Policy Horizons Canada   Horizons de politiques Canada

Canada

INSIGHT 9

DATA COLLECTED ABOUT CHILDREN COULD RESHAPE THEIR LIVES IN THE PRESENT AND FUTURE

Jurisdictions are expressing concerns about children's privacy as AI technologies become more ubiquitous. Pervasive data collection in childhood could offer new opportunities for accessibility and education, but also worsen existing vulnerabilities, erode privacy, and reshape adult lives in the future.

TODAY

Young people are a particularly vulnerable group with regard to data privacy.[1] Their sense of self and ability to make decisions are still developing. Healthy child development involves the ability to experiment and make mistakes without severe and lasting consequences. More jurisdictions are exploring how to protect children's data and privacy rights and address challenges around meaningful consent.[2]

Cases are growing of malicious actors using children's data in ways that impact on their mental health and wellbeing. Critics point to how major tech companies capture attention and revenue through addictive user experiences[3] and dark patterns.[4] Dark patterns are a type of web or app design that can be used to influence your decision making when you are using an app or navigating through a website – for example, by intentionally making it difficult to cancel a service.[5] Social media algorithms exacerbate issues related to negative body image.[6] Generative AI has been implicated in the circulation[7] and development[8] of child sexual abuse materials, both real and AI-generated, by adults and children.

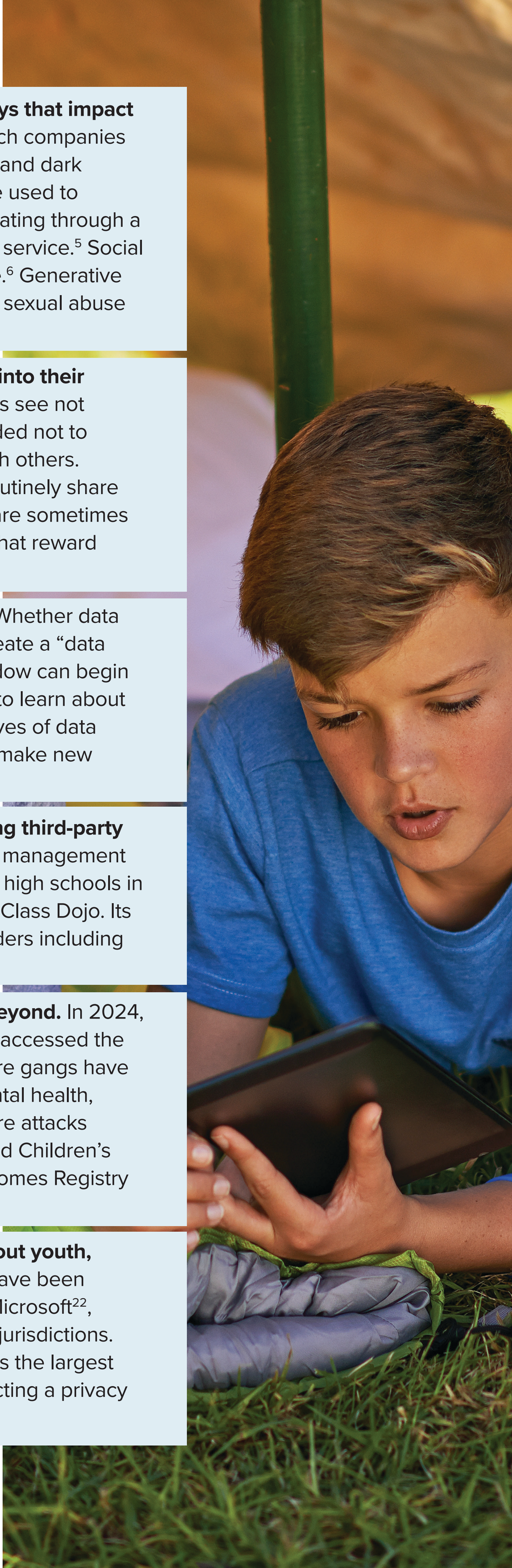
Parents have extraordinary scope to both gain and offer visibility into their children's private lives. For example, keylogger apps can let parents see not only messages a child sent, but also messages they typed but decided not to send.[9] Parents can also share their children's private information with others. Some manage revenue-generating child influencer accounts that routinely share personal information and images of their children. These accounts are sometimes openly followed by pedophiles, who benefit from platform policies that reward engagement.[10]

Unwanted "data" shadows could follow children into adulthood. Whether data is shared by parents or collected by platforms or devices,[11] it may create a "data shadow" that follows children throughout their lives.[12] This data shadow can begin before birth – for example, when parents use DNA testing services to learn about their children's genetic susceptibility to diseases.[13] As these vast troves of data can be stored indefinitely, future AI systems could draw on them to make new inferences about individuals as they grow into adults.

