

**Submission to the Office of the Privacy Commissioner of Canada (OPC):
Exploratory consultation on the development of a children's privacy code**

August 2025

Ava Smithing

Youth Fellow

The Centre for Media, Technology and Democracy at McGill University

Supported by: Sonja Solomun, Helen Hayes, and Sequoia Kim¹

I. Introduction.....	1
Our Core Recommendation: A Dual Regulatory Approach.....	2
II. The Challenge: Building Autonomy Through Privacy Education.....	3
III. Canada's Leadership Moment and Strategic Opportunity.....	4
IV. Proposed Framework.....	5
IV.I. Presumption Against Collection.....	5
IV.II. Age-Tiered Autonomy and Economic Transparency.....	6
IV.III. Functionality-Based Restrictions with Built-in Education.....	7
V. Application and Coverage.....	8
V.I. Who Should Be Covered.....	8
VI. Data Disclosure and Retention.....	9
VII. Privacy Impact Assessments and Child Protection by Design.....	10
VIII. Enforcement and Regulatory Oversight.....	11
IX. Autonomy, Transparency, and Education.....	13
X. Conclusion and Recommendations.....	14

I. Introduction

As a Youth Fellow at the [Centre for Media, Technology and Democracy](#)² at McGill University, I bring a unique perspective to this submission, which is informed by lived experience, academic

¹ Sonja Solomun is the Deputy Director of the Centre for Media, Technology and Democracy. Helen Hayes is the Director of Development and a Senior Fellow, AI Policy at the Centre for Media, Technology and Democracy. Sequoia Kim is the Research Manager at the Centre for Media, Technology and Democracy.

² [Centre for Media, Technology and Democracy](#) at McGill University is an interdisciplinary research centre dedicated to understanding and responding to the social, political, and policy challenges posed by our evolving information ecosystem and digital technologies.

research, and engagement with children's privacy policy in both Canada and the United States. This submission reflects the Centre's commitment to safeguarding children's rights in digital environments, and our belief that children's privacy is not merely a matter of regulatory compliance, but a prerequisite for democratic agency, civic participation, and long-term digital resilience.

Children's privacy is not simply a legal compliance issue — it is a democratic necessity. Privacy is a fundamental component of creating digitally literate, democratically engaged citizens. When children are raised using systems governed by business models that normalize surveillance, targeted manipulation, and commercial exploitation, they learn to expect intrusion rather than privacy and autonomy. In such an environment, it becomes impossible for young people to develop adequate digital literacy and critical agency.

Privacy must follow children wherever they go online. Children should not be forced to seek out privacy protections online, or be restricted from platforms that cannot offer user functionality without gathering undue data from children's accounts. This requires a two-pronged approach to enable children to move through digital spaces with privacy protections that enable, rather than restrict, their access to digital participation.

Canada stands at a pivotal crossroad. As jurisdictions around the world struggle to regulate digital platforms and AI-driven harms, Canada has the opportunity to adopt a rights-based, globally harmonized framework that both protects children and sets international standards. Drawing on global best practices including the U.K. [Age Appropriate Design Code](#),³ the EU [Digital Services Act](#) (DSA),⁴ and the [UN Convention on the Rights of the Child](#),⁵ this submission outlines a dual regulatory approach that can move Canada beyond outdated consent models and toward a new paradigm of default protection, autonomy, and accountability by design.

Our Core Recommendation: A Dual Regulatory Approach

We recommend that the OPC adopt a dual regulatory approach to children's privacy grounded in international best practices, children's developmental needs, and risk-based governance. This model comprises two core pillars:

1. Necessity-based data collection limits: Canada should establish strong, necessity-based limits against the collection of any personal data of children under 18 unless it is demonstrably required for safety or core functionality.

³ Information Commissioner's Office, [Age Appropriate Design Code](#).

⁴ EU, [Digital Services Act](#).

⁵ UN, [Convention on the Rights of the Child](#).

2. Design-based prohibitions with mandatory education: legislation should target specific harmful functionalities while requiring that technology be “explainable” to children through transparent, age-appropriate interactions that build privacy literacy in real-time.

