NAUGHTY OR NICE? WRAPPING UP THE YEAR WITH A LOOK AT CHILDREN'S PRIVACY IN CANADA

Posted on December 18, 2024

Categories: Insights, Publications

This holiday season, think of the children!

We have recently received a number of questions about how Canadian privacy laws apply to children's data.

Canada does not have privacy legislation aimed specifically at children (like COPPA in the U.S.).[1] However, Canada's private sector privacy laws apply to children's personal information and regulators have put a strong emphasis on children's privacy matters in recent years.

The Office of the Privacy Commissioner of Canada ("**OPC**") has made "championing children's privacy rights" one of its key strategic priorities.[2] Similarly, Alberta's Office of the Information and Privacy Commissioner ("**AB OIPC**") has made it a strategic priority to "identify, facilitate and support opportunities to enhance access and privacy education and protections for children and youth."[3] Recently, the OPC issued a Sweep Report on Deceptive Design Patterns (the "**Deceptive Design Report**") which expresses particular concern about deceptive designs in services directed towards children.[4]

Proposed legislation, such as the *Online Harms Act*,[5] and *Consumer Privacy Protection Act*,[6] if passed, would provide greater protections for children's privacy.[7]

Given Canadian privacy regulators' increased attention to children's privacy, and the OPC's stance that children's data is "particularly sensitive"[8] it is paramount that organizations handling such data are up to speed on the nuances of Canadian privacy laws.

In this bulletin, we identify the key questions for private sector organizations attempting to handle children's data in accordance with Canadian law.

1. When (and How) Should an Organization Obtain Consent from Parents?

In the private sector, Canada operates on a consent-based privacy regime, meaning that consent is the primary basis for organizations to collect, use and disclose personal information.

The OPC's guidelines on meaningful consent (the "**Meaningful Consent Guidelines**") state that the ability of

children and youth to provide meaningful consent for the collection, use and disclosure of their information "depends greatly on their cognitive and emotional development." [9] The OPC takes the stance that, in all but exceptional circumstances, anyone under the age of 13 cannot provide meaningful consent.[10]

Quebec privacy laws provide that a child under the age of 14 may not provide consent for the collection of personal information, unless the collection, use or disclosure is clearly for the child's benefit.[11] There is a one-year difference to keep in mind here.

Alberta and British Columbia's respective privacy commissioners have not defined an age threshold under which parental consent is required. They instead take a more contextual view, that organizations must consider whether the individual understands the nature and consequences of the exercise of the right or power in question.[12] With that being said, the British Columbia Office of Information and Privacy Commissioner ("**BC OIPC**") has stated in guidance that the age of consent under BC's *Personal Information Protection Act* is "usually 12 years old."[13]

If the child is under the relevant age of consent, the organization looking to process the child's personal information must obtain consent from a parent or guardian. Even if the child is above the relevant age of consent, it may be prudent to seek parental consent (particularly if an organization's privacy practices are complicated and difficult to explain).

There are further considerations as to how parental consent should be obtained. For example, relying on a child ticking a box on an app or website indicating they have received approval from a parent may not always be sufficient. Moreover, because children's information is considered sensitive, consent obtained from parents should generally be express (opt-in) consent rather than implied (opt-out) consent.[14]

To further complicate matters, some young persons may wish to have privacy *from* their parents. As such, the inadvertent disclosure of the young person's information to their parents may itself be a violation of privacy. This is particularly important with respect to medical and health records. Organizations should obtain legal advice if they are handling children's data in circumstances in which there may be a conflict between a child's wishes and the wishes of their parent.

2. How Can an Organization Obtain Consent Directly from Youth?

Because personal information of youth is inherently sensitive,[15] handling data collected from teenagers who are above the age of consent and have the maturity level to provide meaningful consent will nevertheless require special care. Here are some practices to consider when seeking meaningful consent.

