Guidelines for Online Consent

Office of the Privacy Commissioner of Canada

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner of Alberta

> *"The evidence before the Committee points to the difficulties faced by Canadians when they are asked to provide their knowledge and consent for social media contracts and agreements. It is imperative for the healthy operation of Canada's privacy laws and the safeguarding of individuals' privacy interests that, when consent is given, such consent be meaningful and appropriate in the circumstance, as provided in the PIPEDA principles. The Committee notes that to achieve this, the language put before individuals should be clear and accessible."*

Privacy and Social Media in the Age of Big Data: A Report of the Standing Committee on Access to Information, Privacy and Ethics
April, 2013

1. Introduction

Meaningful consent is an essential element of Canadian private sector privacy legislation. Under privacy laws, organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals understand what organizations are doing with their information.

A 2012 study by the Office of the Privacy Commissioner of Canada (OPC) of popular Canadian websites found that organizations' privacy practices, such as the sharing of personal information with third parties, were not always disclosed in an effective way to consumers online. Moreover, the first-ever Global Privacy Enforcement Network (GPEN) privacy sweep which included participation by the OPC and the British Columbia Office of the Information and Privacy Commissioner - found significant shortcomings in how organizations communicate their privacy practices to consumers. These findings suggest that many companies seem to be struggling with the issue of online consent.

As a result, the OPC, together with the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, have published these guidelines to address the issue of consent requirements under private sector privacy laws and to set out our expectations regarding what organizations should do to ensure that they obtain meaningful consent in the online environment. In practice, this means organizations should have a clear, descriptive and accessible privacy policy and, as circumstances warrant, dynamic privacy explanations, in the course of the user experience.

This document reflects the principles of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and the Alberta and British Columbia *Personal Information Protection Acts* (AB PIPA and BC PIPA). While the AB and BC PIPAs are substantially similar to PIPEDA and all three 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.[1]

What is considered personal information?

Canadian private sector privacy legislation defines personal information as information about an identifiable individual. The Federal Court has ruled that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

A range of data that is specific to the online environment can be considered personal data under specific circumstances,[2] for example:

- location information, including GPS data;
- device identifiers such as IP and MAC address;
- click stream data[3], browser history, bookmarks; and,
- user generated social network data such as comments, ratings, likes and dislikes, Twitter stream, customer service interactions.

Combining disparate bits of information, derived from multiple sources, can also lead to detailed profiles that enable individuals to be identified. Organizations using advanced analytic techniques should be especially mindful of the definition of personal information, as the possibility of re-identification of anonymous data has increased dramatically with advances in technology that allow for vast amounts of data to be collected and combined.

Online challenges to transparency and meaningful consent

The key to obtaining meaningful consent is openness and transparency. When organizations clearly explain their information management practices, and make those explanations easily accessible, individuals are in a better position to make informed decisions about sharing their personal information. Understanding what organizations do with personal information is essential for users when deciding with whom to share personal information and under what circumstances.

Nowhere is this more important than in the online and mobile environments, where complex information management practices, new business models and technological innovation can be

---

[1] For specific questions about how these guidelines apply to your organization, please contact the Commissioner's office in your jurisdiction.
[2] Please address any questions about the definition of personal information to the Commissioner's office in your jurisdiction.
[3] Clickstream data is a record of a user's activity on the Internet, including every page of every website that the user visits, how long the user was on a page or site, and the order in which pages were visited (from webopedia.com)

confusing, if not bewildering, to the average user. Smart phones pose a particular challenge because they collect an extra layer of personal information, including location, which adds complexity to privacy protection. Also, their advanced and multifaceted data collection and processing capabilities reside behind a small screen where privacy explanations must compete for space and user attention.

Technological advances have greatly enhanced organizations' capacity to collect, process and share huge quantities of data in the blink of an eye. With the evolution of the social web and the pervasiveness of data analytics, data collection and processing happens not just on our screens but behind the scenes, where any number of invisible companies can be accessing our personal information. As for people's online behaviour, getting timely access to a service or activity is often our priority when online. Research shows that people want access to an online service or "app" the moment they visit a web site, and tend to click through quickly to do so. It is not surprising that they may devote little attention to seeking out information about privacy protection. This fast paced, data driven and multi-layered environment therefore requires a thoughtful approach to privacy disclosures.

