Canada's Children's Privacy Code

Joint submission to the OPC's Exploratory Consultation

Data is used to drive many norms of the digital world. How children's data are collected, shared, and used impacts most aspects of their digital experience and consequently their lives.[1] From the moment a child opens an application, plays a game, or visits a website, data is being gathered, and inferred: from their mood and friendships to the time they wake up or go to bed. Data collection, use, storage, and disclosure directly affect how children's data is used to inform — or facilitate — decisions that shape both their digital experience and real-life outcomes.

The value of children's data – and the extent to which the digital environment is designed to harvest, share, and sell it for profit, to build profiles or predict behavior – remains largely opaque to most users and almost entirely invisible to all children. Children in Canada have consistently expressed discomfort with this reality. In 2014, 83% of over 5,000 children surveyed in Canada indicated that companies operating social media sites where children post content should not be able to see their content, even though they knew companies could.[2] Young people in Canada have called for regulation that better protects them from these kinds of commercial intrusions.[3]

The current regulatory approach has done little to constrain the commercial collection and exploitation of children's data. In the absence of regulation, companies have embedded data-harvesting strategies into the design of digital products and services, driving users to give up more personal data, time, and attention.[4] As a result, 96% of the 50 websites most popular with children in Canada employ an average of five trackers to continually collect data from children and, although 80% have privacy settings, only 12% set them to private by default.[5]

Canada's situation mirrors global trends. Findings estimate that, on average, 72 million data points are collected on a child before they turn 13.[6] Additionally, 73% of the most popular apps and platforms for kids are monetizing personal information as a routine and central aspect of their business model.[7]

As part of the 2024 Global Privacy Enforcement Network Sweep, the Office of the Privacy Commissioner of Canada (OPC) confirmed that deceptive design patterns are significantly more prevalent in digital products and services aimed at children. This reflects tech companies' deliberate strategy to intentionally manipulate children and maximize data extraction from young users.[8]

The shift away from websites to apps has opened further possibilities for data extraction through the use of software development interfaces provided by large data intermediaries.[9] Children's data is collected not just on websites and apps, but also

---

[1] When we use the terms "child" or "children", we refer to individuals under the age of 18 as defined in the UN Convention on the Rights of the Child, art. 1.
[2] Steeves, Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity, p. 23.
[3] Shade et al., Framing the Challenges of Digital Inclusion for Young Canadians.
[4] 5Rights, Disrupted Childhood: The cost of persuasive design and Pathways: How digital design puts children at risk.
[5] Steeves, Terra Cognita: The Surveillance of Young Peoples' Favourite Websites.
[6] The Washington Post, Your kids' apps are spying on them.
[7] Common Sense Media, 2023 State of Kids' Privacy.
[8] OPC, Sweep Report 2024: Deceptive Design Patterns, p. 5.
[9] Binns et al., Third Party Tracking in the Mobile Ecosystem; Gui et al., Truth in Advertising: The Hidden Cost of Mobile Ads for Software Developers; Ekambaranathan et al., "Money makes the world go around": Identifying Barriers to Better Privacy

through educational technology (EdTech),[10] digital games and gaming consoles,[11] AI-powered connected toys,[12] smart speakers,[13] and various other devices used at school and at home.

Evidence of these practices substantiates children's concerns about the commercialization of their data and underscores the importance of listening to young people. As a population intimately concerned with children's wellbeing, parents share these concerns. The OPC's own research shows that 93% of Canadian parents worry about the amount of personal information companies collect about their children, and 74% do not trust companies to protect that information.[14]

Children are longstanding rightsholders under the UN Convention on the Rights of the Child (UNCRC), which Canada ratified in 1991. Canada must therefore ensure that national laws give full and meaningful effect to children's rights. The UN Committee on the Rights of the Child's General comment No. 25 clarifies that states' duty to protect children's rights extends fully into the digital world. As the federal regulator for privacy, the OPC bears the duties the Convention establishes.

Technology companies also bear a duty to respect children's rights and prevent violations in the digital world; yet, they consistently and repeatedly fail to respect children's rights or uphold even the most basic standards of child safety and privacy.[15] In this context, the role of the OPC, alongside strong, rights-based, and systemic regulation of the private sector, is essential to reverse this pattern and ensure the respect, protection and realization of children's rights online.

