5RIGHTS FOUNDATION

Toward a Safer and Rights-Respecting Digital Environment for Children in Canada

June 2025

One in five internet users is a child in Canada. Technology now shapes almost every aspect of their lives and development, from how they learn and play to how they express themselves.

Yet, the digital world was never designed with children in mind, resulting in a systematic failure to account for their unique needs, vulnerabilities, and rights.

Risky by Design

Children face far more risks than just harmful content, technical bugs, or bad actors in the digital world. Many of those risks are not accidental but are embedded in the very design of digital products and services.

5Rights' Disrupted Childhood: The cost of persuasive design, Pathways: How digital design puts children at risk, Risky by Design, and Twisted Toys show how tech companies make deliberate design choices that shape the experience of children online for the sake of profit.

Children are trapped in highly automated systems designed to maximize attention, reach, and interaction at any cost. Companies make it purposefully hard for children to put down their devices, pushing network growth to the extent that children are introduced to inappropriate adults, and encouraging them to post, share and enhance their content to such a degree that many children feel their 'real selves' are inadequate.

Automated pathways, optimized for commercial goals, routinely expose children to sexualized content,[1] and nudge children toward in-game purchases[2]. They are bombarded with targeted advertising and misinformation,[3] and they subjected to AI power features include chatbots that foster unhealthy emotional attachment, while profiling that deepens inequalities and reinforce discrimination.

The result is a system that exploits children's psychological triggers like social anxiety, fear of missing out, and the need for validation through persuasive and addictive design strategies that purposefully nudge them into risky behaviours, manipulative design and invasive and exploitative data practices[4].

A child who merely 'hovers' over a video is inundated with more of the same. A child who clicks on a dieting tip, is recommended bodies so unrealistic they warp any healthy body image within the span of a week. And even when children honestly report their age –

---

[1] 5Rights research uncovered several pornographic pictures shared in two Recommended public chats on AntiLand: "Hell on Heels" and "Fat Lovers 2.0" in April 2021.

[2] The Rip-Off Games: How the Business Model of Online Gaming Exploits Children. A Parent Zone Report. August 2019.

[3] Facebook executives shut down efforts to make the site less divisive, The Wall Street Journal, May 2020.

[4] Dataethics (2021), Games are gambling with children's data.

however young – they are offered content and experiences that would be illegal in almost any other context.

Alarmingly, the digital world does not merely fail to cater to children's needs – it intentionally preys on their vulnerabilities. Testimony from Meta whistle-blowers Frances Haugen[5] and Arturo Béjar[6] reveals how service providers prioritize business growth at the expense of children's wellbeing. Haugen reported that despite internal data showing that 1 in 3 teen girls[7] suffers body-image problems on Instagram, Meta systematically chooses company profit over public good.

And it is this sort of careless choices and careless design that systematically exposes children to harmful material, commercial surveillance, compulsive behaviour, and other risks undermining children's rights in pursuit of profit.

Privacy and Data Protection

Data fuels many norms of the digital world. In an increasingly connected world, every click, swipe, and scroll generate data - whether shared explicitly, left in digital traces, or inferred by algorithms.[8]

How children's data are collected, shared, and used shapes every aspect of their digital experience and wider lives. With an average of 72 million data points collected on a child before they turn 13,[9] the value and scope of this data collection often remain opaque. It may also be difficult for children to understand lengthy and complex terms and conditions, undermining their agency to give an informed and meaningful consent.[10]

Strong data protection is fundamental for ensuring children's privacy, safety, and agency in the digital environment, and building on the UK Age-Appropriate Design Code and international best practices 5Rights champions enforceable standards that embed privacy by design, limit the commercial exploitation of children's personal information, and ensure accountability and transparency across borders.

Artificial Intelligence

Artificial Intelligence (AI) systems further exacerbate many risks that children face online, including the violation of their right to privacy in the digital world.

AI systems are built, trained on, and designed to harvest enormous quantities of children's data – often without meaningful consent or oversight. Yet, in light of AI's specific characteristics (including opacity, complexity, dependency on data, and autonomous behaviour),[11] children are unlikely to have the developmental capacity,

---

[5] The New York Times (2021, updated 2023) Whistle-blower says Facebook 'chooses profits over safety'

[6] The Wall Street Journal (2023) His job was to make Instagram safe for teens. His 14-year-old showed him what the app was really like

[7] The Guardian, Teenage girls, body image and Instagram's 'perfect storm'.

[8] Digital Futures for Children, Children's data and privacy online.

[9] The Washington Post, Your kids' apps are spying on them.

[10] Digital Futures for Children, Children's data and privacy online.