Schools are collecting ever more information about students, using third-party software and AI analysis tools. Since the pandemic, use of student management apps has grown exponentially in daycares, elementary schools, and high schools in Canada. For example, an estimated 70% of elementary schools use Class Dojo. Its privacy policy states it may share data with third-party service providers including Facebook and Google.[14]

Data breaches have affected children and youth in Canada and beyond. In 2024, school photos of 160 students in Alberta were stolen when hackers accessed the cloud storage provider of a school yearbook company.[15] Ransomware gangs have targeted US public schools, releasing sensitive student data on mental health, sexual assaults, and discrimination complaints.[16] In 2023, ransomware attacks affected institutions such as Toronto's Sick Kids Hospital;[17] Family and Children's Services of Lanark, Leeds and Grenville;[18] and Ontario's Better Outcomes Registry & Network, in which 3.4 million health records were breached.[19]

Corporations and NGOs hold a large amount of sensitive data about youth, which can be vulnerable to breach. Private parental control apps have been breached, exposing monitored children's data.[20] In 2023, TikTok[21], Microsoft[22], and Amazon[23] were fined for children's privacy violations in various jurisdictions. As a non-governmental organization, Kids Help Phone – which holds the largest repository of youth mental health data in Canada[24] – reports conducting a privacy impact assessment[25] and aggregating and anonymizing its data.[26]



FUTURES

The opaque sale, circulation, and analysis of children's data will become more common, begin much earlier in life, and be put to unforeseen uses in the future. The number of data-collecting devices children interact with – at home, school, and beyond – will increase (see Insights 7 and Insight 8). Some of these devices could be more vulnerable to breaches of sensitive information.[27]

AI-powered monitoring technologies could become more important, but could also be subverted. Parents could look to AI-powered monitoring technologies to help control their children's online activities and gatekeep increasingly complex informational and media environments.[28] However, young people could also develop increasingly sophisticated means of evading parental control.

Children and youth could inhabit more highly personalized media environments. Entertainment content and advertising could increasingly be generated or curated by personalized AI companions. Sub- and fan cultures could become increasingly personalized and politicized. Feelings of social isolation could become more prevalent, as well as reduced social cohesion. Some young people may become disillusioned with invasive AI-powered technologies and opt to spend more time offline. However, given the pervasiveness of AI this might not be an option in the future.

The market for youth data may become more competitive as concerns around youth data privacy increase. This could lead tech companies to develop more insidious ways to extract and trade youth data. The age cut-off for being seen as a "child" could differ in different contexts. Data could have to be released when a child attains the age of majority.[29] Age verification technologies,[30] like those currently being used in some US states for pornography websites,[31] could be more widely used to protect youth from predatory adults and adult-only spaces.

Despite the many concerns they raise, new AI-enabled technologies could also collect data in ways that support accessibility.[32] They could be used to develop individualized learning tools that help students progress at their own pace. They could also enhance the quality of pediatric health care by assisting in diagnosis, patient monitoring, and precision medicine.[33]

IMPLICATIONS

- Today's children could face **more frequent and devastating data breaches** throughout their lives
- These breaches could result in forms of **identity theft** that lead to financial loss or the release of sensitive personal information
- **Re-identification of anonymized personal data** could become easier as data breaches become more routine and technologies advance – data that seems **private today may not be tomorrow**
- Lax restrictions could lead to data being used to make **AI-mediated inferences** about youth that **affect their relationships and access to jobs, credit, or insurance** in both childhood and adulthood
- **Increased use of parental control technologies** could lead to undue surveillance and **loss of privacy and autonomy for children**
- AI could make it **more challenging for parents to identify problematic or harmful content**, or easier for youth to conceal their engagement with it
- If awareness of issues related to children's data privacy increases, more developers could be required to launch **child-specific apps and platforms that are held to higher privacy standards**[34] or consider issues such as mental health and addiction

Endnotes

[1] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. Children’s Privacy in the Age of Artificial Intelligence. CSA Group, March 2021.

[2] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. Children’s Privacy in the Age of Artificial Intelligence. CSA Group, March 2021.

[3] Murphy, Chris. Opinion | Algorithms Are Making Kids Desperately Unhappy. The New York Times, 18 July 2023, sec. Opinion.

[4] Leiser, M. R. Protecting Children from Dark Patterns and Deceptive Design. SSRN, 11 December 2023.

[5] Office of Consumer Affairs. Dark Patterns. Government of Canada, 19 July 2023.

[6] Hill, Amelia. Social Media Triggers Children to Dislike Their Own Bodies, Says Study. The Guardian, 1 January 2023, sec. Society.

[7] David, Emilia. ‘AI Image Training Dataset Found to Include Child Sexual Abuse Imagery - The Verge. The Verge, 20 December 2023.