The right to privacy, in particular, is a cornerstone of international law – being enshrined in the Universal Declaration of Human Rights,[16] the International Covenant on Civil and Political Rights,[17] and the UNCRC.[18]

As UNCRC General comment No. 25 emphasizes, upholding "[p]rivacy is vital to children's agency, dignity and safety and for the exercise of their rights".[19] It is also central to the realization of children's rights as a whole, including to education,[20] health,[21] information,[22] freedom of expression,[23] and to enjoy their own culture.[24]

In the face of unprecedented data collection, sharing and monetization, Canada must adopt a robust and effective data protection framework that ensures children's privacy, agency, and safety in the digital environment.

We welcome the OPC's leadership in developing a children's privacy code that extends these protections to all children in Canada. Thirty years after the concept of Privacy-by-Design was first coined by the former Information and Privacy Commissioner of Ontario,[25] this code represents a significant step towards delivering a digital world in which

---

in Children's Apps From Developers' Perspectives; and Grace et al., Unsafe exposure analysis of mobile in-app advertisements.

[10] Digital Futures for Children, EdTech matters for children's learning, privacy and other rights.
[11] CBS News, Microsoft to pay $20 million over FTC charges surrounding kids' data collection.
[12] McStay, Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy.
[13] The Conversation, 'Hey Siri': Virtual assistants are listening to children and then using the data.
[14] OPC, 2024-2025 Public Opinion Research on Privacy Issues, figure 39.
[15] UNCRC General comment No. 25, para. 35; UNICEF, Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment.
[16] Universal Declaration of Human Rights, art. 12.
[17] International Covenant on Civil and Political Rights, art. 17.
[18] UNCRC, art. 16.
[19] UNCRC General comment No. 25, para. 67.
[20] UNCRC, art. 28.
[21] UNCRC, art. 24.
[22] UNCRC, art. 17.
[23] UNCRC, art. 13.
[24] UNCRC, art. 30.
[25] Cavoukian, Privacy by Design: The 7 Foundational Principles.

children's rights are upheld and respected. By aligning with international best practices, the OPC can establish the minimum rules for rights-respecting innovation.[26]

To this end, we strongly recommend that the OPC builds on the UNCRC, its accompanying General comment No. 25, and international best practices – including the UK's Age-Appropriate Design Code and other Children's Codes it has inspired.[27] This is a critical first step towards holding tech companies accountable for respecting children's rights and best interests – by design and default – so that children can enjoy the benefits of technology without their privacy, agency, and security being compromised.

Application of a children's privacy code

The UNCRC enshrines the rights to protection[28] and privacy[29] for all persons under the age of 18. As reaffirmed in UNCRC General comment No. 25, these rights extend fully in the digital world, where "[s]tates parties should require the integration of privacy-by-design into digital products and services that affect children".[30]

In line with international best practices, the children's privacy code should apply broadly to all digital products and services that are used by, directed at, intended for, likely to impact, or likely to be accessed by children.[31] This reflects the reality that children routinely access or use digital products and services regardless of whether they are the intended audience.

Moreover, the risk to children's rights and privacy does not depend on a company's size, market share, or user base. Risk assessments and corresponding obligations under the children's privacy code should therefore apply to all digital products and services likely to be accessed by or impact children – not only those with a significant number of child users.[32] The code must avoid the known shortcomings of the United States' Children's Online Privacy Protection Act (COPPA),[33] and prevent companies from evading responsibilities through disclaimers in the product or service's terms of use that said product or service is not intended for users below a certain age.[34]

Additionally, the principles and guidance in the children's privacy code should also inform the practices of the public sector, including those delivering education and healthcare services across provinces and territories, while respecting those jurisdictions' powers.

Enabling children's privacy rights

Too often, children's right to privacy is undermined by digital products and services that are deliberately designed to harvest vast amounts of personal data. Design features that undermine privacy (such as default settings that maximize data collection) manipulate children's behavior, shape their choices, and pressure them into sharing more data than necessary.[35] Rather than designing with privacy and children's rights in mind, tech companies routinely shift the burden onto children and their families, expecting them to navigate complex privacy settings and terms of service to "consent" to the collection, use, and disclosure of their data.