[11] See 5Rights, Disrupted Childhood: The cost of persuasive design and Children & AI Design Code.

knowledge, or resources to understand or challenge automated decision-making, algorithmic unfairness and the subtle, cumulative, or acute nudges shaping their online experience. From recommender systems steering children towards harmful content, to chatbots fostering unhealthy emotional attachment and profiling that deepens discrimination, unchecked AI systems expose children to serious risks.

In response, 5Rights has been working with engineers, experts and academics, to develop the Children & AI Design Code, the first framework of its kind to offer a practical and rigorous a process for identifying, evaluating, and mitigating the known risks of AI pose to children, and to prepare for future unknowns across the AI lifecycle.

Limited approaches

Despite deliberately designing risky digital products and services, tech companies often shift their responsibility onto parents and users, promoting parental controls and 'user agency' features, such as usage statistics, screen time caps, and linked parent accounts.

Marketed as solutions, these measures are mere band-aids that fail to address the systemic nature of the problem. A product engineered through countless hours of development, millions of dollars, and A/B testing designed to drive engagement will always overwhelm any child's efforts to resist its pull. It's an inherently unfair fight — one that undermines a child's rights, well-being, development, and safety.

This delegation of responsibility only exacerbates the problem by shifting accountability from businesses that employ behavioural psychologists for the specific purpose of maximizing engagement to an overwhelmed parent — or even a child, further compounding the risk.

The way forward: Children's Rights in the digital environment

Children have long-established rights and protections under the United Nations Convention on the Rights of the Child (UNCRC)[12] . A life mediated by technology must be held to the same standards as a life beyond the screen. General comment 25 formally sets out how children's rights apply in the digital environment and requires that a child's best interests be a primary consideration.

Our recommendations — rooted in the UNCRC and its General comment 25[13] — urge signatory states, including Canada, to take substantial measures to regulate the digital environment, such as:

- Take proactive measures to prevent exclusion and discrimination, including discrimination that can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child (UNCRC GC 25 Para. 9-11, in ref. to UNCRC Art. 2).
- Ensure that the best interests of every child are a primary consideration in all actions regarding the provision, regulation, design, management, and use of the digital environment. States should ensure transparency in the assessment of the best

[12] United Nations (1989) United Nations Convention on the Rights of the Child

[13] United Nations Committee on the Rights of the Child (2021) General comment No. 25 on children's rights in relation to the digital environment

interests of the child and the criteria that have been applied (UNCRC GC 25 Para. 12-13, in ref. to UNCRC Art. 3).

- Take all appropriate measures to protect children from content, contact, conduct and contract risks, including violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse), and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. (UNCRC GC 25 Para. 14-15, in ref. to UNCRC Art. 6).
- Require digital service providers to offer or make available services to children appropriate for their evolving capacities (UNCRC GC 25 Para. 19-21, in ref. to UNCRC Art. 5).
- Require businesses to undertake child rights due diligence, in particular child rights impact assessments, and hold them accountable for preventing their networks or services from being misused for purposes that threaten children's safety and well-being. (UNCRC GC 25 Para. 36-38, in ref to UNCRC Art. 4).
- Take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses. (UNCRC GC 25 Para. 38, in ref.to UNCRC Art. 4).
- Require that businesses adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services (UNCRC GC 25 Para 39 in ref. to UNCRC Art. 4).
- Prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling (UNCRC GC 25 Para. 42 in ref. to UNCRC Art. 4).
- Ensure that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development. (UNCRC GC 25 Para. 62 in ref. to UNCRC Art. 13-14).
- Take legislative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Such legislation should include strong safeguards, transparency, independent oversight and access to remedy. States should require the integration of privacy-by-design into digital products and services that affect children. (UNCRC GC 25 Para. 70 in ref. to UNCRC Art.16).
- Regulate against known harms. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights. (UNCRC GC 25 Para. 96, in ref. to UNCRC Art. 24).
- Introduce or using data protection, privacy-by-design, safety-by-design and other regulatory measures to ensure that businesses do not target children using techniques designed to prioritize commercial interests over those of the child. Examples of such techniques are opaque or misleading advertising or highly persuasive or gambling-like design features (UNCRC GC 25 Para. 110, in ref. to UNCRC Art. 31).

C-63 5Rights Preliminary Recommendations:

Canada is following the footsteps of several jurisdictions across the world that have already led the way in setting a high bar and systemic protection for children. The EU (Digital Services Act), UK (Age Appropriate Design Code and Online Safety Act), and USA (California Age Appropriate Design Code Act and Maryland Kids Code), all draw on General comment 25 and require upstream comprehensive risk assessment and risk mitigation for services likely to be accessed by under-18s.

