Kids Rights Canada

The Digital Blackbox

Building digital agency beyond online safety

Written by **Heidi Chan**

6 Feb 2026

WWW.KIDSRIGHTSCANADA.ORG

Executive Summary

A Critical Moment for Action:

Kids Rights Canada has closely monitored the House of Commons Standing Committee on Canadian Heritage (CHPC) regarding the Effects of Influencers and Social Media Content on Children and Adolescents. We commend Parliament for prioritizing this urgent issue that can no longer be delayed. We also extend our deepest gratitude to the community partners whose invaluable insights have shaped this vital discussion.

The Missing Piece: Agency

While current testimony has rightly focused on protection — shielding children from exploitation and algorithmic harm — this approach is important but incomplete. Canada ratified the UN Convention on the Rights of the Child (UNCRC) in 1991, yet current policies still treat children as passive recipients of technology rather than rights-bearing citizens.

The "3 Ps" Framework

A "protection-only" strategy is destined to fail. To truly safeguard our children, we must adopt a comprehensive approach:

- Participation (Agency): Listen to children to understand how they are targeted.
- Provision (Literacy): Provide children with the tools to understand the systems.
- Protection (Safety): Design systems that ensure children are safe by default.

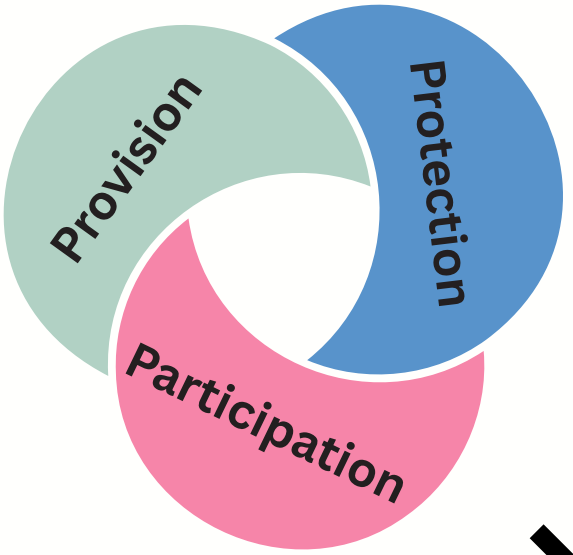
In this report, we will outline how the 3Ps is a useful framework to understand children's role in the digital world, and provide recommendations that lead to genuine child protection and empowerment.

The "3P" Framework:

Why Protection Alone Is Not Enough

Canada ratified the United Nations Convention on the Rights of the Child (UNCRC) in 1991. The UNCRC outlines that children should be treated as both recipients of protection, as well as active participants in the communities that affect their lives.

Although the UNCRC was written in 1989, long before this generation's digital-native children were born, this framework remains an effective tool we have for regulating the digital world. It reminds us that a child's rights are indivisible. While shielding children from harm is vital, a "protection-only" approach is destined to fail because it treats children as passive victims rather than active citizens. To truly keep children safe, legislation must balance all three pillars of the children's rights, being 'Protection', 'Provision', and 'Participation'.



1. Participation

Under Article 12 of the UNCRC, children have the legal right to express their views freely in all matters affecting them, and adults must take them seriously. In the digital context, this means that we must recognize children as active digital citizens with the right to shape the online world..

Children are the primary experts on their own digital lives (1) and are passionately keen to participate in the digital world (2). 95% of young Canadians would like to take an active role in ensuring their safety online (3). However, in reality, they are often treated as passive subjects both on the platform and policy level. They are spoken about, but rarely spoken to (4).

- **On Social Media Platforms:** On most platforms, a child's only mechanism for agency is the ‘Report’ button. Research shows children feel these reports go nowhere, leading to a sense of "learned helplessness" where they stop trying to advocate and protect themselves because they believe the system doesn't care (2).

- **On Policy Making:** Currently, digital safety legislation is drafted almost exclusively by adults. This "adult-centric" approach often results in policies that prioritize restriction rather than resilience (1). When children are excluded from the drafting process, participation becomes tokenistic.

Safety features will only be effective if they are co-designed with the youth they are meant to protect. A room full of adult lawyers cannot predict the social nuance of a 13-year-old’s group chat. Without child participation, we are building safety tools that miss the mark entirely.

2. Provision

Provision traditionally ensures children have access to essential resources like healthcare and education. In the digital world, this definition must expand to include the Right to Accessible Information (Articles 13 & 17). We must ensure children have the access to digital tools that aid their development, as well as equipping children with the digital literacy they need to navigate online spaces.

Currently, social media algorithm operates as a "Black Box," denying children the literacy they need to give meaningful consent. We are failing to provide them with the honest transparency required to navigate these spaces safely.

