OSLER

Insights into Canada's development of children's privacy framework

JULY 21, 2025 11 MIN READ

Related Expertise

- Advertising and Marketing
- Privacy and Data Management
- Risk Management and Crisis Response
- Technology

Authors: Éloïse Gratton, Ad. E., Maryna Polataiko

We previously published an Update on Canada's new *Online Harms Act*. This is the second installment in the Osler Online Harms Series.

In May 2025, the Office of the Privacy Commissioner of Canada (OPC) launched an exploratory consultation on the development of a children's privacy code to encourage international alignment, clarify obligations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and set out its "expectations regarding organizations' handling of children's personal information." In this Update, we provide an overview of recent key legislative and regulatory developments in children's privacy both abroad and in Canada, as well as a summary of the themes and questions raised by the OPC in its exploratory consultation.

AccessPrivacy is hosting an interactive, online workshop regarding this OPC consultation on Friday, July 25, 2025, from 11 a.m. to 1 p.m. ET. See below for more details.

International context

In recent years, international instruments, legislation and regulatory initiatives have increasingly focused on how to protect children's privacy in the digital environment. The UN Convention on the Rights of the Child (UNCRC) set out state parties[1] obligations respecting children's rights, including that the best interests of children be a primary consideration in decisions affecting them. State parties must undertake all appropriate legislative, administrative, and other measures for the implementation of the rights under the UNCRC. In 2021, General Comment No. 25 clarified how states should implement the UNCRC in the digital environment, given its increasing role in children's lives.

Reflecting this growing global emphasis on children's digital rights, several jurisdictions have introduced or strengthened child-focused data protection measures. Pursuant to its mandate under the U.K. *Data Protection Act 2018*, the U.K. Information Commissioner (ICO) prepared — with regard to the U.K.'s obligations under the UNCRC — a code of practice on age-appropriate design for digital services likely to be accessed by children. The resulting U.K. Age-Appropriate Design Code (or Children's Code) came into force in 2020, making it the first statutory code of practice of its kind and providing a model for other jurisdictions. California enacted the *California Age-Appropriate Design Code Act* in 2022, requiring businesses to

consider the best interests of children when designing and delivering online services likely to be accessed by them. More recently, Australia passed the *Privacy and Other Legislation Amendment Act 2024*, which requires its Information Commissioner to develop and register a Children's Online Privacy Code within two years of royal assent.

Elsewhere, data protection authorities have issued guidance addressing children's privacy. In 2021, Ireland's Data Protection Commission (IDPC) published its Fundamentals for a Child-Oriented Approach to Data Processing, introducing child-specific data protection interpretative principles and recommended measures. That same year, France's Commission nationale de l'informatique et des libertés (CNIL) released eight recommendations to enhance the protection of children online through the provision of practical advice and the clarification of aspects of the European Union *General Data Protection Regulation* (GDPR) and the *French Data Protection Act*.

Canadian legislative context

Across Canada, recent legislative proposals have sought to establish statutory frameworks governing children's privacy and safety in the digital environment, and youth privacy has also become a central area of privacy regulatory focus across Canada.

At the federal level, the government of Canada introduced Bill C-63 (the *Online Harms Act*) in 2024, which required prescribed platforms to take steps to protect children by integrating design features respecting the protection of children, such as age-appropriate design. These requirements were to be detailed in regulations respecting child protection design features, such as account options for children, parental controls, privacy settings for children, and other age-appropriate design features. During a parliamentary appearance, the former Minister of Justice and Attorney General of Canada clarified that Bill C-63 would have contemplated age verification mechanisms. While Bill C-63 died on the order paper when Parliament was prorogued, the Liberals have signaled that they are taking a "fresh" look at online harms legislation.

Bill C-216 (the *Promotion of Safety in the Digital Age Act*) was reintroduced in June 2025 as a private member's bill by Hon. Michelle Rempel Garner after Bill C-416 lapsed due to prorogation. Bill C-216 would impose obligations on platform operators, including acting in the best interests of users they know or should reasonably know are minors by mitigating prescribed harms through safety-by-design, providing clear and accessible safety settings to users and parents of users they know or should reasonably know are children and to their parents, and using privacy-preserving age verification algorithms when restricting access to content inappropriate for children.