- **Express, Opt-In Consent:** As a general rule, organizations should always obtain express, opt-in consent when collecting children's personal information, given the sensitivity of this information. Therefore, any

platform aimed towards children should be designed to provide the most privacy-protective settings by default and allow children to "opt-in" to the processing of their personal information for various purposes. This is an explicit legislative requirement in Quebec for any public-facing product or service.[16]

- **Plain and Accessible Language:** Privacy notices that are read and consented to by teenagers should be written in plain and accessible language that is easy to understand for young people. Organizations may consider implementing a youth-focused privacy policy. If a practice is too complicated to explain to minors, an organization probably shouldn't do it in the first place.
- **"Just-in time" Notices:** Just-in-time notices are specific and timely privacy notices that appear when a user is about to provide their personal information. These notices are distinguished from blanket privacy policies that require the user to agree to all possible forms of information collection on a service. "Just-in-time" notices are recommended by the OPC as a design feature to assist in obtaining meaningful consent.[17]
- **Multi-Media Methods:** Using creative methods such as infographics, images, games or videos to convey the information of the privacy policy may also help to ensure consent is meaningful. For example, the Deceptive Designs Report lauded Lego's website for using a short educational video aimed at children to explain the company's privacy practices and its use of cookies.[18] Of course, not every company has the resources to produce an animated video or game as part of their privacy program, but organizations should at least turn their mind to how they can make the privacy program more engaging for youth.
- **Avoiding Deceptive Patterns:** Deceptive design patterns or "Dark Patterns" are user interface design techniques used on websites and mobile apps to influence, manipulate, or coerce users into making decisions that are not in their best interests.[19] These patterns threaten the validity of consent, particularly for children who may be more vulnerable to such influence. To ensure consent is validly obtained, organizations should avoid using deceptive design patterns. We have summarized the deceptive patterns identified by the OPC in a recent bulletin.[20] They include interface interference, nagging, obstruction, forced action, and inaccessible language.
- **Handling Consent Withdrawal and Data Deletion Requests:** Consent cannot be freely given if it cannot be freely withdrawn. The OPC has recommended that organizations design their processes such that children (and their parents if possible) can easily withdraw consent to certain practices or request the deletion or de-indexing of children's data.[21]
- **Limiting Collection Altogether:** Given the difficulty of obtaining consent from children and youth, and the need for express (opt-in) consent, organizations would be wise to limit the collection of children's information altogether. For example, an organization may consider:

    i. age-gating sections of its website or platform;
    ii. forgoing data collection practices (such as advertising cookies) where a user's reported age is

under the relevant age of majority;

iii. encouraging youth to select fake usernames from a list when signing up for a platform, rather than letting them provide their real names; or

iv. collecting anonymized data rather than identifying data.[22]

- **Avoiding Behavioural Advertising:** In its guidelines on privacy and online behavioural advertising, the OPC states that as a "best practice" organizations should not implement behavioral advertising practices for children, as it is difficult to obtain meaningful consent from children to collect information for the purpose of behavioural advertising.[23] As such, behavioural advertising in general should be avoided unless organizations can be reasonably certain the targeted individual is an adult.

When deciding on a consent approach for older teenagers, it is important to consider that the age of majority in Canada varies across provinces and territories (between 18 and 19 years old).[24] Organizations with a national footprint may consider tailoring practices to users aged 18 or younger to ensure all regions are covered.

3. How Should Children's Data be Safeguarded?

If an organization does collect children's personal information, it must protect it with a high degree of safeguards, given the information's sensitive nature. Insufficient safeguards can lead to data breaches, civil litigation, and scrutiny from privacy regulators. For example, in March 2021, the OPC published findings from an investigation conducted on CoreFour Inc. ("**CoreFour**"), which provided a K-12 learning management and analytic system. After identifying certain specific security vulnerabilities, the OPC found that CoreFour "lacked a robust overarching information security framework."[25] The investigation into CoreFour reminds us that, when collecting children's information, organizations should consider whether their current security system is sufficient to handle such sensitive information.

4. Is the Data Being Handled for "Appropriate" Purposes?

Pursuant to Canada's private-sector privacy legislation, organizations can only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances (in Quebec, necessary for "serious and legitimate" purposes). In interpreting whether a practice is appropriate, serious and legitimate, privacy regulators and courts will generally look to the following factors:

- **Necessity.** Is there a demonstrable need or bona fide business interest to collect, use or disclose the personal information?
- **Effectiveness.** Would the practice be effective in meeting that need?
- **Minimally Intrusive.** Are there less intrusive means of achieving the same ends?

