CCCA
ACCJE
Canadian Corporate Counsel Association
Association canadienne des conseillers (ères) juridiques d'entreprises

THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

PIPEDA: Draft Guidelines for Obtaining Meaningful Online Consent

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION AND
CANADIAN CORPORATE COUNSEL ASSOCIATION

December 2017

500–865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access Law Section and Canadian Corporate Counsel Association, with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law Section and Canadian Corporate Counsel Association.

TABLE OF CONTENTS

PIPEDA: Draft Guidelines for Obtaining Meaningful Online Consent

PIPEDA: Draft Guidelines for Obtaining Meaningful Online Consent

I. INTRODUCTION

The Canadian Bar Association Privacy and Access Law Section and Canadian Corporate Counsel Association (CBA Sections) are pleased to comment on *Draft guidelines: Obtaining meaningful online consent* (Consent Guidance) released by the Office of the Privacy Commissioner (OPC) in September 2017.

The CBA is a national association of over 36,000 members, including lawyers, notaries, academics and students across Canada, with a mandate to seek improvements in the law and the administration of justice. The CBA Privacy and Access Law Section comprises lawyers with an in-depth knowledge of privacy and access to information law, and the Canadian Corporate Counsel Association comprises in-house counsel working for public and private companies, not-for-profit associations, government and regulatory boards, hospitals and municipalities.

The CBA Sections have made numerous submissions on the *Personal Information Protection and Electronic Documents Act* (PIPEDA or the Act) since its enactment, including our most recent submissions, PIPEDA (March 2017) and Consent Model for Collection of Personal Information under PIPEDA (July 2016).[1]

II. PERSPECTIVE, VALUE AND NEED FOR GUIDANCE

The requirement for consent is a foundational component of PIPEDA. However, for consent to be valid – to allow individuals to exercise greater control over their personal information – consent must be meaningful. As revealed in a 2012 OPC study,[2] organizations' privacy practices are not always disclosed in an effective way to consumers. Given the increasing challenges of

---

1 Canadian Bar Association, PIPEDA (March 2017), available online (http://ow.ly/WUiV30gQxRC); and Canadian Bar Association, *Consent Model for Collection of Personal Information under PIPEDA* (July 2016), available online (http://ow.ly/Sus130gQxWc).

2 See Office of the Privacy Commissioner of Canada (September 2012), *OPC "web leakage" research project*, available online,(http://ow.ly/IkI330h0pjd) cited in Office of the Privacy Commissioner of Canada (May 2014), *Guidelines for Online Consent*, available online, (http://ow.ly/4D2H30h0ppw).

obtaining meaningful consent in today's ever-changing technological landscape, as well as the emphasis on consent in PIPEDA, the CBA Sections support the issuance of guidance on consent for organizations. The CBA Sections encourage the OPC to continue to seek input from stakeholders on its draft guidance before issuing final guidance. We would welcome any opportunity to review and comment on final guidance from the OPC before it is published.

The CBA Sections have continually advocated for an approach to privacy protection that balances individual privacy rights and the legitimate needs of businesses to collect, use and disclose personal information for reasonable purposes. Our comments on the Consent Guidance are informed by this perspective. We have reviewed the Consent Guidance from the perspective of how useful and helpful it would be for organizations in furthering their compliance with PIPEDA.

III. IMPLEMENTATION

The OPC asks how long it would take to implement its guidance. The CBA Sections note that the Consent Guidance is not intended to add new obligations, but rather to give organizations additional direction and suggestions on how to comply with existing obligations in a fast changing technological and business environment. Organizations vary in size, as do their suppliers, producers, and the services they offer. They can be established players or new market entrants, and in each case the purpose(s) for which consent may be required by these myriad of organizations will also vary. While organizations themselves are best placed to answer this question, we are not convinced of its relevance.

IV. PRESCRIPTIVE VS. PERMISSIVE LANGUAGE

The Consent Guidance shifts between prescriptive and permissive language. At times, it is unclear whether the prescriptive language is referencing statutory obligations or has added requirements beyond the Act. The CBA Sections recommend revising the language of the Consent Guidance to reflect that these are guidance materials. This approach would keep with the principles-based nature of PIPEDA and the approach to guidance previously taken by the OPC. We also recommend greater clarity to distinguish between legal obligations and guidance.

RECOMMENDATION

1. **The CBA Sections recommend revising the language of the Consent Guidance to reflect that these are guidance materials, and to distinguish, where applicable, between legal obligations and guidance.**

V. SPECTRUM OF EXAMPLES

The Consent Guidance currently gives examples of approaches for organisations to consider, with the goal of ensuring that consent processes are understandable, user-friendly and effective. Some of these examples require extensive resources and capacity, and in many cases represent a "gold standard" that is not realistic or practical for many organizations. The CBA Sections believe that the Consent Guidance should be sensitive to commercial realities – if not, it risks not being practical or actionable for organizations of all sizes. We encourage clarification in the Consent Guidance to avoid giving the impression that the examples are required or expected of all organizations. We also suggest that the Consent Guidance give a broader range of illustrative examples, considering small businesses in particular. In addition, we recommend adding a statement in the prefatory paragraph acknowledging that the OPC understands that the operational realities of each organization will continue to be taken into account in adopting best practices.

