# Collecting from kids?

## Ten tips for services aimed at children and youth

Office of the Privacy Commissioner of Canada

The *Personal Information Protection and Electronic Documents Act* (PIPEDA, or the Act) provides that consent for the collection, use and disclosure of personal information must be meaningful, and that user expectations should be taken into consideration in determining the proper form of consent. While the Act does not differentiate between adults, on the one hand, and youth on the other,[1] the Office of the Privacy Commissioner of Canada (OPC) has consistently viewed personal information relating to youth and children as being of particular sensitivity, especially the younger they are, and that any collection, use or disclosure of such information must be done with this in mind (if at all).

This tip sheet extracts valuable lessons from three key Reports of Findings issued by the OPC, for the benefit of organizations that design and/or provide youth-centric online services. The Reports concern: (i) a social network for youth aged 13-18,[2] (ii) an interactive 'online world' for kids aged 6-13,[3] and (iii) a daycare which allowed parents online access to a webcam feed[4] . Many of these lessons are applicable to online services directed towards users of all ages[5]; however, they are particularly important to keep in mind when your users include youth.

It is important to note that these tips represent lessons learned through investigations by the OPC *to this point*, and do not represent the whole of the OPC's position on the collection, use and disclosure of youth information.

1. **Limit, or avoid altogether, the collection of personal information.** PIPEDA requires organizations to limit the collection of personal information to that necessary for their identified purposes. Thus, youth-centric service providers should expect that they will have to explain the necessity of any personal information collected. Given that it can be challenging (or even not possible) to obtain meaningful consent from youth, and in particular younger children, it is a good idea to design services to avoid collecting personal information. However, if collection of some personal information is necessary to provide a service, you should: (i) determine the minimal subset of information that will satisfy your purpose; (ii) determine what level of granularity is required for your purpose (e.g. asking for country of location as opposed to city); (iii) consider how consent is being obtained (see in particular tips 5 and 6 below); and (iv) document these evaluations.

---

[1] For the purposes of this document, 'youth' refers to those aged 18 and below, and includes 'children' under 13 years of age.

[2] PIPEDA Report of Findings #2012-001

[3] PIPEDA Report of Findings #2014-011

[4] PIPEDA Report of Findings #2011-008

[5] In particular, unless otherwise stated, the tips in this document should not be read as applying *exclusively* to the collection, use and disclosure of the personal information of children and youth.

2. **Be careful about 'inadvertent' collection.** Even if you are not intentionally collecting personal information, be cautious about fields that might encourage users to enter it. For instance, in both the social network and 'online world' investigations above, the OPC found that a significant portion of users appeared to be using their real name as their username. Free-text profile fields such as "About Me" may also contain sufficient information to render a user identifiable. Monitor how your users are *actually* using such fields – not just how you *intend* for them to be used.

3. **Have an appropriate retention schedule for inactive accounts.** While you may hesitate to delete personal information that may still be of value to your users, indefinite retention of information in inactive accounts runs counter to the principle that personal information should only be retained as long as needed. You are required to have, and make your users aware of, an appropriate retention schedule for inactive accounts (deletion after a defined period of inactivity, for instance). You also need to have a 'true deletion' option, which allows user accounts to be fully deleted, and not just archived.

4. **Speak to the specific services being provided to youth.** Of late, we are seeing organizations use unified privacy policies which describe the privacy practices of the organization in relation to *all* services it offers. In the 'online world' investigation, we noted that the organization offered different services aimed at both younger children and adults, which had significantly different privacy practice implications although operating under the same privacy policy. We were of the view that this could cause considerable confusion amongst users and their parents. Your privacy policy, or other notifications, should always speak to the specific service being provided – especially where a service is targeted to a privacy-sensitive audience such as youth.

5. **Make sure your users can understand you – or know to engage their parents/guardians.** The ability for youth to provide meaningful consent for the collection and use of their personal information depends greatly on their age, and their cognitive and emotional development. Thus, you should consider the target audience for your service, and explain your practices – and their potential risks – in a manner that they can fully appreciate. If your audience includes younger children, this may not be possible, so you should find a way to communicate, in language that the user will understand, the requirement to involve a parent/guardian in the process.[6]

6. **Consider the user experience.** Beyond the use of appropriate language, you should consider how that language is presented. When your target audience includes youth, you should consider adopting more novel means of presenting privacy information. In the youth social network investigation, we noted that interactive and innovative techniques for informing users about the privacy implications of their decisions, devised specifically with the user group in mind, are more effective in obtaining

[6] For more information on obtaining consent online, see the OPC's Guidelines for Online Consent.

consent than simply links to user agreements and privacy policies. Engage your user experience team, and innovate – why shouldn't the presentation of key privacy information be as user-friendly as every other feature of your service?

7. **Make clear who is agreeing to terms and conditions.** The ubiquitous "I have read and agree to the Terms and Conditions and Privacy Policy" checkbox on registration forms poses an additional difficulty when your users are youth. Is your organization asking the user to agree to these terms, or his or her parent/guardian? Remember, with younger children, the former is not possible given the need for meaningful consent. Moreover, if it is the latter, you must also ask yourself how you are ensuring that the parent/guardian has actually been involved in the process. The answer to these questions needs to be clear to, and consistent between, both you and your users.

8. **Ensure you have proper defaults for the age of your users**. In the youth social network investigation, we found it difficult to believe that a reasonable person would consider it appropriate that default privacy settings would result in users disclosing sometimes very sensitive information to potentially anyone on the Internet. Even in a network based on openness, sharing of personal information is dependent on users having control and being fully informed about, and understanding, the nature and risks of such disclosures. Default conditions often form the basis for how your service will be used. Make sure they match the reasonable expectations of your users.

9. **Know what is happening on your site**. Organizations are required to have in place procedures to protect personal information[7]; however, there is also an expectation – particularly around sensitive information – that these procedures are effective. For instance, in the 'online world' investigation, we found that while users were instructed not to use their real names as usernames, there was no mechanism by which compliance with this instruction was monitored. Similarly, while the organization had contractual protections with online advertisers which forbade the tracking of users, the organization did not take sufficient steps to monitor for this practice. Organizations need to think about whether the mechanisms they have in place to protect the personal information of youth are actually working or being used and/or respected.

10. **Prevention is preferable to monitoring.** Lastly, where possible, it is preferable for organizations to put in place technical (or other) measures that prevent the unauthorized use of childrens' information, rather than relying solely on monitoring and the assumption that third-parties will live up to their contractual obligations. For instance, an organization providing a service for youths may wish to prevent the placing of cookies that could be used for online behavioural advertising[8], in addition to

[7] For more information on accountability, see *Getting Accountability Right with a Privacy Management Program*

[8] The OPC's policy position on Online Behavioural Advertising states, "Given the practical obstacles to obtaining meaningful consent from children, especially implied consent, organizations should avoid knowingly tracking children and tracking on websites aimed at children."

stating in contracts that such tracking measures are not to be used. Knowledge that privacy violations *cannot* happen is much more comforting than belief and hope that they have not happened.

On a final note, in 2012, the OPC released a research paper titled *Surveillance Technologies and Children*[9]. The purpose of this paper was to summarize existing research on the effects of technical surveillance on children, and to develop a better understanding on the impacts of surveillance on children's experiences of, and attitudes towards, privacy. Organizations collecting the personal information of youth – particularly on an ongoing basis – may wish to consult this document to better understand the importance (beyond legislative compliance) of appropriately limiting the collection of such personal information.

[9] Surveillance Technologies and Children