason for providing that the Consent Guidelines will apply beginning on January 1, 2019, is because they understand that organizations will need to amend their consent processes to comply. However, as any organization that recently underwent a GDPR compliance initiative will know, amending privacy policies and practices will take time. Therefore, all organizations should act promptly to review the Consent Guidelines (especially the "must do" list), and review their existing consent processes to determine and implement any necessary modifications.

Guidance on Inappropriate Data Practices: Interpretation and Application of s. 5(3) – *To be applied by the OPC beginning on July 1, 2018.*

Section 5(3) of PIPEDA states that: "an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." Therefore, even with an individual's consent, personal information can only be Processed for appropriate purposes. In the OPC's view, this section of PIPEDA separates legitimate forms of information management from unlawful "no-go zones." The Guidance on Inappropriate Data Practices: Interpretation and Application of s. 5(3) (the "No-go Guidance") sets out the OPC's interpretation of s. 5(3), as informed by prior court decisions, and sets out the no-go zones that would generally be considered to be noncompliant with PIPEDA.

Overall, according to the No-go Guidance, the guiding principle in applying section 5(3) is that individuals' privacy rights should be balanced against the organization's need to Process personal information.

Similar to the Consent Guidelines, the No-go Guidance clearly indicates that organizations must show that Processing of personal information is reasonable in the circumstances, even if individuals have consented to such Processing.

In determining whether the purposes for Processing personal information are appropriate in the circumstances, courts will take into account the specific factual circumstances, including:

- The sensitivity of the personal information;
- Whether the information was collected for a bona fide business need;
- Whether the information effectively meets that business need;
- Whether there are less invasive means of achieving that same end; and
- Whether the loss of privacy is proportional to the benefits.[6]

Based on the above, the No-go Guidance sets out six "no-go zones", which the OPC currently considers to be offside PIPEDA.

1.Collection, use or disclosure that is otherwise unlawful

Organizations should be aware of Canada's federal and provincial laws, and should not Process personal information in any way that violates those laws. For example, organizations cannot Process personal information in a manner that violates credit reporting laws, nor can they require individuals to undergo genetic testing or disclose testing results.

2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law

Data analytics, or other profiling/categorization, which leads to discrimination contrary to human rights laws is generally considered inappropriate under PIPEDA. Unfair or unethical profiling/categorization that does not violate human rights laws may also be found to be inappropriate, and will be assessed on a case-by-case basis.

3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual

Data collection is not appropriate where it is certain or likely to cause significant harm to the individual, including: bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional opportunities, financial loss, identity theft, and/or loss of or damage to property.

4. Publishing personal information with the intended purpose of charging individuals for its removal

Organizations cannot publish sensitive personal information online for the primary purpose of charging individuals for its removal. This amounts to blackmail, and has previously been declared offside PIPEDA.[7]

5. Requiring passwords to social media accounts for the purpose of employee screening

Employers cannot require job applicants or employees to disclose their social media passwords for the purposes of obtaining or maintaining employment.

6. Surveillance by an organization through audio or video functionality of the individual's own device

Even with the individual's consent, organizations cannot collect audio, text, or video information from an individual's phone or computer. However, it may be permissible for the audio or video functionality of a device to be regularly or constantly turned on if necessary to provide a service, if the individual is fully aware of and in control of this function; provided that the information is not recorded, used, disclosed or retained except for the purpose of providing the service.

Key Steps for Organizations

The OPC has provided only a short transition period before it will begin applying the No-go Guidance, on the basis that these prohibited practices are consistent with prior interpretations of PIPEDA. Therefore, organizations should evaluate their current information handling practices before July 1, 2018, to ensure that they do not engage in any Processing of personal information that could fall within any of the OPC's no-go zones.

by Lyndsay Wasser and Sarah Strban (Student at Law)

[1] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, Schedule 1, s 4.3 [PIPEDA].[ps2id id='1' target=''/]
[2] Ibid at s 6.1.[ps2id id='2' target=''/]
[3] Ibid at s. 5(3).[ps2id id='3' target=''/]
[4] See https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.[ps2id id='4' target=''/]
[5] The Alberta, B.C. and Quebec regulators did not agree that it was appropriate to set a specific age threshold.[ps2id id='5' target=''/]
[6] Turner v Telus Communications Inc, 2005 FC 1601 at para 48, 144 ACWS (3d) 392.[ps2id id='6' target=''/]
[7] T (A) v Globe24h.com, 2017 FC 114 at paras 78-79, 275 ACWS (3d) 155.[ps2id id='7' target=''/]

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.