Guidelines for

Obtaining Meaningful Consent

Meaningful consent is an essential element of Canadian private sector privacy legislation. Under privacy laws, organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information. However, advances in technology and the use of lengthy, legalistic privacy policies have too often served to make the control – and personal autonomy – that should be enabled by consent nothing more than illusory. Consent should remain central, but it is necessary to breathe life into the ways in which it is obtained.

Building on previous publications examining the current state of consent, including challenges and potential solutions[1], this document sets out practical and actionable guidance regarding what organizations should do to ensure that they obtain meaningful consent.

This document is being jointly issued by the Office of the Privacy Commissioner of Canada ("OPC") and the Offices of the Information and Privacy Commissioner of Alberta ("OIPC-AB") and British Columbia ("OIPC-BC"). It reflects the principles underlying the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and its substantially similar provincial counterparts: the *Alberta Personal Information Protection Act*; the British Columbia *Personal Information Protection Act*; and, the Quebec Act *Respecting the Protection of Personal Information in the Private Sector*.[2] While all of these Acts are based on the same underlying principles, some differences exist. Organizations are responsible for understanding their specific obligations under the legislation to which they are subject.[3]

Seven Guiding Principles for Meaningful Consent

During the OPC's 2016 Consent Consultations, some suggested that regulators develop templates for privacy policies; we do not believe that should be our role. Rather, our view is that organizations are best placed to find innovative and creative solutions for developing a consent process that respects their specific regulatory obligations as well as the nature of their relationship with their customers. However, in designing such a process, we expect organizations to be guided[4] by the following principles:

1 For instance, the OPC's "A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act" and the outcome of that discussion, the "Report on Consent."

2 Note that the Quebec Commission d'accès à l'information ("Québec CAI") is not a signatory to this document.

3 For specific questions about how these guidelines apply to your organization, please contact the Commissioner's office in your jurisdiction.

4 In this document, the use of the word "shall" indicates an obligation, whereas the use of the word "should" indicates a recommended best practice.

Office of the Information and Privacy Commissioner of Alberta

May 2018

1. Emphasize Key Elements

Information provided about the collection, use and disclosure of individuals' personal information must be readily available in complete form – but to avoid information overload and facilitate understanding by individuals, certain elements warrant greater emphasis or attention in order to obtain meaningful consent.

PIPEDA requires individuals to understand the nature, purpose and consequences of what they are consenting to[5]. In order for consent to be considered valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner[6]. This means that organizations must provide information about their privacy management practices in a form that is readily accessible to those interested individuals who wish to read it in full.

However, the reality is that information buried in a privacy policy or terms of use serves no practical purpose to individuals with limited time and energy to devote to reviewing privacy information. To receive meaningful consent, organizations must allow individuals to quickly review key elements impacting their privacy decisions right up front as they are considering using the service or product on offer, making the purchase, or downloading the app, etc. For this purpose, organizations must generally put additional emphasis on the following key elements:

- What personal information is being collected

  Organizations must identify for individuals what personal information is being, or may be, collected about them. This must be done with sufficient precision for individuals to meaningfully understand what they are consenting to.[7]

- With which parties personal information is being shared

  Individuals expect that the personal information they provide to one organization will not be shared with another without their knowledge and consent. As such, disclosures to third parties must be clearly explained, including the types of information being shared. Organizations should be as specific as possible in enumerating these third parties. In the case where third parties may change periodically or are too numerous to specify, organizations should at the very least specify the types of third parties information is shared with and then use other means (such as layering) to be more specific. Particular attention should be paid to any disclosures to third parties that may use the information for their own purposes, as opposed to simply providing services for the first party.

- For what purposes personal information is collected, used or disclosed

  Individuals should be made aware of all purposes for which information is collected, used or disclosed. At a minimum, they must be informed of purposes in sufficient detail such as to ensure they meaningfully understand what they are invited to consent to. These purposes must be described

5 Please consult relevant legislation in Alberta, British Columbia and Quebec for specific language on valid consent in those provinces.

6 For further practical advice for BC organizations, please refer to BC's guidance document entitled "Practical Suggestions for your Organization's Website's Privacy Policy".

7 Organizations may also wish to indicate that additional information may be collected over the course of the business relationship, and that consent will be sought prior to such collections. See Principle 6 – Make consent an ongoing and dynamic process.

in meaningful language, avoiding vagueness like 'service improvement'. Purposes that are integral to the provision of the service should be distinguished from those that are not, and any available options explained. Organizations should in particular highlight any purposes that would not be obvious to the individual and/or reasonably expected based on the context.