Privacy is a competitive advantage

We recognize that finding ways to supplement privacy policies may require some extra effort and creativity, especially in the mobile environment. However, we are confident in organizations' ability to come up with new and innovative solutions to enhance transparency. Being forward thinking in this area is not only important for privacy but also for organizations' relationship with their users.

Openness about privacy practices and easier user access to that information will lead to greater consumer trust, which is good for business. Privacy is, more than ever, a material consideration in consumers' decisions to purchase or use products and services. Organizations that win and maintain trust in this area will realize a competitive advantage. If people are confident about putting their personal information online, they can more fully participate in the digital economy, which will spur innovation and create economic benefits for Canada.

2. Privacy 101: Consent is required

Under Alberta and British Columbia PIPAs, as well as PIPEDA, organizations are required to obtain consent for the collection, use and disclosure of personal information.

Consent must be meaningful

Privacy laws require individuals to understand what they are consenting to. In order for consent to be considered valid, or meaningful, organizations have to inform individuals of their privacy practices in a comprehensive and understandable manner. Being informed about and understanding an organization's policies and practices allow individuals to provide meaningful consent. Individuals should be able to understand the risks and benefits of sharing their personal information with the organization and be in a position to freely decide whether to do so. Organizations are required to make readily available their policies and practices for the management of personal information. These policies and practices should be clear, comprehensive, and easy to find. If the practices being described are complex and involve

multiple parties, the organization should make a concerted effort to ensure that users can understand all of the elements of the process, including what types of third parties are involved and why.

Under Alberta and British Columbia PIPAs, as well as PIPEDA, organizations are required to obtain consent for the collection, use and disclosure of personal information.

Consent must be meaningful

Privacy laws require individuals to understand what they are consenting to. In order for consent to be considered valid, or meaningful, organizations have to inform individuals of their privacy practices in a comprehensive and understandable manner. Being informed about and understanding an organization's policies and practices allow individuals to provide meaningful consent. Individuals should be able to understand the risks and benefits of sharing their personal information with the organization and be in a position to freely decide whether to do so.

Organizations are required to make readily available their policies and practices for the management of personal information. These policies and practices should be clear, comprehensive, and easy to find. If the practices being described are complex and involve multiple parties, the organization should make a concerted effort to ensure that users can understand all of the elements of the process, including what types of third parties are involved and why.

Organizations should be able to show that the consent they obtained is based on complete and understandable information. Privacy laws specifically require organizations to inform individuals of the purposes for which their personal information will be used. The explanation must be understandable to the average user as well as be easily accessible. Consent is only valid in respect of the purposes the individual was informed about.

What else should organizations know about consent?

Reasonable purpose

It is important to remember that the purposes for which an organization collects and uses personal information must be reasonable 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. 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.

Conditions of service

Often an organization will require some personal information in order to deliver the requested product or service. If an individual refuses to provide the required information, service may be refused. However, individuals cannot be forced into providing consent for sharing information that is over and above what the organization requires to fulfil a specific purpose. This is especially pertinent in the online and mobile environments, where individuals are often focused on getting timely access to a service or activity.

Withdrawing consent

Under private sector privacy laws, individuals have the right to withdraw consent, subject to legal or contractual restrictions. Withdrawal of consent should prevent 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, to the extent that this is technically feasible. 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.[4]

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. For example, if individuals register for an online service that does not use encryption, the organization may be considered to be inadequately safeguarding their personal information, notwithstanding the consent provided.

Privacy legislation also requires organizations to limit the collection of personal information to what is needed to carry out legitimate purposes. Organizations must be able to defend why each piece of personal information is collected and how it is used. And while it may be tempting, organizations should avoid collecting personal information because they believe it might be useful in the future. Canadian privacy laws require organizations to restrict their personal information collection to what is needed for an identified purpose and delete personal information that they no longer need for the original purpose for which it was collected.

The mechanics of online consent

In the offline world, consent is often expressed through a signature. Online, it is more difficult to show consent in a form that is unambiguous and universally recognizable. Under privacy legislation, any online statement or behaviour that can reasonably be interpreted to mean consent, either explicitly or implicitly, may be acceptable depending on the circumstances. However, there should not be any doubt that consent has been given.