---

[26] G7, 2025 Data Protection and Privacy Authorities Roundtable Statement.
[27] Including the California Age-Appropriate Design Code, the Irish Fundamentals for a Child-Oriented Approach to Data Processing, and the Netherlands' Code for Children's Rights.
[28] UNCRC, art. 3
[29] UNCRC, art. 16
[30] UNCRC General comment No. 25, para. 70.
[31] UNCRC General comment No. 25, para. 70; Information Commissioner's Office Age-Appropriate Design Code, Services covered by this Code; and CEN-CENELEC, Workshop Agreement 18016 Age-Appropriate Digital Services Framework, Section 5 and 8.
[32] UNICEF, Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment, p. 6.
[33] 5Rights, But how do they know it is a child? Age Assurance in the Digital World, pp. 9-10.
[34] Grimes, Digital playgrounds: The hidden politics of children's online play spaces, virtual worlds and connected games, Chapter 6.
[35] 5Rights, Pathways: How digital design puts children at risk.

This consent model is deeply flawed. Children and their parents often cannot comprehend or manage the deliberately opaque, lengthy terms and legal complexities that outline how data is collected, processed, and exploited.[36] Further, consent is rarely informed or freely given, particularly when access to education, social life, or entertainment is conditional on agreeing to these invasive data practices.

Published terms must not be allowed to serve as a proxy for compliance. Consent, especially when obtained through a performative and meaningless 'click-through' exercise that children neither fully grasp nor freely choose is meaningless. Presenting information in age-appropriate formats, using clear, concise language, accessible visuals, and interactive elements is essential for transparency, but not sufficient alone to ensure meaningful data protection.[37]

Instead, a proactive and upstream approach that holds tech companies accountable for embedding privacy in the design of digital products and services is needed. This must include clear legal duties to minimize data collection, avoid manipulative practices, ensure genuinely privacy-protective settings from the outset, and respect children's rights and best interests by design and by default.[38] Such measures - which have been demonstrated to be efficient - must also be effectively enforced.[39]

There is significant potential for reforming the Personal Information Protection and Electronic Documents Act to be explicitly grounded in children's rights, in light of Canada's international human rights obligations. Such reform should ensure strong enforcement and independent oversight by the Office of the Privacy Commissioner.[40]

Designing to address privacy impacts and the best interests of the child

As set out in the UNCRC, children's best interests must be a primary consideration in all decisions affecting them, including in the design, development and deployment of digital products and services likely to be accessed by children.[41] Prioritizing the best interests of the child requires consideration of the full range of children's rights. This does not allow for selective interpretation or cherry-picking by companies seeking to highlight certain rights while disregarding others.[42] In particular, when the best interests of the child come into tension with commercial objectives, children's rights must take precedence. While commercial interests are not inherently incompatible with children's, companies have a duty to respect, protect, and fulfil children's rights, and must prioritize children's best interests when conflicts arise.[43]

Failing to afford children's rights and interests a high priority is inconsistent with Canada's obligations under the UNCRC, obligations that require the provision of an environment where a child can enjoy all their rights.

To give real effect to this principle, companies should be required to carry out Child Rights Impact Assessments (CRIAs) - systematic evaluations of how a digital product, service, feature, or policy affects children's rights. These assessments, in conjunction with privacy impact assessments, enable organizations to identify potential risks, evaluate their data practices, and effectively mitigate any potential negative impacts from the outset.[44] They

---

[36] Digital Futures for Children, Children's data and privacy online.
[37] 5Rights, Tick to Agree: Age appropriate presentation of published terms.
[38] UNCRC General comment No. 25, paras. 12, 39, and 70.
[39] Digital Futures for Children, Impact of regulation on children's digital lives; Children and Screens, UK Age-Appropriate Design Code Impact Assessment.
[40] Supreme Court of Canada, Baker v Canada (Minister of Citizenship and Immigration).
[41] UNCRC General comment No. 25, paras. 12, 13, and 110.
[42] Digital Futures for Children, The best interests of the child in the digital environment.
[43] UNCRC, General Comment 14, para 39; Digital Futures for Children, The best interests of the child in the digital environment.
[44] UNCRC General comment No. 25, paras. 36-38.

are a crucial element in ensuring that digital environments are designed with children's best interests in mind.[45]

Being high privacy protective by design and default

Embedding high privacy by default advances children's right to privacy and realizes their right to protection from harm and from commercial exploitation. A high bar of data privacy by design and by default reverses current industry norms of maximizing data collection and ensures children enter the digital world through a more protective starting point, while preserving their agency.