Canada can lead by implementing:

- **Design-based enforcement mechanisms digital platforms and AI systems that prevent harm** rather than solely respond to violations
- **Autonomy-focused frameworks** that treat children as developing rights-holders who learn through consistent interaction with privacy-protective technologies
- **Scalable enforcement mechanisms** that keep pace with technological change through continuous youth consultation and participatory oversight

This approach addresses a critical challenge facing smaller markets, including Canada: large platforms may threaten to age-gate children out rather than respect their privacy rights. Canada can counter this by either ensuring universal privacy protections that make age-gating impossible, or by strategically investing in Canadian safe AI innovation to reduce dependence on exploitative platforms.

II. The Challenge: Building Autonomy Through Privacy Education

Historically, Canadian children have been thrust into digital environments where privacy must be actively discovered, understood, and opted into, if meaningful options even exist at all. This paradigm often creates a form of learned privacy helplessness, teaching young people that surveillance and data extraction are normal. Rather than experiencing privacy as a right, children are conditioned to view it as a feature they must opt into — one that is hard to access, poorly explained, and often functionally incompatible with the products they use. This is not a technical flaw; it is the logical consequence of a business model that prioritizes engagement and monetization over user safety. **Young Canadians want privacy, transparency and education.**⁶ Although research indicates that many young Canadians do not view access to and storage of their data by Big Tech platforms as inherently problematic, they do call for more transparency about these data practices, and have indicated a strong preference to be educated about data privacy and design interactions.⁷

Traditional consent often fails child users, not only because they can struggle with learned privacy helplessness, or resist privacy protections due to apathy or consent fatigue, but also

⁶ Department of Justice of Canada, [Youth Views on Addressing Privacy](#).

⁷ MediaSmarts, [Young people's attitudes towards privacy](#).

because understanding privacy rights requires nuance that Big Tech companies are unwilling to provide. Even well-intentioned reforms requiring opt-in consent still place responsibility on users to understand complex data practices designed by behavioural psychology teams that, in many cases, leave users surrendering function for privacy.

We must build children's capacity to understand privacy through ongoing, literacy-building interactions on platforms, rather than expect them to make informed decisions about their privacy in high-pressure moments. We propose requiring that Big Tech implement clear, embedded explanations about data access and storage in all privacy-affecting features on their platforms. This “functionality-based approach” to privacy literacy requires platforms to work transparently by educating children, in real time, about privacy as a right they deserve, not a burden they must manage.

III. Canada's Leadership Moment and Strategic Opportunity

Around the world, regulators are grappling with how to protect children's privacy in a global digital economy that is shaped by monopolistic practices and extractive AI systems. For example, recently [proposed updates](#)⁸ to the U.S. [Children's Online Privacy Protection Act](#)⁹ show both progress and persistent limitations: while new targeted advertising restrictions represent progress, they still fundamentally rely on parental consent mechanisms that can actually enable user surveillance rather than genuine protection.

These federal limitations are compounded by variations in enforcement at the state level, demonstrating the challenges of implementing children's privacy protection in fragmented regulatory environments where different jurisdictions have different ideas of what children need to be safe online. Some jurisdictions have even incorrectly treated necessary privacy audits as infringements on speech rights rather than essential oversight mechanisms. While the U.S. continues to navigate tensions between corporate speech claims and parental oversight, Canada is fortunately not bound by the same structural constraints. With fewer domestic platform interests shaping the debate, Canada is uniquely positioned to lead with an approach to privacy legislation that centers children's digital rights and wellbeing.

Outside of North America, The U.K.'s Age Appropriate Design Code has driven measurable platform changes, including default privacy settings and profiling restrictions, demonstrating that comprehensive approaches can achieve meaningful results. The U.K. approach, however, faces

⁸ Senator Edward Markey of Massachusetts, “[Senators Markey and Cassidy Reintroduce Children and Teen’s Online Privacy Protection Legislation](#).”

⁹ Federal Trade Commission, [Children's Online Privacy Protection Rule \("COPPA"\)](#).

particular difficulties with the enforcement of algorithmic design requirements, which extend beyond traditional data protection frameworks. The focus on algorithmic outcomes, such as requiring platforms to make recommender systems 'safer,' creates enforcement challenges because regulators must audit abstract algorithmic behaviour as opposed to the use of data by those algorithmic systems. Our proposed functionality-based approach addresses this by focusing on data inputs as the core of protection policy. This creates clear, binary compliance standards: either a platform collects behavioural profiling data from children, or it does not.