RECOMMENDATIONS

2. **The CBA Sections recommend (a) clarifying the Consent Guidance to avoid giving the impression that examples are expected or required of all organizations, and (b) giving a broader range of illustrative examples in the Consent Guidance, considering small businesses in particular.**
3. **The CBA Sections recommend adding a paragraph in the Consent Guidance stating that the OPC recognizes that operational realities of organizations will continue to be taken into account in adopting best practices.**

VI. RISK OF HARM

A. Consequences of Collection, Use and Disclosure

The CBA Sections appreciate that the concept of harm plays an important role in privacy protection. However, the Consent Guidance, as currently drafted, risks confusing the concept of

"risk of harm" with an individual's appreciation of the consequences that result from the collection, use or disclosure of personal information. Put another way, the Consent Guidance could cause an individual to believe a risk of harm exists every time personal information is provided to an organization. We encourage the OPC to further consider and clarify the relationship between "risk of harm" and consequences of collection, use and disclosure of personal information, as set out in section 6.1 of the Act. The discussion of "risk of harm" in the Consent Guidance, and particularly its inclusion as a key element required to obtain meaningful consent may take the Consent Guidance beyond the requirements of section 6.1 of PIPEDA. Additional clarification of the relationship between "consequences" and "risk of harm" and about the scope of disclosure is needed in offering organizations' guidance on obtaining consent.

Assuming there is no significant difference between the "risk of harm" concept in the Consent Guidance and the "consequences of the collection, use or disclosure" concept set out in s.6.1, the CBA Sections recommend replacing the subheading "Risk of Harm" with "Consequences of collection, use or disclosure". The text under this subheading should be revised to say: "Individuals should be made clearly aware of any known or foreseeable consequences arising from the collection, use or disclosure of personal information for any given purpose".

Subject to the below discussion about foreseeability and types of risk, the CBA Sections support guidance that encourages organizations to disclose the consequences of their collection, use and disclosure of individuals' personal information in a comprehensive, but plain language manner, that facilitates understanding of those consequences by lay people.

B. Foreseeability and Types of Risk

The concept of "risk of harm" opens up a grey area: it is difficult for organizations to determine all foreseeable harms as well as the level and remoteness of risk that warrants disclosure. Moreover, given the competitive environment in which most organizations subject to PIPEDA operate, it is unrealistic to expect an organization to make those disclosures if its competitors are not clearly required to do likewise and if the requirements are not effectively enforced to ensure a level playing field in the marketplace. To the extent that the "risk of harm" guidance is suggestive and not enforceable, it may not be in the interests of organizations to follow it even where they are able to do so.

The Consent Guidance is unclear as to the *types* of risk that organizations are expected to disclose. For this part of the Consent Guidance to be useful to organizations, the CBA Sections

recommend more clarity and detail as to the nature of risk contemplated by the guidance. We discuss below several considerations and questions about the types of risk that organizations may be expected to disclose.

Risks of Security Breaches

The CBA Sections question whether organizations are expected to disclose the risk of a security breach, despite compliance with PIPEDA security requirements, or to disclose risks arising from unforeseen failure of the organization's security safeguards (or those of entities with whom it shares the data) – i.e., risks that arise purely by virtue of the information being collected and stored.

Third Party Access

The CBA Sections question whether organizations are expected to disclose the fact that the information is necessarily available for access by law enforcement agencies, fraud investigators and others authorized under PIPEDA. If so, are they expected to enumerate the types of harm to individuals that access could entail? We also question whether organizations are expected to disclose the risk that personal information could end up in the possession of an unidentified third party with less effective security measures or for purposes that have not been identified and consented to.

Remote Risks

The CBA Sections question whether organizations are expected to identify and disclose remote risks arising from the increasing use of data analytics, consumer targeting and personalization of offers. If so, how are they expected to explain those risks.

In reviewing the Consent Guidance, some members of the CBA Sections assumed that references to "risk of harm" in the Consent Guidance are not intended to require organizations to enumerate in their consent materials any known or foreseeable risk of harms that could arise from the unforeseen failure of the organization's safeguards. If that assumption is incorrect, then the language in the Consent Guidance should be clarified on this point. They note, however, a concern about imposing an obligation on organizations, since they believe that the current language of PIPEDA does not require organizations to inform individuals about risk of harm when obtaining consent.

