Children's Privacy in the Age of Artificial Intelligence

Children are living in an AI world

Artificial intelligence (AI) is playing a growing role in children's lives, fundamentally reshaping their everyday experiences. More and more of children's routine activities – from play, to learning, to social connection – are now embedded with AI technologies. Used responsibly, the expansion of AI has the potential to make children's lives better. But AI also poses significant risks for children's privacy.

Right now, Canadian policy responses to AI and digital privacy overlook the specific privacy rights, needs, and circumstances of children. This is a problem because children need privacy for their safety, their development, and their autonomy. Targeted action is needed to address this critical policy gap and develop a child-specific approach to privacy in the age of AI.

What are the risks to children's privacy?

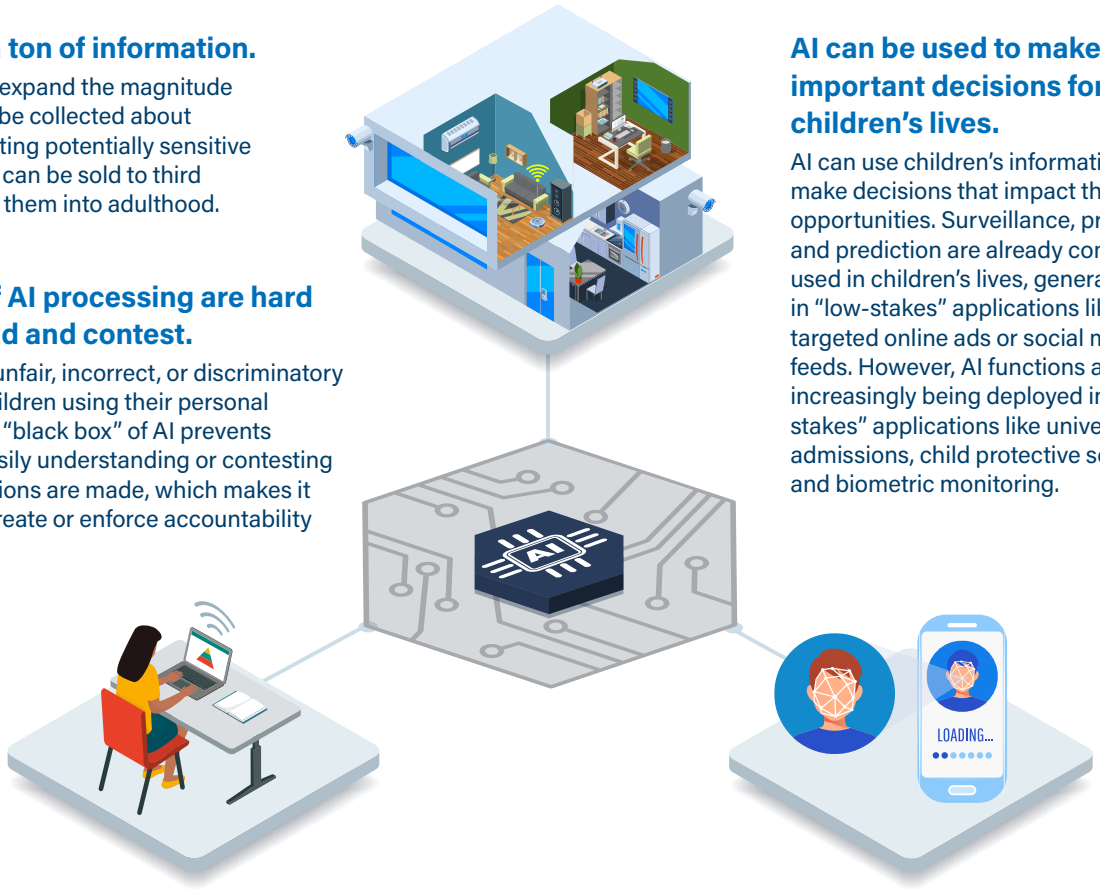
Children's privacy is multifaceted; it includes their ability to move through spaces freely, make mistakes, have age-appropriate independence, and control what information they share. By collecting data on children for algorithmic processing, AI may pose potential risks to all these aspects of children's privacy. This is because:

AI requires a ton of information.

AI technologies expand the magnitude of data that can be collected about children, generating potentially sensitive information that can be sold to third parties or follow them into adulthood.