Canada's Strategic AI Leadership Opportunity: As a global AI leader, Canada's position depends on establishing public trust through responsible innovation frameworks. Clear boundaries around children's data will provide a foundational framework for future AI governance, making it easier to build comprehensive protections rather than retrofitting safeguards after systems are already deployed. This proactive approach will demonstrate that ethical AI development is not only possible, but advantageous, encouraging broader adoption through public trust while positioning Canada as the international standard-setter for responsible AI governance.

It is likely that the United States will be the next jurisdiction to regulate AI, creating a massive market for compliance software. Canada should invest now through tax credits and grants for privacy-compliant Canadian AI development. When companies need compliance tools for the U.S. market, Canadian companies will be positioned to dominate this sector, securing both economic advantage and global privacy leadership.

IV. Proposed Framework

IV.I. Presumption Against Collection

Canada should establish a strong legal presumption against data collection from individuals under 18, with collection permitted only when organizations demonstrate it is strictly necessary for safety and core product functionality. This burden-shifting requires organizations to justify their data collection practices rather than require users to prove the inappropriateness of that collection.

Crucially, monetization of children's data should not qualify as "core functionality." While organizations argue that advertising supports "free" services, commercializing children's personal information represents exactly the exploitation privacy protection should prevent. Organizations serving children should develop business models that are not dependent on extracting value from children's information.

Organizations must demonstrate not only that collection supports the necessary functionality of their products, but that they have implemented privacy-protective alternatives and collect as little data as possible. This incentivizes innovation in privacy-protective design while establishing clear boundaries between users and platforms.

Specific data categories should be automatically disabled for under-18 users:

- Location tracking (except demonstrably necessary safety functions)
- Biometric data collection (prohibited except limited health related circumstances with explicit safeguards)
- Conversational data from AI systems (complete prohibition for collection, retention, or use in training)
- Behavioural profiling data (prohibited for comprehensive psychological profiles)

Children should access the highest privacy protections without requiring parental consent. While parental involvement may be appropriate for certain decisions, access to privacy protections should never be contingent on parental permission.

IV.II. Age-Tiered Autonomy and Economic Transparency

Canada should implement age-appropriate tiers that respect children's developing autonomy while protecting them from exploitation:

Ages 14-15: Basic Personalization Only

- Can opt-in to basic, non-harmful personalization features: for example, an opt-in feature that allows users to expressly self-select information about device type, age, and city/town location.
- Cannot opt-in to behavioural profiling or engagement maximization or any monetization of their data.
- All opt-ins require a clear explanation: For example, "This feature uses your listening history to suggest similar music. No data is sold or used for advertising."

Ages 16-17: Personalization with Economic Transparency

- Can opt-in to more complex personalization features
- Can opt-in to monetization ONLY with dual consent (both youth and parental) and mandatory economic disclosure

- Mandatory economic transparency for ALL monetization opt-ins: For example, "We make \$5.50 per month from your data. We sell your information to Meta, Amazon, and Acxiom for advertising purposes. If you opt out, we make \$0 from your data."
- Must show concrete impact: For example, "Your data will be shared with 247 companies including your school district."

Ages 18+: Full Autonomy

- Complete decision-making authority over their data

This framework recognizes that children should never be able to consent to financial exploitation, even if they think they want to, while still providing older teens with meaningful choices about non-exploitative features.

IV.III. Functionality-Based Restrictions with Built-in Education

Rather than determining whether services are "directed at children" to trigger enforcement, enforcement should trigger based on platforms' specific functionalities and data practices. This prevents platforms from evading responsibility by claiming ignorance while implementing features designed to engage young audiences.