[8] Duboust, Oceane. “Society Needs to Be Alert”: Most People Are Unaware AI Is Being Used to Create Child Abuse Content | Euronews. Euronews Next, 19 February 2024.

[9] SecureKin. Keylogger App To Record Your Child’s Keystrokes. Accessed 23 May 2024.

[10] Valentino-DeVries, Jennifer, and Michael H. Keller. A Marketplace of Girl Influencers Managed by Moms and Stalked by Men. The New York Times, 23 February 2024, sec. U.S.

[11] Owen. New AI Toys Spark Privacy Concerns for Kids. GZERO Media, 12 December 2023.

[12] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. Children’s Privacy in the Age of Artificial Intelligence. CSA Group, March 2021.

[13] Bala, Nila. Opinion | Why Are You Publicly Sharing Your Child’s DNA Information? The New York Times, 2 January 2020.

[14] ClassDojo. Third Party Service Providers. Accessed 23 May 2024.

[15] DaSilva, Tomasia. Hackers Steal Children’s School Photos Following a Privacy Breach. Global News, 14 February 2024.

[16] Bajak, Frank, Heather Hollingsworth, and Larry Fenn. Ransomware Criminals Are Dumping Kids’ Private Files Online after School Hacks. Canadian Security Magazine, 5 July 2023.

[17] Omstead, Jordan. SickKids Cyberattack: Ransomware Group LockBit Apologizes Saying “partner” Was behind Attack. CTV News, 3 January 2023.

[18] Lee, Austin. “I Am Deeply Troubled”: Data Breach Impacts Clients at Lanark County Family Services Organization. CTV News, 14 February 2024, sec. Ottawa.

[19] Tsekouras, Phil. Did You Give Birth between 2010 and 2023 in Ontario? Your Personal Health Information Was “likely” Impacted by a Data Breach. CP24, 25 September 2023.

[20] Ali, Suzan, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions. In Proceedings of the 36th Annual Computer Security Applications Conference, 69–83. ACSAC ’20. New York, NY, USA: Association for Computing Machinery, 2020.

21 Woollacott, Emma. TikTok Hit With €345 Million Fine For Failing To Protect Children. Forbes, 18 September 2023.

22 Matza, Max. Microsoft to Pay $20m for Child Privacy Violations. BBC, 6 June 2023.

23 Singer, Natasha. Amazon to Pay $25 Million to Settle Children's Privacy Charges. The New York Times, 31 May 2023, sec. Technology.

24 Kids Help Phone. Kids Help Phone and the Vector Institute Announce Important Partnership for Enhanced Human-Centric Innovations for Youth e-Mental Health Services from Coast to Coast to Coast. Accessed 23 May 2024.

25 Kids Help Phone. Questions about Kids Help Phone Insights, Answered! Accessed 23 May 2024.

26 Kids Help Phone. Kids Help Phone and the Vector Institute Announce Important Partnership for Enhanced Human-Centric Innovations for Youth e-Mental Health Services from Coast to Coast to Coast. Accessed 23 May 2024.

27 Bennett, Drake. How a Massive Hack of Psychotherapy Records Revealed a Nation's Secrets. Bloomberg, 22 April 2024.

28 Wood, Stuart. Exploring the Awareness and Usage of Parental Controls to Support Digital Safety. Internet Matters (blog), July 21, 2023.

29 Beauvais, Michael, and Leslie Regan Shade. How Will Bill C-27 Impact Youth Privacy? Schwartz Reisman Institute (blog), October 8, 2022.

30 McConvey, Joel R. Wizz Dials up Biometrics from Yoti to Prevent Sextortion, Achieve EU Compliance. Biometric Update (blog), February 15, 2024.

31 Mithani, Jasmine. The 19th Explains: Why Some States Are Requiring ID to Watch Porn Online. The 19th, January 29, 2024.

32 Costabel, Milagros. I'm Totally Blind. Artificial Intelligence Is Helping Me Rediscover the World. Slate, 11 October 2023.

33 Shu, Li-Qi, Yi-Kan Sun, Lin-Hua Tan, Qiang Shu, and Anthony C. Chang. Application of Artificial Intelligence in Pediatrics: Past, Present and Future. World Journal of Pediatrics 15, no. 2 (April 1, 2019): 105–8.

34 UNICEF. Children and AI: Opportunities and Risks. Geneva: UNICEF, 2018.

PDF: PH4-219/2025E-PDF
ISBN: 978-0-660-76899-1

Aussi disponible en français sous le titre : Les données collectées sur les enfants pourraient remodeler leur vie au présent et à l'avenir.

DISCLAIMER
Policy Horizons Canada (Policy Horizons) is the Government of Canada's centre of excellence in foresight. Our mandate is to empower the Government of Canada with a future-oriented mindset and outlook to strengthen decision making. The content of this document does not necessarily represent the views of the Government of Canada, or participating departments and agencies.