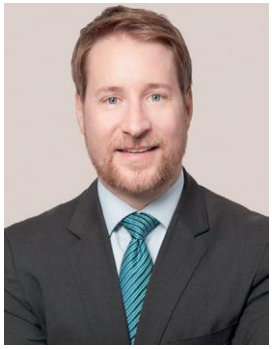
Canadian Privacy Law Review

VOLUME 15, NUMBER 9 Cited as (2018), 15 C.P.L.R. AUGUST 2018

• PRIVACY COMMISSIONER ISSUES KEY GUIDELINES FOR CONSENT AND INAPPROPRIATE DATA PRACTICES •

Alex Cameron, Partner, Daniel Fabiano, Partner, and Robin Spillette, Summer Student, Fasken Martineau LLP

Alex Cameron



Daniel Fabiano

Robin Spillette

On May 24, 2018, the Office of the Privacy Commissioner of Canada published two important guidance documents in respect of activities regulated pursuant to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"):

- Guidelines for Obtaining Meaningful Consent (the "Consent Guidelines"), which includes a checklist for consent and is effective on January 1, 2019; and
- Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3) effective on July 1, 2018 (the "Data Practices Guidance").

The publication of the above guidance documents comes on the heels of the Commissioner's consultation on consent and the recent updating of guidance on "Recording of Customer Telephone Calls". In this bulletin, we review the Consent Guidelines and Data Practices Guidance and highlight implications for organizations that are subject to PIPEDA.

• In This Issue •

LexisNexis®

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $325.00 per year (print or PDF)
$495.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

GUIDELINES FOR OBTAINING MEANINGFUL CONSENT

The Consent Guidelines provide that organizations should follow seven key principles in seeking to obtain meaningful consent under PIPEDA. These are reviewed below.

1. Emphasize Key Elements

Emphasizing key elements in consent (and any associated public-facing privacy policy) can improve an individual's understanding of the consequences of giving consent, and thereby contribute to meaningful consent. The Consent Guidelines provide that organizations must generally put particular emphasis on the following elements:

a) What personal information is being collected, used and disclosed: Organizations should identify all information that will or may be collected, with sufficient precision to permit individuals to understand what they are consenting to.

b) The purpose for which the information is being collected, used or disclosed: Organizations should describe these purposes in sufficient detail to ensure that individuals have a meaningful understanding of them; vague descriptions should be avoided. Any purposes that are not integral to the provision of the organization's products or services, and any uses that would not be reasonably expected given the context, should be emphasized.

c) Information-sharing with third parties: Where organizations share information with a large number of third parties, or where the parties may change over time, an organization should list the types of organizations with which they are sharing information, and give users the ability to access more details if they desire. Any third parties that will be using the information for their own purposes, rather than for advancing the purposes of the first party, should be emphasized.

d) Whether there is a risk of harm arising from the collection, use or disclosure of information: Organizations should consider emphasizing harms that may be associated with the activity for

which consent is sought, including both direct as well as indirect harms (*e.g.*, unauthorized use of information). The risk of harm refers to any risk of significant harm (that is, more than minimal or a mere possibility) after accounting for any mitigating procedures taken by the organization. Individuals must be aware of the consequences of their consent in order for that consent to be meaningful. This includes indirect risks, such as third party misuse of information.

2. Allow individuals to Control the Level of detail

Organizations should make privacy disclosures more manageable and accessible by allowing individuals to decide how, when, and how much information about an organization's privacy practices the individual accesses at any given time. Layered disclosure is one such approach. Layered disclosure starts by displaying more abstracted, general information, and allows individuals to obtain more detail on discrete topics if they wish. Additionally, privacy disclosures should be readily available so that an individual can return and re-read about an organization's privacy practices. This approach supports meaningful consent, as it allows individuals an opportunity to reconsider and potentially withdraw consent if they object to any of the organization's practices.

3. provide individuals with Clear Options to say 'yes' or 'no'

Organizations must not require individuals to consent to the collection, use or disclosure of more information than is necessary for the product or service which is being provided. For a collection, use, or disclosure to be "necessary", it must be integral to the provision of that product or service (*i.e.*, required to fulfill the explicitly specified and legitimate purpose). If any other information is to be collected on an opt-in or opt-out basis, individuals should be able to choose whether or not to consent to the collection of this additional information, and this choice should be clear and accessible, unless an exception to consent applies.

4. Be innovative and Creative

Organizations should think about moving away from simply transposing paper-based policies into their digital environments, and seek innovative ways to obtain consent. "Just-in-time" notices, for example, are an alternative to obtaining all consents "up-front". For example, a cell phone application that, rather than asking for access to location data upon installation, asks for this consent the first time the individual attempts to use the application in a way which requires location data, provides more context to the individual and a better understanding of what is being collected and why. Other interactive tools such as videos, or click-through presentations which explain privacy policies, and mobile interfaces, could also be used. Additional information regarding mobile apps is provided in the Commissioner's guidance: "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps".

5. Consider the target individual's perspective

To ensure that consents and privacy disclosures are user-friendly and understandable, organizations must be mindful of the perspective of target individuals. This involves the use of an appropriate level of language, clear explanations and a comprehensible display. It also involves consideration of the types of devices that target individuals will be using (laptops, mobile phones, tablets, etc.). Organizations may wish to understand the perspective of target individuals by consulting with them, running pilot tests and focus groups, engaging with privacy experts and following industry best-practices.