Digital services that deploy the following functionalities are subject to heightened regulation when accessible by children:

- Behavioural recommender systems trained on children's data
- Algorithmic nudging toward over-disclosure (e.g., streaks, simulated affection, or reward loops)
- AI agents interacting with minors
- Default settings that enable location tracking, biometric profiling, or emotion-inference models
- Infinite scroll or autoplay features designed to maximize engagement time
- Social pressure mechanics (public follower counts, "seen" indicators, etc.)
- Gamification features that reward data disclosure

When platforms use these features, they must educate children about privacy in real-time through objective explanations:

- Behavioural recommender systems must show users what data drives recommendations: For example, "This recommendation analyzed your last 47 clicks and inferred you prefer fitness content."
- AI systems interacting with children must clearly explain data use: For example, "This conversation will be stored for 30 days and used to improve responses. It will not be used for advertising."
- Privacy settings must use plain language showing real impact ("visible to 247 people including teachers") rather than technical jargon
- Economic transparency must be embedded: For example, "This feature generates \$2.30 monthly revenue from your data through targeted advertising."
- All explanations must be factual and objective, never manipulative or designed to encourage data sharing

Regular transparency check-ins: Platforms must provide quarterly prompts asking children if they want to continue sharing their data, with clear information about what has been collected to date, how it has been used since the last check-in, and how software updates have impacted their privacy.

Recent legal developments around age verification demonstrate that technology companies possess sufficient data to identify child users when required by law.¹⁰ Organizations should use existing capabilities for protection rather than pleading ignorance.

V. Application and Coverage

V.I. Who Should Be Covered

Enacted in 1998, the United States' [Child Online Privacy Protection Rule](#) (COPPA) remains the sole comprehensive children's data protection law in North America. COPPA has fundamental limitations that allow platforms to claim ignorance about whether they serve child users, despite implementation of features specifically designed to attract young audiences. This audience-based approach creates perverse incentives where platforms benefit from claiming not to know the demographics of their users. In reality, however, most large platform companies employ teams of user experience designers, behavioural psychologists, and data scientists to optimize engagement with exact target demographics.

¹⁰ See *The Wall Street Journal*, "[The Facebook Files](#)" and Electronic Privacy Information Center (EPIC), "[Supreme Court Rules that Government Can Impose Age Verification Requirements on Porn Sites Subject Only to Limited Privacy Safeguards](#)."

Emerging international children's privacy frameworks often rely on numerical demographic standards (i.e. that the platform has a "significant number of child users") for implementation. This, however, allows platforms to escape responsibility by downplaying or disregarding their child user base. **Canada should reject percentage-based thinking and instead establish a privacy regime that necessitates implementation even under circumstances where the likelihood of child use is low.**

This functionality-based approach focuses on service behaviour and data collection rather than claimed audiences. Organizations should use existing technological capabilities for age-appropriate protections rather than pleading ignorance.

If organizations want to restrict children's access to their products/services, they must justify this decision to children in clear language, including how their product violates data protections set out in Canada, and why it is impossible for their product to offer higher standards of privacy for users. This approach would place the burden on organizations to objectively explain their business prioritization choices instead of blaming regulatory compliance for access restrictions.

VI. Data Disclosure and Retention

Complete prohibitions:

- AI model training or commercial profiling data: Children's personal information cannot be used to train AI systems or create commercial profiles, as this enables persistent manipulation across platforms and over time
- Data broker access: Data brokers cannot access children's information as minors cannot enter valid contracts and such access creates inherent safety risks
- Behavioural and emotional data from chatbot interactions: Complete prohibition on collection, retention, or use of conversational data from AI interactions with children

Restricted disclosures:

- Location and biometric information — except specific safety functions benefiting the child
 - Educational and developmental data — except with explicit educational purpose and safeguards
-

VII. Privacy Impact Assessments and Child Protection by Design

Organizations deploying covered functionalities must complete comprehensive Child Privacy Impact Assessments (CPIA) that fundamentally differ from standard privacy assessments. CPIAs must demonstrate how children's best interests and developmental needs are integrated into every design decision, moving beyond compliance checklists into preemptive protection analysis.

CPIAs must evaluate each proposed feature against the UN Convention on the Rights of the Child's best interest standard, requiring organizations to document why any data collection serves children's wellbeing rather than commercial interests. Organizations cannot simply assert their features benefit children. They must provide developmental research supporting their claims and demonstrate consideration of less invasive alternatives, documenting why these alternatives are not ultimately chosen.