- Risk of harm and other consequences

  Under PIPEDA[8], for consent to be valid, it must be reasonable to expect that individuals understand the consequences of the collection, use or disclosure to which they are consenting[9]. One such consequence, about which individuals should be made clearly aware, is risk of harm – and, in particular, those residual risks which remain after an organization has applied any mitigation measures designed to minimize the risk and impact of potential harms. If there is a meaningful risk that such residual risk will materialize and will be significant, the OPC is of the view that it is a potential consequence about which individuals must be notified.

  The OPC's premise is that if an organization identifies potential harms that may arise from the collection, use or disclosure of personal information, PIPEDA's accountability principle will require that the organization will seek to minimize this risk. In some cases, mitigation efforts will reduce the risk significantly. In other cases the risk will remain meaningful. Only meaningful residual risks of significant harm must be notified to individuals.

  By meaningful risk, we mean a risk that falls below the balance of probabilities but is more than a minimal or mere possibility. 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.[10]

  Note that where there is a likely (probable) risk of significant harm, the intended collection, use or disclosure would generally be considered inappropriate under subsection 5(3) of PIPEDA and therefore should not be the subject of consent.

  Risk of harm should be considered broadly, and in addition to harms which arise directly from the activity, can include reasonably foreseeable harms caused by bad actors or others[11] (e.g. unauthorized re-use of social media information intended for a limited audience).

At this time, there is no prescribed form in which the above elements should be highlighted so as to give them prominence. We encourage organizations to consider adopting standardized mechanisms, to the extent that best practices emerge in the future in different sectors. Organizations should also consider the principles which follow in this document in determining the most appropriate means of communicating these key elements, while keeping in mind the requirement for additional emphasis on this information.

8 This language is not currently in the Personal Information Protection Acts of Alberta or British Columbia.

9 PIPEDA subsection 6.1: "For the purposes of clause 4.3 [Consent] of Schedule 1, the consent of an individual 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."

10 Section 10.1(7) of PIPEDA; coming into force November 1, 2018.

11 The potential risk of data breach – and the security safeguards put in place to mitigate this risk – do not need to be given additional emphasis, but should be discussed within the organization's full privacy disclosure.

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

Information must be provided to individuals in manageable and easily-accessible ways (potentially including layers) and individuals should be able to control how much more detail they wish to obtain, and when.

Beyond the four elements above, the level of detail required to make a consent decision will vary by individual, and by situation. One person may be comfortable with a quick review of summary information; another may want to do a deeper dive. One person may want to do a more in-depth review of an organization's privacy practices up-front; another may look at information piece-meal, returning to it later when they have more time or depending on what services they are using and when. Individuals may also want the opportunity to review in detail the information that they 'clicked-through' when they signed up for the service originally. All approaches to seeking privacy information should be respected and supported by organizations.

Presenting information in a layered-format[12], or by another means that supports user-control over the level of detail provided to them, helps make better sense of lengthy, complex information by offering a summary of the key highlights up front. Moreover, this information should remain available to individuals as they engage with the organization. Consent choices are not made just once; at any time, individuals should be able to re-consider whether they wish to maintain or withdraw their consent, and full information should be available to them as they make those decisions.

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

Individuals cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service – they must be given a choice. These choices must be explained clearly and made easily accessible. Whether each choice is most appropriately 'opt-in' or 'opt-out' will depend on factors discussed in the "Form of Consent" section of this document.

Collections, uses or disclosures of personal information over which the individual cannot assert any control (other than to not use a product or service) are called conditions of service. For a collection, use, or disclosure to be a valid condition of service, it must be integral to the provision of that product or service such that it is required to fulfill its explicitly specified and legitimate purpose. Organizations should be transparent and prepared to explain why any given collection, use or disclosure is a condition of service, particularly if it is not obvious.

Otherwise, for all other collections, uses and disclosures, individuals must be given a choice (unless an exception to the general consent requirement applies).

4. Be innovative and creative

Organizations should design and/or adopt innovative consent processes that can be implemented just-in-time, are specific to the context, and are appropriate to the type of interface used.