- **Proportionality.** Is the loss of privacy proportionate to the benefits, taking into account the sensitivity of the information that may be processed?[26]

One of the factors involved in this analysis is the degree of sensitivity of the personal information at issue.[27] Since children's data is understood to be inherently sensitive, it stands to reason that the need to process children's data must be sufficiently great for the practice to be proportionate.

5. Conclusion

The combination of increasing interest from regulators and the evolving legislative landscape regarding children's privacy in Canada makes data collection from children a complex area for organizations to navigate. When providing services that may collect information from children, organization should seek appropriate legal advice to ensure their consent and data management practices are sufficient.

McMillan's experienced Privacy and Data Protection team can assist organizations comply with regulatory requirements in all Canadian jurisdictions.

[1] *Children's Online Privacy Protection Act of 1998*, 15 USC §6505, available here.
[2] *Office of the Privacy Commissioner of Canada Strategic Plan 2024-2027*, s.v. "Strategic priority 3: Championing children's privacy rights", available here.
[3] AB OIPC, *Strategic Business Plan 2024-2027*, available here.
[4] Office of the Privacy Commissioner of Canada ("**OPC**"), *Sweep Report 2024: Deceptive Design Patterns*, (2024) at 19, available here. **[Deceptive Design Report]**
[5] Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2024, available here. **[Bill C-63]**
[6] The *Consumer Privacy Protection Act* ("**CPPA**") would be enacted under Bill C-27, the *Digital Charter Implementation Act, 2022*. We have summarized this legislation in our bulletin: *Privacy Reform is on the Table Once More: Canada Introduces the Digital Charter Implementation Act, 2022* (June 2022), available here.
[7] See section 65 of the proposed *Online Harms Act* in Bill C-63, which requires "age appropriate design". The CPPA specifically denotes children's data as sensitive, and imposes new protections for children's privacy rights.
[8] OPC, *Protecting the privacy rights of young people* (28 November, 2023), available here. Under Canada's proposed *Consumer Privacy Protection Act* under Bill C-27, the personal information of minors is explicitly identified as sensitive information: section 2(2).
[9] OPC, *Guidelines for obtaining meaningful consent* (August 2021), available here, s.v. "Consent and children".

[Meaningful Consent Guidelines]

[10] *Meaningful Consent Guidelines*, s.v. "Consent and children".

[11] *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, s 4.1. **[Quebec Act]**

[12] Meaningful Consent Guidelines, s.v. "Consent and Children".

[13] BC OIPC, *Competitive Advantage: Compliance with PIPA and the GDPR* (March 2018), section 3.2.2, available here.

[14] Under *PIPEDA*, sensitive information requires express consent. See *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, at Schedule 1, Principle 4.3.6. **[PIPEDA]**

[15] OPC, *Investigation into CoreFour Inc.'s compliance with PIPEDA* (29 March 2021), PIPEDA Findings #2021-002, para 112, available here. **[CoreFour]**

[16] *Quebec Act*, s 9.1.

[17] *Meaningful Consent Guidelines*, s.v. "Be innovative and creative: 'Just-in-time' notices".

[18] *Deceptive Design Report*, s.v. "Case-Study: Lego".

[19] *Deceptive Design Report*, s.v. "Background".

[20] Kristen Pennington, "Canadian Privacy Regulators Issue Resolution about Deceptive Design Patterns", McMillan LLP, (14 November 2024), available here.

[21] OPC, *Companion document – Putting best interests of young people at the forefront of privacy and access to personal information* (5 October 2023), available here, s.v. "6. Allow for deletion or deindexing and limiting retention".

[22] However, organizations should be aware that certain anonymization processes may be at risk of re-identification. See our recent bulletin on this subject: *2024 Uptake: Risks of Anonymized and Aggregated Data* for more insights on the issue.

[23] OPC, *Guidelines on privacy and online behavioral advertising*, (December 2015), s.v. "Tracking of Children", available here.

[24] For a summary of the age of majority in different provinces and territories, see *Putting Children's Interest First - Federal-Provincial-Territorial Consultations on Custody and Access and Child Support* (December 2022), online available here.

[25] *CoreFour*.

[26] OPC, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, (24 May 2018), s.v. "Inappropriate purposes or No-Go Zones".

[27] *CoreFour*, para 39.

by Robbie Grant and Aki Kamoshida (Articling Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.