Building on these international advances, Bill C-63 recognizes the crucial need to deliver a higher level of protection for children, particularly for their mental and physical health. However, the Bill currently presents some gaps:

- The Bill does not adequately prioritize children's rights, address the broader range of risks to children, or hold companies accountable for the broader impact of their products and services on children.
- The scope of protection for children is very narrow compared to similar international frameworks such as the EU's Digital Services Act and the UK's Online Safety Act. Both go beyond measuring harmful content or social media and also include strong provisions to address systemic risks, the role of design and the commercial incentives emphasising prevention rather than reactive mitigation.
- The Bill's language focused on "incorporating design features" suggests adding a mitigation measure rather than focusing on proactive prevention and safety by design and default.

Some key points to address these gaps:

Overall, the scope of protection of C-63 should be strengthened for children, and the duty of care should be expanded to reflect the full spectrum of risks children face.

The digital environment exposes children to commercial, contact and conduct risks. [14] By extending the scope of this Bill beyond social media and harmful content generated by users, to encompass all services accessed by children, this Bill can achieve its intended objective of promoting safety for children in Canada.

In Summary (d)2), and provision 65: **add a duty to respect children's rights,[15] and best interests[16,17] with reference to the Convention on the Rights of the Child and General comment 25.**

---

[14] Guidelines for industry on Child Online Protection 2020, p. 20 Recognise that the digital world exposes children to content, contract, contact and conduct risks.

[15] Under the United Nations Convention on the Rights of the Child (UNCRC), to which Canada is a State Party, children are rights holders, and General comment No. 25 applies these rights to the digital world.

[16] Article 3 of the United Nations Convention on the Rights of the Child (UNCRC),

General comment No. 25, para 12-13, 69: Ensuring that in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interest of every child is a primary consideration (Para. 12 -13) and that businesses do not prioritize commercial interests over those of the child (General comment No. 25, para 39, 41, 53, 110).

[17] Guidelines for industry on Child Online Protection 2020, p. 55. Recognise the principle of the best interests of the child as a primary consideration in any matters affecting them.

Provision 65: Ensure the duty to protect children and their rights includes a high level of privacy, safety, [18] and security by design and default on the face of the Bill, and to be further developed in regulations.

Design choices play a fundamental role in steering children towards or away from risk. A safety by design approach requires services to embed safety into all stages of their product design process, identifying and mitigating risks before harm occurs.

General comment 25 makes clear that companies should design products and services on a foundation of children's rights, preventing [19] harm from happening in the first place, rather than just addressing it after it has already occurred (as also reflected in the OSA and DSA).

Bill C-63 presents an opportunity to shift the tech industry away from a "move fast and break things" habit to a culture that champions children's rights and safety. By encouraging effective risk assessment and mitigation rather than focusing on limiting and chasing harmful content, this Bill can drive upstream change and transform how online services and products operate.

In provisions 55(1), 56, and 62 (1)a)iii): the scope of protection and risk mitigation should go beyond harmful content and takes account of the full range of risks to children, in particular content, contact, conduct and commercial risks.

Similarly, the risk assessment required through the proposed digital safety plan should not be limited to harmful content, but encompass a broader assessment of risks to children and their rights. Platform should assess and evaluate how their business models, features, algorithms, and functionalities can contribute to or mitigate risks to children. [20,21, 22]

---

[18] The 2021 OECD Recommendation on Children in the Digital Environment calls on States to pay due regard to providing a safe and beneficial digital environment for children through the design, development, deployment and operation of such products and services, including through taking a safety-by-design approach to address risks.

[19] General comment 25 para. 39: Businesses should respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment.

[20] General comment 25 para. 36-38: Requiring businesses to undertake child rights due diligence, in particular child rights impact assessments, and holding them accountable for preventing their networks or services from being misused for purposes that threaten children's safety and well-being.

[21] ITU Guidelines for industry on Child Online Protection 2020, p. 28 Identifying child rights impacts on different age groups as a result of company operations and the design, development and introduction of products and services.

[22] The UK Online Safety Act requires tech companies to carry out children's risk assessments that look at how the design of their services, their business models, functionality, algorithms and other features can contribute to or alleviate the risk of harm to children. The OSA risk assessments must also look at certain functionalities that can impact how a child might use the service. For example, features like 'autoplay' of video or sound content have been found to promote addictive behaviours. Assessments must consider the risk of harm to children in different age groups to ensure the services children use or engage with are age-appropriate.

Likewise, the EU Digital Services Act require Very large online platforms to undertake comprehensive risk assessments annually to measure any negative impact of their service on children's rights or any impact on users' physical and mental well-being. They must specifically examine risks related to the design of online interfaces, algorithms, and automated decision-making that may lead to addictive behaviour. To mitigate any identified risks, very large online platforms must adapt design features, algorithmic design, terms and conditions, recommendation systems, data practices - with the best interests of the child in mind.