When seeking consent online, organizations should do more than simply transpose in digital form, their paper-based policies from the offline environment. The digital environment is dynamic in nature, and its capabilities should be considered and taken advantage of. Organizations are encouraged to use a variety

12 The Center for Information Policy Leadership, Hunton & Williams LLP. "Ten steps to develop a multilayered privacy notice.".

of communications strategies – including "just-in-time" notices, interactive tools and customized mobile interfaces – to explain their privacy practices, including the following:

"Just-in-time" notices

An important consideration in obtaining meaningful consent in the online environment is the speed with which transactions take place. In wanting to quickly access information and services, users often feel a sense of urgency in making decisions about sharing their information. It is therefore important for organizations to bring relevant privacy information to the forefront where it is conspicuous, quick to access, and intuitive. For example, if a user's age is being requested to register for an online service, a just-in-time notice explaining why this information is needed should appear near the space where the user would input the information. As another example, if a user's location is required to enable a certain feature of a service, a just-in-time notice explaining this and requesting access can be made when that user first accesses the feature, rather than only when signing up for the service originally.

Interactive Tools

Organizations have also been using the interactive properties of the Internet to aid in the presentation of privacy information. We have seen examples in which organizations create interactive walkthroughs of their privacy settings (presenting them to users at initial sign-up, and then again periodically as 'refreshers'), videos explaining key concepts, and/or infographics and similar visual tools.

Customized mobile interfaces

Mobile devices present an amplified communication challenge. Individuals' time and attention are at a premium, and the medium does not lend itself to lengthy explanations. As such, organizations need to highlight privacy issues at particular decision points in the user experience where people are likely to pay attention and need guidance the most. In that context, privacy information needs to be optimized to be effective in spite of the physical limitations of screen size. Our mobile apps guidance is a good resource when designing the mobile consent experience.

5. Consider the consumer's perspective

Consent processes must take into account the consumer's perspective to ensure that they are user-friendly and that the information provided is generally understandable from the point of view of the organization's target audience(s).[13]

Consent is only valid where the individual can understand that to which they are consenting. Organizations put significant resources into the design of user experiences and interactions; surely, they can put similar efforts toward ensuring that their consent process is understandable, user-friendly and customized to the nature of the product or service they are offering as well as their target audiences.

Organizations should consider both the content of privacy communications and their accessibility from the perspective of their users. This includes using clear explanations, a level of language suitable to a diverse audience, and a comprehensible means of displaying and/or communicating information.

Organizations should also ensure that privacy policies and notices are easily accessible from all devices members of their target audience(s)may be using, including digital health technologies, smart phones,

13 For instance, see footnote 9, which sets out Section 6.1 of PIPEDA.

tablets, gaming devices, as well as more traditional PCs or laptops. If the practices being described are complex and involve multiple parties, the organization should make a concerted effort to ensure that users can easily access and understand all of the key elements.

In order to do all of this effectively, organizations may consider:

- Consulting with users and seeking their input when designing a consent process;
- Pilot testing or using focus groups to ensure individuals understand what they are consenting to;
- Involving user interaction/user experience (UI/UX) designers in the development of the consent process;
- Consulting with privacy experts and/or regulators when designing a consent process; and/or,
- Following an established 'best practice,' standard or other guideline in developing a consent process.

The suggestions above are non-exhaustive, and are intended to be scalable depending on the size of organizations and the amount and type of personal information they collect, use or disclose.

6. Make consent a dynamic and ongoing process

Informed consent is an ongoing process that changes as circumstances change; organizations should not rely on a static moment in time but rather treat consent as a dynamic and interactive process.

Ensuring the effectiveness of individual consent is a dynamic process that does not end with the posting of a privacy policy or notice, but rather, continues as organizations innovate, grow and evolve. When information flows are complex, as they often are, organizations should provide some interactive and dynamic way to anticipate and answer users' questions if the information provided is not clear or gives rise to follow-up questions. While providing 1-800 numbers may not be feasible or practical in a fast-paced online environment, there are myriad other ways organizations can do this, such as, developing and regularly updating FAQs, using new smart technologies, chatbots, etc.

When an organization plans to introduce significant changes to its privacy practices, it must notify users and obtain consent prior to the changes coming into effect. Significant changes include using personal information for a new purpose not anticipated originally or a new disclosure of personal information to a third party for a purpose other than processing that is integral to the delivery of a service.

Organizations should also consider periodically reminding individuals about their privacy options and inviting them to review these.

Lastly, as a best practice, organizations should periodically audit their information management practices to ensure that personal information continues to be handled in the way described to individuals.

7. Be accountable: Stand ready to demonstrate compliance

Organizations, when asked, should be in a position to demonstrate compliance, and in particular that the consent process they have implemented is sufficiently understandable from the general perspective of their target audience(s) as to allow for valid and meaningful consent.

In order for an organization to demonstrate that it has obtained valid consent, pointing to a line buried in a privacy policy will not suffice. Instead, organizations should be able to demonstrate – either in the case of a complaint from an individual or a proactive query from a privacy regulator – that they have a

process in place to obtain consent from individuals, and that such process is compliant with the consent obligations set out in legislation. This is an integral part of not only the consent process, but of an effective accountability regime.