As efforts to protect children online continue across Canada, Québec has taken its own legislative steps to address the issue. In June 2024, the National Assembly of Québec established the Select Committee on the Impacts of Screens and Social Media on Young People's Health and Development, mandating the Committee to examine the impact of screens and social media on young people's health and development. Following extensive consultations, this Committee issued a series of recommendations relevant to children's privacy, including that the Québec government establish a digital age of majority prohibiting registration for, and access to, social media platforms before age 14, assess which entity or agency would be most appropriate to develop standards or guidelines for digital platforms, and conduct a rigorous analytical review before mandating age verification mechanisms in any business sector, or for any company given significant privacy implications. The Committee also recommended that the Québec government update applicable laws to require digital platforms to take into account risks to minors when their products are "designed primarily for use by minors or are predominantly used by minors" by requiring measures such as privacy by design and prohibiting 'deceptive interfaces'.

Youth privacy has also become a central area of regulatory focus across Canada. In October 2023, the federal, provincial and territorial privacy commissioners and ombuds with responsibility for privacy oversight issued a joint Resolution on the Best Interests of the Child. The OPC subsequently cited "championing children's privacy rights" as a key strategic priority in its Strategic Plan for 2024-2027. In June 2024, the OPC launched a consultation on age assurance guidance. The following month, the OPC, OIPC BC, and OIPC AB published the results of their Deceptive Design Pattern 'Sweep' on children's services. In October 2024, the OPC issued a Statement on AI and Children with G7 Data Protection and Privacy Authorities. These regulatory initiatives have signaled an emphasis on embedding child-specific obligations across the lifecycle of digital service design and operations, and key themes have emerged, including an emphasis on the "best interests of the child," age-appropriate transparency, privacy by default, deceptive practices, concerns about artificial intelligence and children, and a push for alignment with global standards.

OPC consultation on children's privacy code

The OPC's exploratory consultation on the development of a children's privacy code in May 2025 draws extensively from global precedents such as the U.K. Children's Code and the OPC's own Resolution on the Best Interests of the Child. More specifically, the OPC states that it seeks to encourage international alignment, "clarify obligations under PIPEDA," and set out its "expectations regarding organizations' handling of children's personal information." Following the consultation, which is open until August 5, 2025, the OPC intends to draft a children's privacy code elaborating on its expectations regarding the obligations of organizations.

The OPC is seeking comments on its role in ensuring that the best interests of the child are upheld, other privacy considerations relevant to the establishment of a children's privacy code, areas/industries where the OPC should provide sector or industry-specific guidance, and anticipated challenges or solutions in applying a children's privacy code.

Bellow, we summarize the topics and questions highlighted in the OPC consultation, which include the application of the code, meaningful consent and privacy rights, privacy impact assessments, transparency, privacy by default, deceptive practices, and limiting disclosure.

1. Application of code: The OPC adopts the UNCRC definition of "children" as individuals under 18. It proposes a tiered applicability model, where services "directed at children" are "squarely" in-scope and mixed-audience services are in scope if they are "likely to be accessed" by children — a threshold mirroring the *U.K. Data Protection Act*, *California Age-Appropriate Design Code Act*, and IDPC Children's Fundamentals [PDF]. The OPC indicates that organizations will be expected to take "reasonable measures" to assess their user base and, if a "significant number" of children access their services, adapt data practices (e.g., via age assurance). The OPC's consultation questions concern differential application to child-directed and mixed-audience services, risk-based triggers, and how to define, adjust or remove the "significant number" threshold.
2. Consent and rights: Drawing on UNCRC General Comment No. 25, the OPC takes the position that consent should reflect "children's evolving capacities" to be meaningful. Below age 13, parental consent generally remains the default. The OPC further states that parental access rights may be limited based on children's privacy rights and best interests, and organizations are expected to verify requestor identities and child/parent

relationships. Children must have "simple means" to exercise correction rights, including receiving data in a "readily understandable" form. The OPC also reiterates its recommendation that organizations enable the right to deletion and deindexing. The OPC's consultation questions concern how to assess a child's capacity to consent, how to obtain and verify parental consent, how to tailor disclosures to different developmental stages, and how to address withdrawal of consent.