Organizations have many options for obtaining online consent. Common online equivalents of a signature are clicking an "I agree" button or selecting online choices by ticking off a check box. Consent can also be expressed by an action, for example, downloading an application after reading what personal information the application will be accessing and how it will be used. Consent can sometimes be inferred by non-action, for example, where an opt-out option has not

[4] *Guideline 6G: Record Keeping and Client Identification for Financial Entities,* Financial Transactions and Reports Analysis Centre of Canada, July 2010.

been exercised. Organizations are free to come up with architecture that works best in a given environment, keeping in mind that consent should be expressed in an appropriate form depending on the nature of the information, the context, and the reasonable expectations of users.

It is good practice for organizations to put in place procedures for individuals to provide consent, and to retain proof that consent has been obtained. Situations may arise where organizations may need to demonstrate that they have obtained consent, and having proof of consent built into a documented process will help accomplish that.

Meaningful consent under privacy legislation cannot be obtained without organizations being up front with users about their information handling policies and practices. A common tool is a privacy policy, as described below.

3. Privacy policies and what they should contain

Organizations should be fully transparent about their privacy practices.

- Privacy policies should have a full description of what information is collected, for what purposes it is used, and with whom it is shared.
- Privacy policies should be easily accessible, simple to read, and accurate.
- Organizations should regularly review their privacy policies and update them as necessary.

The most basic way for an organization to inform users about its privacy practices is through a privacy policy. The GPEN Privacy Sweep found that, globally, 23 percent of websites had no privacy policy at all.

Individuals must receive sufficient information to be able to understand what they are consenting to. They should know:

- what information is being collected, especially if the information is not coming directly from them;
- why information is being collected;
- what will the information be used for;
- who will have access to the information;
- how will the information be safeguarded;
- how long will the information be retained;
- whether individuals can opt out of certain practices, such as behavioural advertising; and,
- if information is being shared with third parties:
    - what types of third parties;
    - what will the third parties be doing with the information; and
    - whether the third parties are located in a foreign jurisdiction, and potentially subject to other laws.

Organizations should present privacy information in a way that is easily understandable and readable to the average person[5]. This can be accomplished through clear explanations, a level of language suitable to a diverse audience, and easily readable font size. A privacy policy should also be made accessible in a conspicuous manner, such as a hyperlink on the organization's landing page, so that users can easily locate it. Organizations should also ensure that privacy policies are easily accessible from all devices the individual may be using, including smart phones, tablets, and gaming devices, as well as PCs.

When an organization plans to introduce significant changes to the privacy policy, it should notify users in advance and consider asking users to confirm that they consent prior to the changes coming into effect. Significant changes include a new arrangement to share personal information with a third party, or using personal information for a new purpose.

Finally, as a best practice, organizations should periodically audit their information management practices to ensure that personal information is being handled in the way described by their privacy policy.

Transparency of privacy practices is a dynamic process that does not end with the posting of a privacy policy but rather continues as websites grow and evolve. For general information on privacy management practices, please refer to our guidance document, "Getting Accountability Right with a Privacy Management Program."

4. Privacy policies are not always enough

Communicating privacy practices is not a one-size-fits-all proposition.

- The manner in which privacy practices are communicated should depend on the environment, the audience, and the level of complexity of the organization's handling of personal information.
- In addition to privacy policies, other types of privacy disclosures, like just-in-time notifications, should provide privacy explanations at key points in the user experience.
- Organizations should be creative in deciding when and how to provide privacy information to users.

[5] 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"

What research says about privacy policies

Traditionally, organizations have used privacy policies to convey information management practices to the public. However, over the years, privacy policies have been the subject of much criticism for their opaque and legalistic language, and the effort required to read them. Widely cited research found that Internet users would need 244 hours per year to read the privacy policies of the sites they visited.

The OPC's research into popular Canadian websites and their disclosures of personal information to third parties showed that organizations' privacy practices are not always disclosed in a meaningful way to consumers. The GPEN Privacy Sweep found that 33 percent of privacy policies viewed were of limited benefit to the average consumer seeking a clear explanation of how personal information was being used.

A 2012 OPC Survey found that Canadians rarely consult online privacy policies and when they do, they often find them unclear. Only one in five respondents said they either always (6%) or often (14%) read privacy policies. Another 29% said they sometimes read privacy policies, while half either rarely (26%) or never (24%) do. Sixty-two percent of respondents found privacy policies to be either somewhat vague (36%) or very vague (26%).