6. make Consent a dynamic and Ongoing process

Consent should be an ongoing, dynamic and interactive process (and not a one-off process). Periodic reminders and refreshers about an organization's privacy practices should be implemented, as well as an ongoing and practical ways for individuals to obtain more information.

7. Be accountable: Stand ready to demonstrate compliance

Organizations should be ready to prove that they have obtained meaningful consent, including showing that their consent process is understandable and accessible. One such way to do this is for organizations to be aware of these guidelines, as well as the guidance provided by the Commissioner in "Getting Accountability Right with a Privacy Management Program", and to show that they have followed them.

ADDITIONAL TOPICS ADDRESSED IN THE CONSENT GUIDELINES

appropriate form of Consent

In addition to the seven guiding principles above, the Guideline reminds organizations of the need to consider what type of consent is appropriate given the circumstances. While in some situations implied consent may be adequate, there are some circumstances which will generally require express consent, including: (a) when the information being collected, used or disclosed is sensitive in nature; (b) when an individual would not reasonably expect certain information to be collected, used or disclosed given the circumstances, and (c) when there is a more than minimal risk of significant harm.

CONSENT AND CHILDREN

Another contextual factor is whether the target individuals include children. When children are involved, organizations should take into account the fact that children will generally have different emotional and cognitive processing abilities than adults. This affects their ability to understand how their personal information is being used, and hence will affect their ability to give meaningful consent. The OPC requires that, for children 13 and under, a parent or guardian give consent on the child's behalf. When the target individuals include minors who are able to provide consent themselves, organizations should still take their maturity into account, and should be ready to show how they have done so.

At the conclusion of the Consent Guidelines, the Commissioner provides a useful checklist of "Should do" and "Must do" action items for organizations seeking to obtain meaningful consent under PIPEDA.

GUIDANCE ON INAPPROPRIATE DATA PRACTICES

Concurrently with publishing the Guidelines, the Commissioner published the Data Practices Guidance, which sets out various considerations that organizations should keep in mind when assessing whether a certain practice may be contrary to subsection 5(3) of PIPEDA.

Subsection 5(3) of PIPEDA is an overarching requirement which provides that: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances." In order words, even with an individual's consent, there are certain purposes that would be unacceptable under PIPEDA on the grounds that a reasonable person would not consider them to be appropriate.

Like meaningful consent, whether or not a purpose is inappropriate requires a contextual approach. As summarized in the Data Practices Guidance, the following factors have been applied by the Commissioner and the courts:

- 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 (which includes consideration of the degree of sensitivity of the personal information at issue).

In addition, as set forth in the Data Practices Guidance, the Commissioner has established a list of prohibited purposes under PIPEDA, which they

have deemed "No-Go Zones". The Commissioner considers that a reasonable person would not consider the collection, use or disclosure of information to be appropriate in these circumstances. Currently, the list of "No-Go Zones" may be summarized as follows:

- Collection, use or disclosure that is otherwise unlawful (*e.g.*, violation of another law);
- Collection, use or disclosure that leads to profiling or categorization that is unfair, unethical or discriminatory in a way which is contrary to human rights law;
- Collection, use or disclosure for purposes that are known or likely (on a balance of probabilities) to cause significant harm to the individual (*e.g.*, bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit record or damage to or loss of property);
- Publishing personal information with the intended purpose of charging individuals for its removal (*i.e.*, "blackmail");
- Requiring passwords to social media accounts for the purpose of employee screening; and
- Surveillance by an organization through the use of electronic means (*e.g.*, keylogging) or audio or video functionality of the individual's own device.

While these "No-Go Zones" are important to note, organizations should also remember that the list is not binding, determinative or exhaustive, and that subsection 5(3) requires a contextual analysis. What a reasonable person would consider appropriate is a flexible and evolving concept which will be revisited by the Commissioner from time to time.

IMPLICATIONS FOR ORGANIZATIONS SUBJECT TO PIPEDA

The Commissioner's guidance documents do not have the force of law and are not binding on organizations. However, they plainly set out the Commissioner's expectations, provide a benchmark against which the Commissioner will assess practices in the context of a complaint, audit or investigation, and provide a useful reference for organizations seeking to comply with PIPEDA.

It is also important to note that, over time, previous Commissioner guidance documents, including "Guidelines for Processing Personal Data Across Borders", have come to set the *de facto* standard and practices under PIPEDA. Organizations should familiarize themselves with the new guidance documents and consider steps to amend practices as necessary. For example, organizations which use mobile and online interfaces can refer to work which is already being done regarding the implementation of privacy icons, and privacy dashboards to help obtain meaningful consent. These and other potential solutions are discussed in the Commissioner's discussion paper, "Consent and Privacy".

Finally, in considering compliance with the new guidelines discussed in this bulletin, organizations should be mindful of the consequences of failing to obtain meaningful consent or failing to process information for appropriate purposes as required by PIPEDA. For example, a failure to obtain meaningful consent from a large number of individuals could undermine the basis upon which key business operations are premised. This could not only render those operations non-compliant with PIPEDA but also give rise to class action litigation risk for a privacy breach (*e.g.*, processing personal information for commercial purposes without adequate consent).