3. Privacy impact assessments: The OPC highlights that organizations should identify and minimize risks of harm to embed privacy and best interests of children into product design. In line with the U.K. approach, the OPC indicates that the privacy impact assessment (PIA) process should involve consultations with children, parents, teachers, or child advocates — though the OPC emphasizes that PIAs "consider the perspectives and experiences of children as individuals, and as a group, through an intersectional lens." The OPC's consultation questions include how to integrate and assess the "best interests" principle in PIAs, which impacts should be considered, and how to involve stakeholders.
4. Transparency: Citing its 2024 Sweep Report, the OPC identifies "complex and confusing" privacy policies as the most common "deceptive design pattern." According to the OPC, privacy notices should be "concise, prominent and clear," age-appropriate, and presented in a "variety of ways" (e.g., interactive formats). They should address user controls, default settings, privacy risks, and "any other" relevant topics (e.g., content moderation). Further, the OPC indicates that tracking should be avoided or clearly disclosed. Citing its Resolution on Deceptive Design, the OPC calls for presenting privacy choices using neutral language and design. The OPC's questions address notice content, tailoring notices by age and capacity, communications for both parents and children, and what resources could help parents explain "privacy implications" to children.
5. Privacy by default: The OPC references U.K. and California statutory requirements to endorse privacy-protective default settings (e.g., 'private' content, disabling ad targeting, age-appropriate tools and consents). According to the OPC, tracking — including location tracking — should generally be off by default, with geolocation requiring explicit consent. Further, the OPC notes that training AI with children's data and AI systems impacting children may warrant restrictive defaults or avoidance. The OPC's questions address retention-limiting measures (e.g., auto-expiring messages), factors informing retention and disposal policies, practices to avoid, and scenarios justifying less restrictive defaults.
6. Deceptive practices: The OPC reports that the 2024 GPEN Sweep [PDF] found widespread "deceptive design patterns": inaccessible language, 'interface interference' (biased design), nagging (repeated prompts), 'obstruction' (barriers), and 'forced action' (requiring unnecessary data). Highlighting standards like the U.K. Children's Code, the OPC opposes "manipulative or deceptive design or behavioral incentives" that 'nudge' children into poor privacy choices, harmful behaviour, providing unnecessary data, or disabling protective settings, and encourages 'nudges' promoting privacy and well-being. The OPC also notes that design and usability should also be tested to detect and remediate deceptive patterns. The OPC's consultation questions include how design can encourage privacy-protective behaviours, help children make informed choices, and reduce harms.

7. Limiting disclosure: Citing U.K. and California codes, the OPC emphasizes limits to transfers and disclosures of children's data, subject to legal exceptions or a child's best interests. For example, it articulates the view that disclosures should require assessing a child's capacity to consent (or the need for parental consent) and that disclosures be avoided absent express consent, legal authority for a purpose in the child's best interest, or a legal duty to protect the child. The OPC recommends that organizations explain disclosures (including the types of data shared) and that third-party use be limited through safeguards beyond monitoring and contractual assurances. The OPC's consultation questions concern safeguards against unauthorized use, notification to children when their data is shared, and the types of data and purposes for which disclosure should not be permitted.

Conclusion

As Canada moves towards a more defined framework for children's privacy, regulatory, legislative and policy developments continue to evolve rapidly. With the OPC's consultation underway and new legislative initiatives at both the federal and provincial levels, Osler's privacy team will continue to monitor developments closely, and provide timely updates and insights as this important area of privacy law takes shape.

AccessPrivacy Webinar

As the proposed children's code could have significant impact on a broad range of organizations that may process personal information of minors — including organizations providing services not specifically directed at children — AccessPrivacy is hosting an interactive, online workshop on Friday, July 25, 2025, from 11 a.m. to 1 p.m. ET. Click here to register.

The targeted, moderated discussion is designed to assist organizations and trade associations in understanding the development process, application and impact of a potential code, and in framing their own submissions for the OPC's consultation. As part of this interactive forum, we invite stakeholders to participate in the discussion and provide feedback. The event will be recorded and a copy will be submitted to the OPC as part of its consultation process. Representatives from the OPC have been invited to attend in an observer capacity.

To watch the webinar on demand, subscribe to the AccessPrivacy Knowledge Portal, an online platform with key resources to support privacy professionals in their day-to-day privacy and access challenges.

---

[1] A "State Party" to a treaty is a state that has expressed its consent, by an act of ratification, accession or succession, and where the treaty has entered into force (or a state about to become a party after formal reception by the United Nations Secretariat of the state's decision to be a party).