CPIAs must assess impacts unique to children, including children's understanding of long-term consequences of data collection and storage. Organizations must specifically analyze how features might exploit children's developmental characteristics and document mitigation strategies and identified risks, with step-by-step plans for implementation that auditors can use to ensure risks were appropriately mitigated. **Organizations must avoid deploying inherently high-risk features even with mitigation plans, particularly where less harmful alternatives exist.**

Organizations must establish CPIA Advisory Panels comprising representative populations of their platform's users, selected through stratified sampling to ensure demographic representation. These panels must convene at multiple design phases, including initial concept development, minimum viable product testing, and pre-launch review. Members must be fairly compensated for their time and efforts, and organizations must publish transparent reports detailing what the advisory council suggested, what the organization implemented, and what they did not implement and why. These panels should complement, not replace, consultation with professionals, teachers, parents, and other adults.

CPIAs must examine disproportionate impacts on vulnerable groups of children, including those with disabilities, Indigenous children, 2SLGBTQI+ youth, and children from marginalized populations. Children's experiences of privacy, safety, and autonomy are shaped by multiple identity factors that should be considered through intentional consultation, with understanding that intersecting vulnerabilities can be exacerbated by certain platform features.

CPIAs must include detailed analysis of how organizations' revenue models create incentives for or against child protection, explicitly documenting potential conflicts between

commercial objectives and child welfare, and demonstrating how design decisions prioritize children's interests when conflicts arise.

Ongoing Assessment and Real-World Impact Monitoring: CPIAs must be updated annually as well as before any significant feature changes in order to reflect new research on child development and digital harms. Organizations must implement systematic monitoring, including regular child user surveys, behavioural analytics tracking concerning usage patterns, and partnerships with mental health organizations and youth-led organizations to identify platform-related harms. Organizations must establish clear metrics for child wellbeing, including user agency (can children find and use privacy controls?), comprehension (do children understand data collection?), and autonomy (are children making free choices or responding to manipulation?).

When monitoring reveals concerning patterns, organizations must demonstrate specific design changes in updated CPIAs, test revisions with reconvened Child Privacy Advisory Panels, and engage independent researchers to validate impact assessments.

VIII. Enforcement and Regulatory Oversight

The proposed functionality-based approach creates clearer enforcement pathways than traditional regulatory models by focusing on auditable data practices rather than subjective content assessments. The OPC should implement functionality-based enforcement that creates clear compliance pathways while ensuring meaningful protection for children through participatory oversight mechanisms.

Technical Audit Framework

The OPC must establish mandatory technical audits for all organizations deploying covered functionalities accessible to children. These audits verify compliance through technical inspection of data collection systems, API configurations, database schemas, and data flow architectures. Organizations must provide complete technical documentation demonstrating that prohibited data types are not collected, stored, or processed, and that required protections are implemented at the system level rather than through policy alone.

Youth Oversight and Enforcement Panels

The OPC should establish regional Youth Privacy Oversight Panels comprising children, young adults, and youth advocates who participate in audit design, review enforcement decisions, and

evaluate the real-world effectiveness of implemented protections. These panels should include diverse representation across age groups (13-15, 16-18, 19-25), cultural backgrounds, abilities, and digital literacy levels. Panel members should be fairly compensated and provided with objective training from technical and policy experts on privacy concepts and regulatory processes.

Participatory Audit Design: Youth Oversight Panels should collaborate with OPC technical teams to design audit protocols that reflect how children actually use platforms rather than how adults assume they do. This includes identifying which features children find most problematic, which privacy controls they actually understand and use, and which design patterns most effectively manipulate their behaviour.

Proactive Compliance Verification

Rather than responding only to complaints, the OPC should conduct regular proactive audits based on functionality deployment, with Youth Oversight Panels helping to prioritize which platforms and features require immediate attention based on youth community concerns. Organizations using behavioural recommender systems, AI interactions with children, or data monetization features trigger automatic audit requirements.

