Children's Privacy in the Age of Artificial Intelligence

Summary for Policymakers

Artificial intelligence (AI) is playing a growing role in the lives of children, with significant implications for their privacy. Despite these risks, Canadian policy responses to AI and digital privacy protection remain adult-centric, overlooking the specific privacy rights, distinct needs, and unique circumstances of children. Targeted action is needed to address this critical policy gap and develop a child-specific approach to privacy in the age of AI.

The need for a child-specific approach

AI is fundamentally changing the world children live in. More and more, children's everyday spaces and activities – from play, to learning, to health care – are embedded with this technology. While AI has rapidly expanded, policy responses to emerging privacy challenges have focused on adults, overlooking important child-specific considerations:

- **Children have distinct and established privacy rights.** These rights are protected under the *UN Convention on the Rights of the Child* and emerging digital rights frameworks. Privacy also enables other children's rights, including their right to non-discrimination, freedom of expression, and freedom of assembly.
- **Privacy is critical to realizing children's developmental needs**. Privacy enables children to tackle challenges, make mistakes, explore their identities, and comfortably move through other experiences of growing up.
- **Children have less capacity to exercise their privacy than adults.** Children's privacy is often dependent on the proactive effort of others to promote their best interests and consider their evolving capacities.

About the Children's Privacy in the Age of Artificial Intelligence report

This brief is based on a CSA Group research report entitled *Children's Privacy in the Age of Artificial Intelligence* written by Jasmine Irwin, Alannah Dharamshi, and Noah Zon. The report builds on CSA Group's previous work on *Children's Safety and Privacy in the Digital Age* and was developed with generous support from the Office of the Privacy Commissioner of Canada's Contributions Program.

Just as children's privacy rights, needs, and circumstances differ from adults, the privacy risks from AI may have heightened impacts for children's present and future lives:

Data risks: AI requires data to learn and improve, incentivizing the mass collection of data. The sheer magnitude and scope of data collected about children today is unprecedented and poorly regulated. Children's data captured and processed by AI systems may include sensitive information. This data can be shared or sold to third parties and may follow children into adulthood.

Function risks: AI applications often use data in ways that infringe on children's privacy and autonomy. AI functions like surveillance, profiling, decision-making, and inference are already commonly used in children's lives, generally in "low-stakes" applications like targeted online ads. However, AI functions are increasingly being deployed in "high-stakes" applications like university admissions, child protective services, and biometric monitoring.

Oversight risks: AI can produce unfair, incorrect, or discriminatory outcomes for children using their personal information. The "black box" of AI can prevent humans from easily understanding or contesting how these algorithmic decisions are made. A lack of formalized governance or common standards for AI means that those who create, deploy, or profit from AI systems are currently subject to minimal transparency and accountability requirements.

The current policy landscape

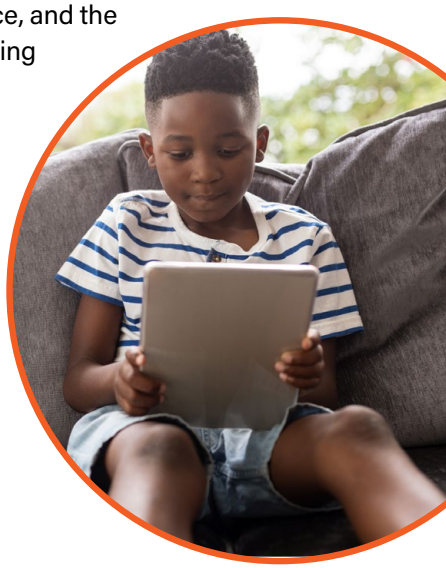
Governments and organizations across the globe are beginning to recognize and take action to address emergent privacy risks associated with AI. However, there has been minimal engagement with children's rights as a distinct issue. There is an opportunity for Canada to demonstrate international leadership on protecting and promoting children's privacy in the development of AI governance.

Canada is currently in the process of modernizing both of its major pieces of privacy legislation:

Legislation for commercial actors: Bill C-11, if passed, would enact the *Consumer Privacy Protection Act* (CPPA), effectively replacing many privacy provisions under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and enact the *Personal Information and Data Protection Tribunal Act.*

Legislation for federal public services: The Department of Justice has launched a consultation and review of the *Privacy Act.*

However, to date, this overhaul of Canada's privacy landscape has not included meaningful attention on children's privacy rights, needs, and perspectives. Bill C-11 mentions minors only once, and the discussion paper on modernizing the *Privacy Act* states that the government is not planning to consider "special rules", including for groups like children. **If unaddressed, this oversight represents a missed opportunity with profound implications for present and future generations of young Canadians.**



Recommendations to promote children's privacy

Action is needed to protect and promote Canadian children's privacy in the age of AI. The following efforts are required for any policy development to be effective:

- **Consider children as a distinct and vulnerable population** with rights, needs, and circumstances that differ from the majority (adults).
- **Involve children in privacy and AI policy development** to realize their right to participate in decisions that affect their lives and gain insights from their lived experiences.

It will also require different types of interventions that target three specific stages of the AI lifecycle: before deployment, during adoption, and after use.

Before deployment

Design and development of AI systems

Ideally, AI design would not just protect but actively promote children's privacy, facilitating the conditions needed for growth and exploration. Decision-makers should:

- **Mandate and operationalize children's privacy by design** to ensure any AI-enabled product or service likely to be accessed by a child is built for their privacy by default.
- **Require children's privacy impact assessments** so that there is early evaluation of potential risks to children's privacy prior to the deployment of AI systems.

During adoption

User privacy and choice

When using AI technologies, children and their caregivers need to be equipped with the right tools to make informed choices about their privacy. Decision-makers should:

- **Develop educational resources for children, teachers, and parents** to increase awareness and comprehension of privacy rights and potential risks of AI.
- **Require child-friendly notices and terms of service (ToS)** so that children can understand how giving or declining consent will impact their privacy.
- **Encourage certification and consumer labelling** of AI technologies that allow consumers to easily identify and differentiate products and services on the basis of data and privacy considerations.
- **Provide dynamic and granular consent options** to give children and their guardians more meaningful privacy choices, including the ability to give partial consent, withdraw consent, and object to automatic decision-making.

After use

Oversight and accountability

Once AI technologies are in use, oversight and accountability interventions are needed to monitor systems, adjudicate contested outcomes, and assign responsibility for violations to children's privacy and associated harms. Decision-makers should:

- **Mandate organizational oversight mechanisms** including human intervention in AI systems and Privacy Officers as identifiable points of oversight and responsibility.
- **Fund independent oversight institutions** with meaningful enforcement powers to investigate violations of children's privacy and bring complaints on their behalf.
- **Introduce strict penalties for privacy violations** that impact children to deter noncompliance and encourage organizations to promote children's privacy.