Under Canada's privacy laws, information management policies and practices may be communicated in a variety of ways. For example, PIPEDA's Openness Principle states that the method chosen to convey privacy practices "should depend on the nature of its business and other considerations."

There is no doubt that privacy policies serve an important accountability function. But at the same time, they can be overly long, opaque and ineffective at communicating information. Based on our experiences in overseeing private sector privacy legislation, it has become increasingly clear to our offices that in many cases, privacy policies in the online environment may not be sufficient to fulfil legislated consent requirements. This is particularly true for mobile technologies.

Improving on privacy policies

Laudable efforts have been made to improve privacy policies. For example, explanations of privacy practices can come in a variety of forms and can be used to present information at different moments of the online experience. The OPC has said in its Online Behavioural Advertising Guidelines that organizations should consider how to effectively inform individuals of their practices, by using a variety of real-time communication methods, such as online banners, layered approaches, and interactive tools like mouse hover pop-ups[6].

"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,

[6] The action of moving a mouse over a designated area causes a pop-up window to appear that can contain text (from webopedia.com).

users often feel a great 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.

Layered notices

Layered notices[7] help make better sense of lengthy, complex information by presenting a summary of the key highlights up front. Having read the highlights, the user has the option to click through to a condensed notice that covers all the basic information in concise, easy to read language. A complete version of the privacy policy that addresses all legal requirements is also available to the user.

Icons

Icons[8] are being explored as a simplified way of notifying users of organizations' key information management practices. The concept is to design icons that would communicate what users want to know, such as: does the site share personal information with third parties? Does the site engage in behavioural targeting? How long does the site retain personal information? These standardized icons would then appear on websites, helping users to quickly decide whether they want to interact with the site.

User Expectations

Organizations should consider user expectations when deciding which of their practices to highlight and when to do so. For example, if there is a use or disclosure a user would not reasonably expect to be occurring, such as the sharing of information with a third party, the organization has an even greater responsibility to be transparent and obvious in its explanation. Just-in-time notifications or icons are a good way of highlighting privacy practices in such cases.

As was explored in the report on the OPC's 2010 Consultations on Online Tracking, Profiling, and Targeting, and Cloud Computing, there are also many entities accessing information in the background – ad networks, data brokers, and/or data analytics companies. It is essential that they and their practices be brought to the forefront of users' minds as users make decisions whether or not to share their information.

In the Online Behavioural Advertising Guidelines, the OPC discourages overreliance on privacy policies as a way of obtaining meaningful consent. Organizations are encouraged to use a variety of communication tools, including online banners, layered approaches, and interactive tools to explain their practices.

---

[7] The Center for Information Policy Leadership, Hunton & Williams LLP. "Ten steps to develop a multilayered privacy notice."
[8] For example, the Mozilla Privacy Icons Project.

Challenges of mobile technologies

What holds true about communicating privacy practices in the fixed online environment is amplified with the use of mobile technologies. In the mobile environment, new business models are constantly evolving, the audience is diverse, and information is being processed at an even greater pace. Moreover, the medium does not lend itself to lengthy explanations.

When individuals' time and attention are at a premium, organizations need to highlight privacy issues at decision points in the user experience where people are likely to pay attention and where they need guidance. For example, whenever users are asked to provide information, such as at registration, they should be informed why each piece of data is needed and how it will be used. Privacy information needs to be optimized to be effective in spite of the physical limitations of screen size.

Our mobile apps guidance for promoting best practices among mobile application developers acknowledges that effectively conveying information about privacy choices is not a simple exercise. In addition to privacy policies, users should be provided with specific, targeted notifications when they need to make a decision about sharing their personal information. An effective privacy notice also needs to take into account users' familiarity with the concepts being described, not to mention their fragmented attention.

5. Children and youth

Organizations should recognize and adapt to special considerations in managing the personal information of children and youth.

- Children's information is considered sensitive and merits special consideration under privacy laws.
- Organizations should implement innovative ways of presenting privacy information to children and youth that take into account their cognitive and emotional development and life experience.

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

In general, children's information is considered to be sensitive and merits heightened protection under the law. For example, according to the OPC's Online Behavioural Advertising Guidelines, organizations should avoid knowingly tracking and profiling children on web sites aimed at children given the great difficulty in obtaining meaningful consent from very young users of the Internet.