Such demonstrations may include – but are not limited to – showing, when called upon, that the organization has considered and implemented the principles in this document. Again, regulators' expectations around the steps an organization has taken to demonstrate compliance and accountability will depend on the size of organizations and the amount and type of personal information they collect, use or disclose.

For general information on privacy management practices, please refer to our guidance document, "Getting Accountability Right with a Privacy Management Program."

Determining the Appropriate Form of Consent

Beyond the above principles, it is important for organizations to consider the appropriate form of consent to use (express or implied) for any collection, use or disclosure of personal information for which consent is required. While consent should generally be express, it can be implied in strictly defined circumstances.[14] The Supreme Court of Canada has recently confirmed that in making this determination, organizations need to take into account the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context.[15]

Organizations must generally obtain express consent when:

- The information being collected, used or disclosed is sensitive;
- The collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,
- The collection, use or disclosure creates a meaningful residual risk of significant harm.[16]

Sensitivity

There is no "bright line" separation of what is, and is not, sensitive information. Certain categories of information (such as health or financial) will generally be considered sensitive, but even non-sensitive information can become sensitive depending on the circumstances. For example, an individual piece of information considered non-sensitive on its own, could become sensitive depending on what it is capable of revealing when combined with other personal information about the individual.[17] Conversely, in certain circumstances, personal information generally considered sensitive may become less so where other related information is already in the public domain, depending on the purpose for which such information is being made public and the nature of the relationship between the parties involved.[18]

Reasonable expectations

In determining the appropriate form of consent, organizations should also consider the reasonable expectations of the individual in the circumstances. For example, if there is a use or disclosure a user

14 *Royal Bank of Canada v. Trang*, 2016 SCC 50 § 23. See also Alberta PIPA, sections 8(2) – 8(2.2), 8(4).

15 Ibid.

16 See the discussion of meaningful residual risk of significant harm earlier in this document (Guiding Principle for Online Consent 1: Emphasize Key Elements).

17 *R. v. Spencer*, 2014 SCC 43; See also OPC Report of Findings #2015-001.

18 *Royal Bank of Canada v. Trang*, 2016 SCC 50 § 36.

would not reasonably expect to be occurring, such as certain sharing of information with a third party, the downloading of photos or contact lists, or the tracking of location, express consent would likely be required.

In some cases, other contextual factors may come into play. For example, where an organization considers disclosure to a third party, the identity of the third party and their purpose in seeking access to the information may be relevant. Depending on the circumstances, an individual might reasonably expect that information could be disclosed to a third party with a legal entitlement to it; however, an individual would not reasonably expect disclosure to individuals who are merely curious or seek the information for nefarious purposes.[19]

Risk of harm

Underlying the contextual analysis of both sensitivity and reasonable expectations is risk of harm to the individual. Harm should be understood broadly, including material and reputational impacts, restrictions on autonomy, and other factors. Guiding Principle 1, above, states that individuals must be notified where there is a meaningful risk that a residual risk of harm will materialize and will be significant. The OPC is of the view that in such a situation, an individual would reasonably expect that consent for such a collection, use or disclosure would be express, not implied. Again, this assumes that the risk of harm does not meet a threshold which would contravene the "appropriate purpose" requirement described below (e.g. where there is a likely or probable risk of significant harm), in which case the purpose would be considered offside subsection 5(3) of PIPEDA.

Consent and Children

The ability of children and youth to provide meaningful consent for the sharing of their personal information depends greatly on their cognitive and emotional development. Given the difficulties that adults have in understanding what is happening with their personal information in a complex environment, it would be unrealistic to expect children to fully appreciate the complexities and potential risks of sharing their personal information. In recognition of this, private sector privacy legislation allows for consent through an authorized person, such as a parent or legal guardian.

We recognize that the maturation process is an evolving one, as youth are introduced to– and thus begin to develop an understanding of - information-based services at increasingly early ages. The OPC is of the view that while a child's capacity to consent can vary from individual to individual, there is nonetheless a threshold age below which young children are not likely to fully understand the consequences of their privacy choices, particularly in this age of complex data-flows. On the other hand, the OIPC-AB, OIPC-BC and Quebec CAI do not set a specific age threshold, but rather consider whether the individual understands the nature and consequences of the exercise of the right or power in question.[20] As such, where a child is unable to meaningfully consent to the collection, use and disclosure of personal information (the OPC takes the position that, in all but exceptional circumstances, this means anyone under the age of 13), consent must instead be obtained from their parents or guardians. For minors

19 Ibid, §§ 45-46.

20 However, in Quebec youth under 14 cannot give consent for medical care, nor are they able to request access to personal information of a medical or social nature.

able to provide meaningful consent, consent can only be considered meaningful if organizations have reasonably taken into account their level of maturity in developing their consent processes and adapted them accordingly. Organizations undertaking such collections, uses or disclosures should pay special mind to Guiding Principle 7, and stand ready to demonstrate on demand that their chosen process leads to meaningful and valid consent.