Research indicates that individuals very rarely change default settings.[46] Requiring high privacy by default for children's accounts enables privacy-preserving experiences, reducing unnecessary data collection and limiting data sharing with third parties.

Requiring privacy by design and by default provides a robust baseline of protection; alleviates the challenges associated with obtaining and managing informed consent; and ensures that children's data is protected regardless of their abilities to grasp the nuances of data privacy.

Avoid deceptive practices

Digital products and services often use default settings that encourage and facilitate extensive data collection, which provides the least privacy protection. These pre-selected privacy-invasive default settings are designed to guide user behavior, influence decisions, and manipulate children into sharing more personal data than necessary.[47]

Persuasive and addictive design strategies are deliberately employed to capture users' attention and maximize their engagement, driving increased data collection that results in more targeted advertising opportunities and, consequently, higher profits for tech companies.[48]

Towards Best Practices for Children's Privacy

Grounded in children's rights and informed by international best practices – as outlined in 5Rights' Approaches to Children's Data Protection – we recommend the OPC develop its children's privacy code on the following 15 principles. Inspired by the UK's Age-Appropriate Design Code, these principles offer a practical framework for embedding children's rights, best interests, and privacy into digital products and services by design and default.

1. BEST INTERESTS OF THE CHILD: The best interests of the child should be a primary consideration when designing and developing digital services likely to be accessed by children. Meaningfully consulting with children from different age groups, backgrounds and abilities is crucial to understanding their best interests. When the child's right to privacy conflicts with the needs or wishes of others, including corporations, the service provider must prioritize the best interests of the child.[49]
2. CHILD RIGHTS IMPACT ASSESSMENTS: Organizations must undertake Child Rights Impact Assessments (CRIAs) - in conjunction with privacy impact assessments - to assess and mitigate risks to the rights and freedoms of children likely to access their service(s). CRIAs must consider differing ages, capacities, accessibility and development needs, and the full range of risks to children's

[45] UNICEF, Assessing child rights impacts in relation to the digital environment; Department of Justice, Child Rights Impact Assessment tool and e-learning course.
[46] CNET, Default settings for privacy -- we need to talk.
[47] 5Rights, Pathways: How digital design puts children at risk.
[48] 5Rights, Disrupted Childhood: The cost of persuasive design.
[49] UNCRC, art. 3; UNCRC General comment No. 14, para. 4; UNCRC General comment No. 25, paras. 12-13.

privacy, safety and security - including content, contact, conduct and contract risks – and must be made publicly accessible.[50]

3. AGE-APPROPRIATE APPLICATION: Organizations must take a risk-based approach to recognize the age of their users and ensure they effectively apply these standards to child users. They may either establish a user's age with a level of certainty proportionate to the risks to the rights and freedoms of children or apply the standards to all their users. Any age assurance mechanisms in use must be privacy-preserving, proportionate, effective, age-appropriate, accessible, transparent and secure.[51]
4. TRANSPARENCY: Published terms, policies, community standards and privacy information, must be concise, prominent and presented in language and formats that are clear and suitable to the age of the child. Additional specific 'bite-sized' explanations should be provided at the point of use or feature activation.[52]
5. DETRIMENTAL USE OF DATA: Children's personal data must not be used in ways that have been shown or are likely to be detrimental to their well-being or contrary to industry codes of practice, other regulatory provisions or Government advice. This includes the use of personal data to extend engagement, recommend harmful content or actions, or unduly influence children's behavior, notably via automated processes or dark patterns.[53]
6. POLICIES AND COMMUNITY STANDARDS: Published terms, policies and community standards (including but not limited to privacy policies, age restrictions, behavior rules and content policies) must be upheld, including by providing appropriate moderation and support in local languages.
7. DEFAULT SETTINGS: Default settings must respect children's rights. Settings must be set to 'high privacy' by default, unless services can demonstrate a compelling reason, taking account of the best interests of the child. Features designed to extend engagement or influence behavior must be off by default. When privacy settings are set to "off" by default, users have to actively and intentionally enable them, a step that most do not take.[54]
8. DATA MINIMISATION: Only the minimum amount of personal data needed to provide the elements of a service in which a child is actively and knowingly engaged should be collected. The need to protect children must never be construed as a justification for collecting excessive data.[55]
9. DATA SHARING: Providers and operators must not disclose children's data unless they can demonstrate a compelling reason to do so, with the best interests of the child as the primary consideration. Particular safeguards should be in place for data collected in educational settings.[56]
10. GEOLOCATION: Geolocation settings must be turned off by default, unless a compelling reason that takes into account the best interests of the child requires otherwise. Services must provide a clear, visible indicator for children when location tracking is active. Any option making a child's location visible to others must automatically reset back to 'off' at the end of each session.[57]
11. PARENTAL CONTROLS: If parental controls are provided, they must respect children's rights by design. Children must be given age-appropriate information about how these controls operate. If an online service allows a parent or legal guardian to monitor a child's online activity or to track their location, children must receive a clear, visible notice that they are being monitored.[58] Functionalities should also be age-appropriate and respectful of the child's rights and agency.