This failure of provision manifests in two critical ways:

- **The "Consent" Fiction:** Existing social media "Terms of Service" are often 5,000+ word legal documents written at a postgraduate reading level (5). Children click "I Agree" without knowing what they are agreeing to (6). Expecting a child to read and understand these contracts is unreasonable.

- **The Algorithmic Black Box:** Children are constantly targeted by algorithms based on invisible data points. They see extreme or commercial content without knowing why it was chosen for them, making them vulnerable to manipulation because they cannot distinguish between organic reality and targeted advertising (7).

3. Protection

Protection means shielding children from abuse, neglect, and exploitation (Article 19). All actions concerning children should also use their best interest as a primary consideration (Article 3). In the digital world, this definition must expand to include the invisible architecture of the platforms themselves. We must regulate systems to prevent harm before it happens.

This includes, but is not limited to, protecting children from:

- **Developmental Exploitation:** Algorithms that weaponize psychological vulnerabilities (like FOMO or body image insecurity) to maximize engagement.
- **Sextortion**: Criminals posing as peers to coerce children into sending intimate images, then blackmailing them.
- **AI & Deepfakes Exploitation**: The non-consensual creation of imagery using a child's face (often harvested from innocent social media posts).
- **Economic Exploitation:** The unregulated use of "kidfluencers" whose labor and privacy are monetized without legal safeguards.

Currently, platforms are designed to maximize profit, "time on device" and engagement, often by exploiting human psychological vulnerabilities (8). Features like infinite scroll, auto-play, and aggressive notifications create a digital environment that creates compulsive behavior, and children are susceptible to dangerous content targeted directly at them, prioritizing corporate profit over the developmental needs of the child .

Recommendations

A Call to Action

For the Federal Government

Establish a National Youth Advisory Council:

We cannot regulate the digital world without the architects who will live in it. The Government should mandate a permanent, formal Youth Council to review all digital safety policies before they are passed. This ensures children are active partners in governance, not just passive subjects of consultation.

For the Education Sector

Mandate Digital Literacy Education in Schools:

We must move towards a Digital Citizenship Framework by prioritizing civic empowerment in education. Schools must teach children how the algorithm works, how data is monetized, and how to critically analyze algorithmic bias. We must teach children not just how to use the tools, but how the tools use them.

Recommendations

A Call to Action

For Social Media Platforms

Legislation must require platforms to adopt the "Best Interests of the Child" as a non-negotiable technical standard, enforced through three key mechanisms:

- **Safety by Design**: Features proven to exploit developmental vulnerabilities — such as infinite scroll, auto-play, and reward loops — must be legally reclassified as "Design Defects" and banned for minors.

- **Safety by Default:** When a user is under 18, the default setting of the app must be the safest possible version, such as turning off by default the Geolocation, Direct Messaging from strangers, and Data collection etc. The burden of safety must shift from the child to the platform. No child should have to "opt-in" to safety.

- **Child-Friendly Terms:** Replace dense legal contracts with mandatory child-friendly summaries using simple language and icons appropriate for the user's age.

- **"Just-in-Time" Notifications:** Mandate pop-up interventions at critical moments (e.g., before posting a public photo) to encourage mindful decision-making.

- **Responsive Feedback Loops:** Replace the "Report" void with functional tools that allow children to flag unwanted content, with a legal requirement for the algorithm to immediately adjust and stop showing that content.

Conclusion

We stand at a critical crossroads in the history of childhood. For too long, our approach to digital safety has been defensive — defined by restrictions against emerging harms. We have built higher walls, but we have failed to teach children how to climb.

But a wall is not a strategy. And a child is not a passive problem to be managed.

The digital world is no longer separate from the "real" world; it is the playground, the classroom, and the town square of the 21st century. To deny children agency in this space is to deny them their citizenship. If we continue to treat children merely as data points to be monetized or victims to be shielded, we will fail them.

References

1. Livingstone, S., & Pothong, K. (2022). Imagine the internet of the future: A child-centred vision for the metaverse. London School of Economics and Political Science. https://doi.org/10.2193/LSE.4i5n3208

2. Third, A., & Moody, L. (2021). Our rights in the digital world: A report on the children's consultation to inform General Comment No. 25. 5Rights Foundation. https://5rightsfoundation.com/uploads/Our_Rights_in_the_Digital_World.pdf