What Else Should Organizations Know About Consent?

Lastly, there are some final considerations which need to be kept in mind by organizations designing their consent processes.

Appropriate purpose

It is important to remember that the purposes for which an organization collects and uses personal information must be appropriate and defined. Even with consent, privacy laws require organizations to limit collection, use and disclosure of personal information to purposes that a reasonable person would consider appropriate under the circumstances[21]. In other words, an individual's consent is not a free pass for organizations to engage in collecting and using personal information indiscriminately for whatever purpose they choose.

Withdrawing consent

Under private sector privacy laws, individuals have the right to withdraw consent, subject to legal or contractual restrictions. Withdrawal of consent should be respected and put a stop to any further collection and use of the individual's personal information. It may also mean that data held by an organization about an individual should be deleted depending on the circumstances. For example, if a user deletes his account on a social networking site, the organization should delete his personal information on the site. There may be limited circumstances where an organization may need to retain some information about an individual who has withdrawn consent. For example, a "do not contact" list of email addresses could be retained for individuals who have requested no further communication from an online service. Moreover, other laws may require that information be retained. For example, financial sector legislation and regulations require organizations to retain information such as client credit files and credit card applications for five years from the day of closing of the account to which they relate.[22]

Consent is not a silver bullet

Finally, it is important to note that consent does not waive an organization's other obligations under privacy laws, such as overall accountability, collection limitation, and safeguards. In other words, if an individual consented to have their personal information handled contrary to legal requirements, the organization would still be considered in contravention of those requirements.

21 Inappropriate data practices – interpretation and application of subsection 5(3)

22 *Guideline 6G: Record Keeping Requirements for Financial Entities*, Financial Transactions and Reports Analysis Centre of Canada, June 2017.

Checklist

The measures set out in this document can be separated into obligations arising from legal requirements (those things an organization must do to obtain meaningful consent) and best practices (those things an organization should consider in order to improve their consent process). We recommend reading the entire document in order to understand context and nuance and reading your jurisdiction's legislation for your specific legal obligations, but we provide the following checklist as a quick reference.

Must Do

To obtain meaningful consent and meet their related obligations under Canadian privacy law, organizations must:

- [ ] Make privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:
    - What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to.
    - With which parties personal information is being shared
    - For what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to.
    - Risks of harm and other consequences
- [ ] Provide information in manageable and easily-accessible ways.
- [ ] Make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service.
- [ ] Consider the perspective of your consumers, to ensure consent processes are user-friendly and generally understandable.
- [ ] Obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties.
- [ ] Only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate, under the circumstances.
- [ ] Allow individuals to withdraw consent (subject to legal or contractual restrictions).

Form of Consent

- [ ] Obtain explicit consent for collections, uses or disclosures which generally: (i) involves sensitive information; (ii) are outside the reasonable expectations of the individual; and/or (iii) create a meaningful residual risk of significant harm.

Consent and Children

- [ ] Obtain consent from a parent or guardian for any individual unable to provide meaningful consent themselves (the OPC takes the position that, in all but exceptional circumstances, this means anyone under the age of 13), and ensure that the consent process for youth able to provide consent themselves reasonably considers their level of maturity.

Should Do

- [ ] Allow individuals to control the amount of detail they wish to receive, and when.

- [ ] Design or adopt innovative and creative ways of obtaining consent, which are just-in-time, specific to the context, and suitable to the type of interface.

- [ ] Periodically remind individuals about the consent choices they have made, and those available to them.

- [ ] Periodically audit privacy communications to ensure they accurately reflect current personal information management practices.

- [ ] Stand ready to demonstrate compliance – in particular, that the consent process is understandable from the perspective of the user.

- [ ] In designing consent processes, consider:

    - Consulting with users and seeking their input;
    - Pilot testing or using focus groups to evaluate the understandability of documents;
    - Involving user interaction / user experience (UI/UX) designers;
    - Consulting with privacy experts and/or regulators; and/or,
    - Following established best practices or standards.