Mandatory Research Transparency and Data Access

The OPC should require organizations to provide qualified researchers with access to anonymized platform data necessary for studying children's digital experiences and platform impacts. This includes usage patterns, feature interaction data, and anonymized records of how children engage with privacy controls. Research access requirements should mirror emerging frameworks like the EU Digital Services Act's [researcher access provisions](#),¹¹ ensuring independent oversight of platform impacts while protecting individual privacy.

Organizations cannot hide behind trade secrets when children's wellbeing is at stake. Mandatory data transparency enables the research community to identify emerging harms, validate platform claims about child protection, and inform evidence-based policy development.

Government Investment in Canadian Privacy Innovation

Canada should strategically invest in privacy-compliant AI development through tax credits and grants for Canadian companies developing privacy-protective technologies. This positions Canada to lead the global market for compliance tools when other jurisdictions regulate. As the

¹¹ EU, [Delegated act on data access under the Digital Services Act \(DSA\)](#).

U.S. inevitably regulates children's privacy, Canadian companies will be positioned to provide the compliance infrastructure, securing both economic advantage and global privacy leadership.

This investment should prioritize:

- AI systems implementing privacy-by-design that can operate without behavioural profiling
- Age-appropriate interface design tools
- Privacy transparency and education technologies
- Compliance monitoring and audit systems

Evidence-Based Penalty Structure

Enforcement actions should escalate based on platforms' specific functionalities and the documented harms of their products rather than on arbitrary company size thresholds, with Youth Oversight Panels providing input on which violations cause the most significant real-world harm to children. Platforms using multiple prohibited functionalities or demonstrating intentional circumvention of protections face enhanced penalties, while those making good-faith compliance efforts receive proportionate responses.

IX. Autonomy, Transparency, and Education

Children's privacy literacy cannot be supplemental but must be embedded in digital systems' structural design. Privacy education should happen through ongoing interaction with privacy-protective technologies, not separate resources children may never access.

Essential Components:

- **Youth co-design of privacy interfaces** ensuring controls reflect children's actual needs through deliberative forums such as Youth Assemblies, Forums, and Dialogues
- **Embedded transparency** making data practices visible through interface design via the functionality-based approach
- **Confidence-building prompts** helping children understand that they are exercising control over their digital experience
- **Progressive disclosure** providing information most relevant to the child prominently, with detailed information available upon request

The goal with these components is to teach child users that privacy is a right they deserve, not a burden they must manage or a technical problem they must solve. **Every interaction with technology should reinforce child user agency and help them understand their digital rights.**

X. Conclusion and Recommendations

Privacy is not just a legal principle. It is a developmental tool necessary for creating a resilient, digitally literate population capable of using digital platforms and adopting AI tools safely. Implementing these crucial privacy protections will build a generation that better understands the pitfalls and perils of digital surveillance and persuasion, is equipped with the knowledge and understanding of how to avoid privacy-violating digital platforms and tools, and can fully participate in digital society knowing that their agency is protected.

Canada has the opportunity to prove that protecting children's privacy enhances rather than restricts innovation. By investing in privacy-protective technologies and requiring transparency by design, Canada can demonstrate that ethical business models are not only possible, but advantageous.

To that end, our core recommendations to the OPC are as follows:

- I. Implement necessity-based data collection limits with clear burden of proof on organizations
- II. Establish age-tiered autonomy with economic transparency for all monetization
- III. Require functionality-based, educational transparency that teaches privacy through design
- IV. Create participatory enforcement by investing in and supporting the development of Youth Oversight Panels
- V. Invest strategically in Canadian privacy innovation to secure global leadership
- VI. Ensure privacy is a hallmark of children's online experience, rather than relegating child users to specific "privacy-safe" online destinations

Further Questions for the OPC:

- I. Should Code prohibit dark patterns entirely? Especially when directed to or accessible to minors?
- II. Should Canada mandate sandbox testing of age-appropriate designs (ex. UK ICO) before product deployment?

III. What legal tools can help children assert rights independently especially in contexts of conflict or harm?

Enforcement of these recommendations should focus on the design of products, and should not put the onus on users, especially children, to navigate and understand complex privacy provisions. Canada can lead the world in demonstrating that children's privacy protection creates stronger, more innovative digital economies while preparing young people for full democratic participation in an AI-driven future.