RECOMMENDATIONS

4. **The CBA Sections recommend clarifying the relationship between risk of harm and consequences of collection, use and disclosure of personal information, as set out in section 6.1 of PIPEDA.**
5. **The CBA Sections recommend clarifying the types of risks that organizations are expected to disclose.**
6. **The CBA Sections recommend replacing the subheading "Risk of Harm" in the Consent Guidance with "Consequences of collection, use or disclosure".**
7. **The CBA Sections recommend revising the text under the subheading "Risk of Harm" to say: "Individuals should be made clearly aware of any known or foreseeable consequences arising from the collection, use or disclosure of personal information".**

VII. APPLICATION OF IMPLIED AND EXPRESS CONSENT

The CBA Sections are concerned about the following statement in the Consent Guidance about the appropriate form of consent: "[w]hile consent should generally be express, it can be implied in strictly defined circumstances", and its attribution to the recent Supreme Court of Canada decision in *Royal Bank of Canada v. Trang.*[3]

First, PIPEDA does not state any general preference to one form of consent over another. Rather, Section 4.3.6 of Schedule 1 to PIPEDA states that the form of consent may vary, according to the circumstances:

> The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

While Schedule 1 states that express consent will generally be required for sensitive personal information, it equally provides that implied consent is generally appropriate for non-sensitive information, and acknowledges that consent can be reasonably implied in certain situations.

---

3 SCC 2016 50 [*Trang*].

Nothing in PIPEDA suggests as a general requirement that the form of consent required for the collection, use and disclosure of personal information should be express, and nothing supports the notion that implied consent may only be used in "strictly defined circumstances." Instead, with the recent addition of section 6.1, PIPEDA's consent requirements focus on the meaningfulness of consent obtained via whatever method is employed, express or implied. Consent may be implied if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure in question.

If, rather than stating the law, the OPC meant to recommend (as guidance) that organizations generally seek express consent and rely on implied consent only in "strictly defined circumstances", this part should be revised to make that clear and should include more guidance on the "strictly defined circumstances" to which it refers.

Second, the decision in *Trang* does not support the notion that PIPEDA generally requires express consent. In *Trang*, the personal information at issue was a mortgage discharge statement, containing financial information such as the principal amount registered, the remaining balance and the applicable interest rate. Typically, financial information is considered to be sensitive – a point argued by the OPC and explicitly accepted by the Court in *Trang*. The Court also indicated[4] that the degree of sensitivity of specific financial information is a contextual determination. The Court's comments about consent in *Trang* must therefore be read in that context (and also taking into account the plain wording of PIPEDA). In particular, the Court's statement to the effect that PIPEDA generally requires express consent should be read as noting that the Act generally requires express consent *when dealing with sensitive information*. Similarly, the statement that "implied consent may be accepted in strictly limited circumstances" should be read as saying "implied consent *with respect to the disclosure of less sensitive financial information* may be accepted in strictly limited circumstances."

Indeed, *Trang* ultimately found that, notwithstanding the general requirement for express consent for financial information, the mortgage statement at issue could be disclosed to the judgment creditor based on implied consent, taking into account the particular circumstances of that case. In *Trang,* parts of the mortgage information at issue were already in the public domain - this financial information was made available to the public for the purpose of allowing creditors to make informed decisions. The OPC correctly cites *Trang* in the third sentence under "Determining the Appropriate Form of Consent" in the Consent Guidance.

[4] *Ibid*. at para 36.

The Consent Guidance should be revised to clarify the reference to *Trang* and to correctly characterize PIPEDA's requirements respecting the form of consent.

RECOMMENDATION

8. **The CBA Sections recommend revising the Consent Guidance to clarify the reference to *Trang* and to correctly characterize PIPEDA's requirements on the form of consent, by revising the statement: "[w]hile consent should generally be express, it can be implied in strictly defined circumstances."**

VIII. CONCLUSION

The CBA Sections appreciate the opportunity to comment on the Consent Guidance. We encourage the OPC to continue to give guidance to organizations on compliance under PIPEDA, and we trust that our comments will be of assistance in obtaining meaningful consent. We would be pleased to offer any clarifications or discuss any of these matters in further detail.

IX. SUMMARY OF RECOMMENDATIONS

The CBA Sections recommend:

1. **revising the language of the Consent Guidance to reflect that these are guidance materials, and to distinguish, where applicable, between legal obligations and guidance.**
2. **(a) clarifying the Consent Guidance to avoid giving the impression that examples are expected or required of all organizations, and (b) giving a broader range of illustrative examples in the Consent Guidance, considering small businesses in particular.**
3. **adding a paragraph in the Consent Guidance stating that the OPC recognizes that operational realities of organizations will continue to be taken into account in adopting best practices.**
4. **clarifying the relationship between risk of harm and consequences of collection, use and disclosure of personal information, as set out in section 6.1 of PIPEDA.**
5. **clarifying the types of risks that organizations are expected to disclose.**
6. **replacing the subheading "Risk of Harm" in the Consent Guidance with "Consequences of collection, use or disclosure".**
7. **revising the text under the subheading "Risk of Harm" to say: "Individuals should be made clearly aware of any known or foreseeable consequences arising from the collection, use or disclosure of personal information".**

8. **revising the Consent Guidance to clarify the reference to *Trang* and to correctly characterize PIPEDA's requirements on the form of consent, by revising the statement: "[w]hile consent should generally be express, it can be implied in strictly defined circumstances."**