---

[50] UNCRC General comment No. 25, paras. 23 and 38. For guidance, see Department of Justice, Child Rights Impact Assessment tool and e-learning course and UNICEF, Assessing child rights impacts in relation to the digital environment.
[51] UNCRC General comment No. 25, para. 114.
[52] UNCRC General comment No. 25, paras. 39, 49, 59, and 72
[53] UNCRC General comment No. 25, para. 96.
[54] UNCRC General comment No. 25, paras. 70, 75, and 77.
[55] UNCRC General comment No. 25, paras. 55 and 69.
[56] UNCRC General comment No. 25, para. 73.
[57] UNCRC General comment No. 25, paras. 40, 68, and 88.
[58] UNCRC General comment No. 25, paras. 75, 76, and 103.

12. PROFILING: Options that use profiling must be switched off by default, unless a compelling reason that takes into account the best interests of the child requires otherwise. Profiling is only allowed if appropriate measures are in place to protect the child from any potential harm, particularly regarding the exposure to content detrimental to their health or well-being. Profiling for targeted advertising is forbidden.[59]
13. DARK PATTERNS: Practices that distort or impair children's ability to make autonomous and informed choices are prohibited. These include persuasive design strategies, gambling-style features, hidden costs, unfair terms and conditions, and techniques that lead or encourage children to provide unnecessary personal data or to weaken or turn off their privacy settings.[60]
14. CONNECTED TOYS AND DEVICES: Connected toys and devices must include effective tools to ensure a high level of privacy, safety and security for children.[61]
15. ONLINE TOOLS: Finally, prominent and accessible tools must be provided to help children understand and exercise their data protection rights, report any privacy concerns, and exercise their remedial rights.[62]

Signatories:

Organizations:

1. 5Rights Foundation
2. Bridge2Future
3. Canadian Coalition for the Rights of Children
4. Canadian Paediatric Society
5. The Centre for Media, Technology and Democracy
6. Children and Screens: Institute of Digital Media and Child Development
7. The Dais, Toronto Metropolitan University
8. Digital Futures for Children centre
9. The eQuality Project
10. Embrace Health Foundation
11. The Helix Foundation
12. Inspiring Healthy Futures
13. Kids Play Tech
14. Landon Pearson Centre for the Study of Childhood and Children's Rights
15. MediaSmarts
16. National Council of Women of Canada
17. OpenMedia
18. Privacy & Access Council of Canada
19. The Waltons Trust

Individuals:

20. Dr. Kate Butler
21. Michael J. S. Beauvais
22. Prof. Dr. Leanne Bowler
23. Perry Bulwer
24. Prof. Dr. Prudence Caldairou-Bessette
25. Prof. Dr. Tara M. Collins
26. Ron Ensom
27. Michelle Gordon
28. Prof. Dr. Sara M. Grimes
29. Dr. Emmie Henderson-Dekort
30. Dr. Amy Hurley
31. Prof. Bartha Maria Knoppers, OC, OQ, AdE

[59] UNCRC General comment No. 25, para. 42
[60] UNCRC General comment No. 25, paras. 40 and 110.
[61] UNCRC General comment No. 25, para. 2.
[62] UNCRC General comment No. 25, paras. 36, 48, and 55.

32. Dr. Stefania Maggi
33. Dr. Hala Mreiwed
34. Prof. Dr. Mona Pare
35. Sharon Polsky MAPP
36. Prof. Dr. Leslie Regan Shade
37. Dr. Teresa Scassa
38. George Stamatis
39. Prof. Dr. Valerie Steeves
40. Prof. Dr. Tatyana Terzopoulos
41. Kathy Vandergrift