Outcomes of AI processing are hard to understand and contest.

AI can produce unfair, incorrect, or discriminatory outcomes for children using their personal information. The "black box" of AI prevents humans from easily understanding or contesting how these decisions are made, which makes it challenging to create or enforce accountability mechanisms.

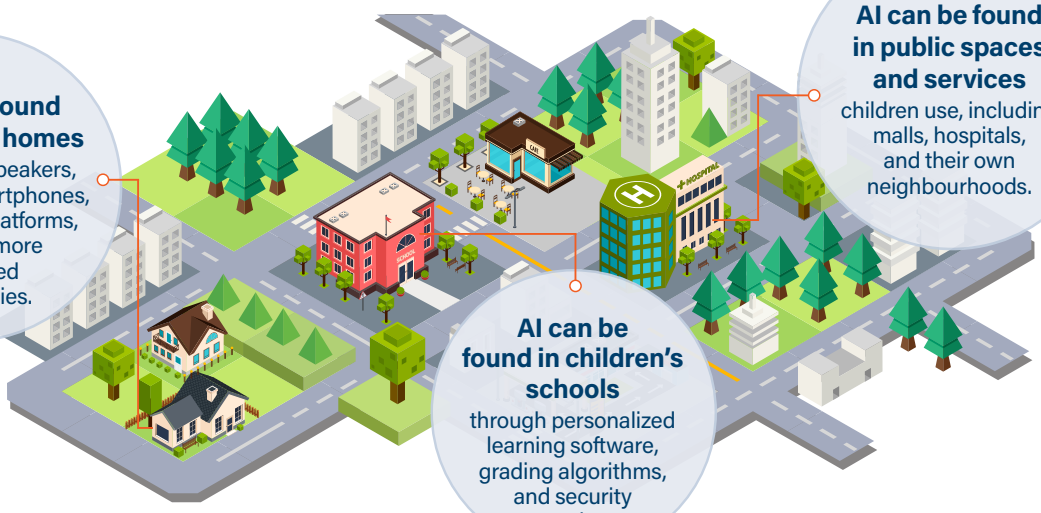


AI can be used to make important decisions for children's lives.

AI can use children's information to make decisions that impact their opportunities. Surveillance, profiling, and prediction are already commonly used in children's lives, generally in "low-stakes" applications like targeted online ads or social media feeds. However, AI functions are increasingly being deployed in "high-stakes" applications like university admissions, child protective services, and biometric monitoring.

What kinds of AI do kids interact with?

AI can be found in children's homes
within smart speakers, smart toys, smartphones, social media platforms, and many more connected technologies.



AI can be found in public spaces and services
children use, including malls, hospitals, and their own neighbourhoods.

AI can be found in children's schools
through personalized learning software, grading algorithms, and security tech.

What action needs to be taken?

Children are navigating this new technological context with little consideration for their best interests from developers and policymakers alike. More action is needed to protect and promote Canadian children's privacy in the age of AI. For policy development to be effective, it will require efforts to **both consider the unique needs of children and to involve children themselves in policy development**. To meet children's needs in an AI world, we need to:

Promote children's privacy in the design of AI.

Ideally, AI design would not just protect but actively promote children's privacy, facilitating the conditions needed for growth and exploration from the very beginning. We need to:

- ☑ **Mandate and operationalize children's privacy by design.**
- ☑ **Require children's privacy impact assessments prior to deployment of AI systems.**

Enhance child and caregiver knowledge 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. We need to:

- ☑ **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 so that children can understand how giving or declining consent will impact their privacy.**
- ☑ **Encourage certification and easy-to-understand consumer labelling of AI technologies.**
- ☑ **Provide more consent options, including the right to object to automatic decision-making and a "right to be forgotten".**

Increase oversight and accountability.

More accountability interventions are needed to monitor AI systems, adjudicate contested outcomes, and assign responsibility for violations to children's privacy. We need to:

- ☑ **Mandate organizational oversight mechanisms, including Privacy Offi ers.**
- ☑ **Fund independent oversight institutions with real enforcement powers.**
- ☑ **Introduce strict penalties for privacy violations that impact children.**

Where can I read more?

This summary 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 support from the Office of the Privacy Commissioner of Canada's Contributions Program.

CSA GROUP™