

Protecting child and youth privacy online

Summary

When children and youth spend time online, [their personal information is collected and used](#). Profiling and tracking user data enables digital platforms and services to drive profits through tailored content designed to maximize engagement. While complicated or manipulative privacy practices negatively impact all users, children and youth are uniquely vulnerable. Without appropriate safeguards for child and youth privacy online, sensitive or personal information can be collected, used and shared, with serious and potentially life-long impacts.

To protect child and youth privacy online, Canada must create a strong legislative framework that establishes special protections for children and youth, holds digital platforms and services to account, and upholds and advances the [UN Convention on the Rights of the Child \(UNCRC\)](#).

Recommendation

The Government of Canada must develop and enforce robust digital privacy legislation and protections that embed special protections for children and youth to improve online safety and support healthy development and well-being.

The issue

How time, attention, and personal information are used for profit

When someone uses digital products and services, platforms collect personal data, including:

- Information directly provided by the user when creating a profile, such as name and age.
- Information that is “learned” based on user engagement, such as friends/followers, likes and interests, political views, sexual orientation, gender identify, facial features, voice prints, health concerns, or GPS location.

Children and youth are not protected from extensive data collection:

- [96% of the 50 websites](#) most popular with children in Canada use an average of five trackers to continually collect user data.
- [73% of the most popular apps and platforms](#) for kids collect and monetize personal information as a routine aspect of their business model.

Online platforms and services are [deliberately designed](#) to grab and hold attention. [According to 5Rights Foundation](#), online platforms have “embedded data-harvesting strategies into the design of digital products and services, driving users to give up more personal data, time, and attention.” User data is extremely valuable to digital platforms and services. Almost [98% of Meta’s revenue comes from advertising](#), relying upon personal data from billions of users to drive profits.



**Centre for Healthy
Screen Use**

AT THE CANADIAN PAEDIATRIC SOCIETY



Canadian
Paediatric
Society

Why privacy and data practices matter for children and youth

When everything that young people see and do online is [monitored and tracked](#), and content they post or share can be used by others, the risks to health and well-being are significant. Digital platforms and services typically use opaque or deceptive privacy practices that [don't seek meaningful consent](#) before tracking, profiling, targeting ads, and personalizing content. These practices are in direct conflict with [privacy-by-design standards](#)¹, and fail to adequately protect developing children and adolescents who may not be able to provide informed consent.

Current privacy and data practices contribute to [heavy or inappropriate](#) screen use that can [displace opportunities](#) to learn, play, sleep, and interact with family and friends. [Passive scrolling and high screen time](#) have also been linked to heightened anxiety in teens. In 2023, the [U.S. Surgeon General](#) warned that features which deliberately maximize user engagement—including algorithms that use personal data to deliver targeted content, autoplay and infinite scroll—put child and youth physical and mental health at risk. The Canadian Paediatric Society's (CPS) [call to action on social media](#) echoes this warning, recognizing social media platforms' short- and long-term effects on child and youth health and well-being.

What needs to be done

A children's privacy code for Canada

In 2025, the Office of the Privacy Commissioner of Canada (OPC) launched an [exploratory consultation](#) on developing a children's privacy code, which would require digital platforms and services to be designed and operated in the best interests of children and youth. The CPS participated in this consultation through a roundtable discussion, an [independent written submission](#) and a [joint submission](#) developed by the 5Rights Foundation.

1 Privacy-by-design requires proactively embedding strong privacy practices into the design and function of digital platforms and services to ensure the maximum degree of user privacy is engaged by default.

The CPS recommends that a children's privacy code prioritize:

1. **Child rights:** A Canadian children's privacy code should be rooted in a child rights perspective, advance the best interests of children, and uphold Canada's commitments under the UNCRC.
2. **Duty of care:** Digital platforms and services should be held responsible for providing special protections for children and youth online.
3. **Privacy-by-design:** Privacy-by-design should be the standard for digital platforms and services. aligning with existing international age-appropriate design codes ([UK](#), [California \(US\)](#) and [Europe](#)) and [safety-by-design principles](#) ([UK](#) and [Australia](#)).
4. **Age and developmentally appropriate communication:** Digital platforms and services must provide short, plain language, prominent, age appropriate, and developmentally appropriate information on their data and privacy policies.
5. **Effective enforcement and oversight:** To be effective, a children's privacy code must include transparent and independent enforcement and oversight.

Taking action

The monetization of time, attention and personal information has led to the use of manipulative design and privacy practices by digital platforms and services. These practices have especially significant impacts on the development and well-being of children and youth. To protect the privacy of children and youth online, Canada urgently needs a **meaningful and enforceable digital privacy framework that prioritizes children and youth's need for special protections in online spaces.**

For more information on the CHSU's digital health policy recommendations: [Advocacy Priorities.](#)