3. Steeves, V. (2014). *Young Canadians in a Wireless World, Phase III: Online Privacy, Online Publicity*. MediaSmarts.

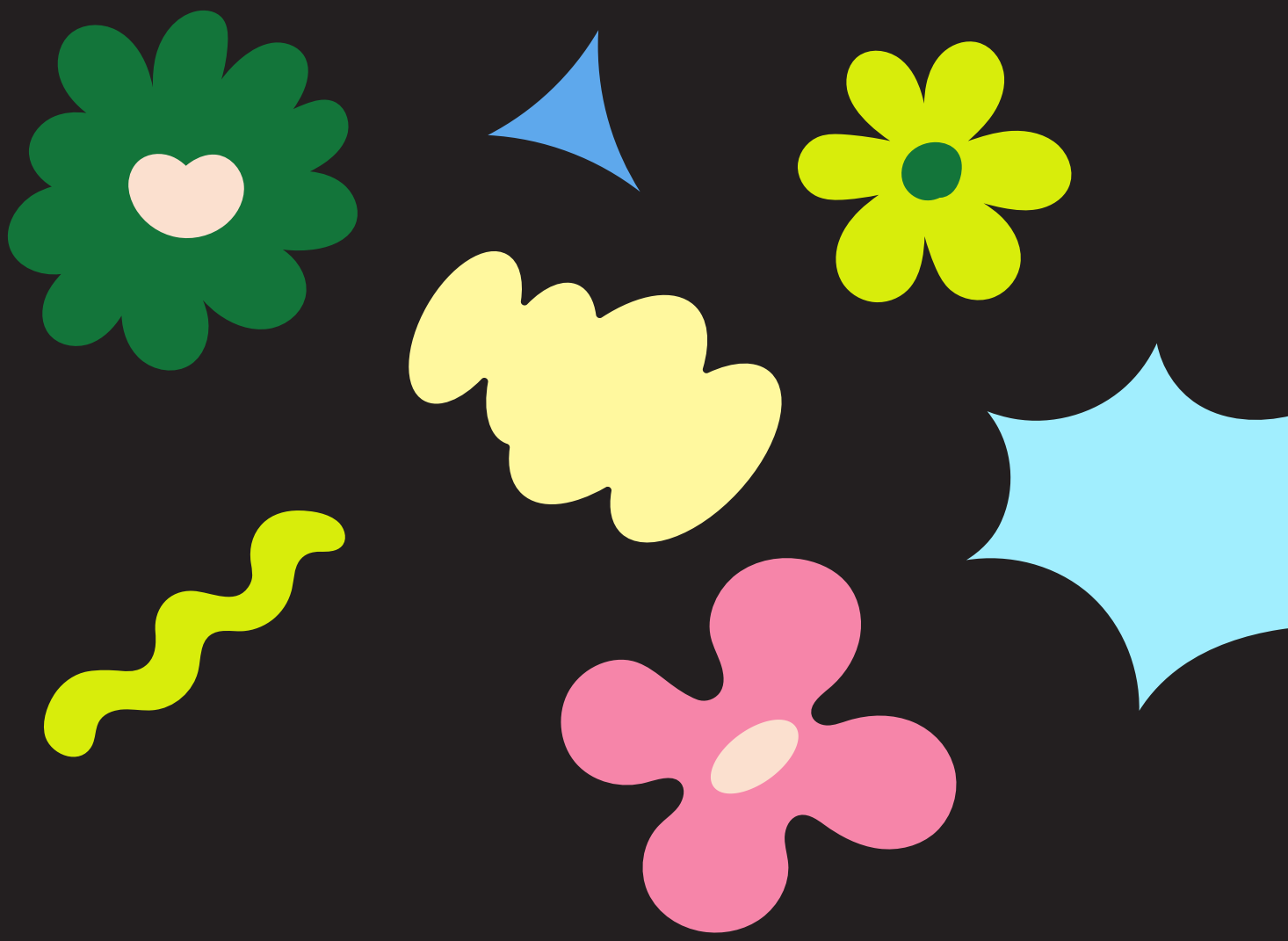
4. Helsper, E. J., Rao, S., & Lyons Longworth, M. (2025). Left out and misunderstood: Children in digital policies. A global review. Digital Futures for Children centre, LSE and 5Rights Foundation. https://eprints.lse.ac.uk/130444/

5. Children's Commissioner for England. (2017). Growing up digital: A report of the Growing Up Digital Taskforce. https://assets.childrenscommissioner.gov.uk/wpuploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf

6. Arone, J. (2024). You'll need a college education to read the terms of service for these social media sites. All About Cookies. https://allaboutcookies.org/social-media-terms-of-service

7. Polanco-Levicán, K., & Salvo-Garrido, S. (2022). Understanding Social Media Literacy: A Systematic Review of the Concept and Its Competences. International journal of environmental research and public health, 19(14), 8807. https://doi.org/10.3390/ijerph19148807

8. Scott, L. (2025). The ethics of exploitation: How social media profits from attention, addiction, and data manipulation. NSU Undergraduate Law Journal, 1(1). https://nsuworks.nova.edu/nulj/vol1/iss1/2/



Thank you!

info@kidsrightscanada.org

www.kidsrightscanada.org