In an investigation of Nexopia, a youth-oriented online social network, one of the issues the OPC examined was whether meaningful consent had been obtained for the collection of registration information. In its findings, the OPC expressed its doubts about the efficacy of passively relying on users to read and agree to the terms of a lengthy privacy policy to obtain consent from youth. The OPC said:

> *Recent research into youth Internet usage, as well as the consistent messages our Office hears from young people through our outreach work, indicates that while some youth users read online privacy policies, more interactive and innovative techniques devised specifically with youth in mind, and with the goal of informing them of the privacy implications of their decisions before they click, are more effective in obtaining consent than links to user agreements and privacy policies.*

Nexopia agreed to present its privacy policy in a way that takes into account the age of its users, such as presenting the policy in clickable theme-based pieces.

Conclusion

Under Canadian private sector privacy laws, organizations are required to obtain consent for the collection, use and disclosure of personal information. Consent is considered valid if individuals have been adequately informed of the organization's information handling practices so that they can reasonably understand what they are consenting to.

Organizations should have clear, comprehensive and accessible privacy policies online. They should also endeavour to convey privacy information at key points in the user experience to help users overcome the challenges of trying to understand how their personal information will be used online.

Given the evolving nature of users' experiences in the online environment, organizations should adapt their practices accordingly in order to obtain meaningful consent. Organizations are encouraged to communicate with users in a manner that is more creative, dynamic and interactive.

Greater transparency of privacy practices will help give individuals the assurance that their personal information is being handled with care and will increase their trust in online activities. Trust is essential for Canada's digital economy to thrive and for Canadians to partake in the economic benefits that the Internet offers.

REFERENCES AND RESOURCES

- Task force on consumer consent, London School of Economics. "From Legitimacy to informed consent: mapping best practices and identifying risks." May 2009.
- The Department of Commerce Internet Policy Task Force. "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." December 2010.
- The Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change." Preliminary FTC Staff Report. December 2010.
- The Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." FTC Staff Report. March 2012.
- Calo, Ryan M. "Against Notice Scepticism." July 2011.
- Lawson, Philippa and O'Donoghue, Mary. "Approaches to consent in Canadian data protection law." *Lessons from the Identity Trail*. Chapter 2.
- Perrin, Stephanie, Black, Heather H. , Flaherty David H. and Rankin T. Murray. "*The Personal Information Protection and Electronic Documents Act: An Annotated Guide*."2001.
- Cranor, Lorrie Faith. "Privacy Tool User Studies." November 2012. Presentation to the National Telecommunications and information Administration internet Policy Task Force.
- Kerr, I. et al "Soft Surveillance. Hard Consent. "
- Article 29 Working Party. "Opinion 15/2011 on the definition of consent." July 13, 2011.
- The OPC's PIPEDA Self-Assessment Tool.
- OECD. "Making Privacy Notices Simple: An OECD Report and Recommendations." *OECD Digital EconomyPapers*, No. 120, OECD Publishing. 2006.

Key considerations for obtaining meaningful online consent

Organizations are required to obtain individuals' meaningful consent for the collection, use and disclosure of personal information.

- Individuals must be informed about an organization's information management practices in order to be in a position to provide consent that is considered meaningful under privacy laws.
- Purposes for which organizations collect, use and disclose personal information have to be identified at or before the time of collection.
- If organizations decide to use personal information for a new purpose after it has already been collected, they must inform the individuals concerned and obtain their consent.
- Obtaining consent does not release organizations from their other obligations under privacy laws, such as overall accountability, safeguards, and having a reasonable purpose for collecting, using and disclosing personal information.

Organizations should be fully transparent about their privacy practices.

- Privacy policies should have a full description of what information is collected, for what purposes it is used, and with whom it is shared.
- Privacy policies should be easily accessible, simple to read, and accurate.

Communicating privacy practices is not a one-size-fits-all proposition.

- The manner in which privacy practices are communicated should depend on the environment, the audience, and the level of complexity of the organization's handling of personal information.
- In addition to privacy policies, other types of privacy disclosures, like just-in-time notifications, icons or layered notices, should provide privacy explanations at key points in the user experience.
- Organizations should be creative in deciding when and how to provide privacy information to users.

Organizations should recognize and adapt to special considerations in managing the personal information of children and youth.

- Children's information is considered sensitive and merits special consideration under privacy laws.
- Organizations should implement innovative ways of presenting privacy information to children and youth that take into account their cognitive and emotional development and life experience.