United Nations High Commissioner’s Call for inputs on the solutions to promote digital education for young people and to ensure their protection from online threats — Canadian perspective

May 3, 2024

Introduction

Diana Rosemberg and Melanie Selvadurai, women with decades of combined experience, have collaborated extensively with global conglomerates to tackle privacy and technology challenges in their roles as management consultants specializing in privacy and data protection. Through this call for inputs, our goal is to leverage our expertise to assist organizations in crafting more compassionate technology solutions.

The COVID-19 pandemic accelerated the integration of technology into our daily lives, facilitating connections and enhancing access to information. Big tech companies utilize our personal data to tailor the content we come across, resulting in an increased visibility of our search preferences. Now is the moment to recognize how our data shapes our perceptions of the world and to purposefully control the information we provide. As a society, it's imperative that we ensure young people are not further marginalized as we transition into the next era of technology. We advocate for incorporating privacy principles to develop solutions that promote digital education for young people and safeguard them from online threats caused from loss of privacy.

The following response specifically addresses the Canadian landscape of digital education on privacy for young people when using social media platforms. We outline the current challenges Canadian youth encounter in accessing digital education related to the harms associated with social media platforms due to inadequate privacy practices. We provide an overview of the steps the Canadian government is taking to address deficiencies in accessing and promoting digital education on privacy. Additionally, we discuss recent Canadian bills aimed at empowering young people to assert their human rights on social media platforms. Finally, we conclude by highlighting the challenges and offering recommendations for young people in safeguarding their privacy and addressing the impact on human rights.

This response covers the queries outlined in the call for submissions:

Question 1

What are the main challenges that young people in your country face in accessing digital education? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

Canadian young people in Canada, particularly those from marginalized and vulnerable backgrounds, face several challenges in accessing digital education. Canadian literature[1] further underscores these challenges, revealing gaps in access to digital technology, affordability issues, and disparities in digital literacy and cybersecurity. Marginalized groups, including Indigenous People, 2SLGBTQ+ individuals, racialized communities, recent immigrants, people with disabilities, seniors, and women, are disproportionately impacted by these challenges. Additionally, online bullying and discrimination are prevalent, with incidents being over twice as prevalent towards minority groups.[2]

These are the key issues that contribute to the challenges that young people face in Canada:

Income disparities: Canadian literature on the topic underscores that household income is the strongest predictor of internet access and speed. Low-income households, including those in rural and remote areas of Canada and Indigenous communities, often lack access to affordable, high-quality internet service due to cost barriers. This digital divide perpetuates socio-economic inequities and limits opportunities for marginalized youth to access digital education resources.[3]

Geographical barriers: Rural and remote areas face unique challenges in terms of internet access and speed due to Canada's size and population dispersion. While efforts have been made to improve broadband infrastructure, disparities persist, with rural and Indigenous communities experiencing lower rates of broadband adoption compared to urban areas. These geographical barriers further exacerbate the digital divide and hinder marginalized young people's ability to access digital education resources.[4]

Device accessibility: Access to internet-enabled devices is another critical factor in digital education access. The high cost of devices, coupled with income disparities, often leaves marginalized youth without adequate access to technology. This lack of access can impede their ability to participate in virtual learning environments and access online educational resources, further widening the education gap.[5]

Digital literacy and education: While internet access is essential, digital literacy skills are also crucial for effectively navigating online spaces and utilizing digital education resources. However, the report highlights disparities in digital literacy education across different regions and jurisdictions in Canada. Inconsistent resources

[1] "Digital equity: focusing on every Canadian's digital future." Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

[2] Shade, L. R., Bailey, J., Burkell, J., Regan, P., & Steeves, V. "Framing the challenges of digital inclusion for young Canadians." In *Citizenship in a Connected Canada: A Policy and Research Agenda.* Eds. Dubois, E. and Martin-Bariteau (Ottawa, ON: University of Ottawa Press, 2020). 57–73. https://www.equalityproject.ca/wp-content/uploads/2023/01/Framing-the-Challenges-of-Digital-Inclusion-for-Young-Canadians.pdf.

[3] "Digital equity: focusing on every Canadian's digital future." Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

[4] "Digital equity: focusing on every Canadian's digital future." Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

[5] "Digital equity: focusing on every Canadian's digital future." Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

and training opportunities for educators contribute to uneven outcomes for students, particularly those from marginalized backgrounds who may already face systemic barriers to education.

Privacy concerns: As digital education becomes increasingly prevalent, privacy concerns also emerge, particularly regarding the collection, usage, and sharing of personal data. The outdated privacy regime in Canada, poses challenges in safeguarding young people's privacy rights in online learning environments. Addressing these privacy concerns is essential to building trust and ensuring the safe and ethical use of digital education platforms for all students.[6]

One of the most significant challenges to accessing digital education in Canada is the establishment of safe online spaces where youth can have their privacy rights respected. The prevailing commercial model of big tech, characterized by online surveillance and exploitation, poses substantial risks to the privacy and well-being of young Canadians. As noted by the scholar Soshana Zuboff,[7] surveillance capitalism treats private human experiences as free raw material for profit, leading to extensive data collection and manipulation practices. This surveillance culture not only poses privacy risks to young individuals, but also erodes their autonomy in digital spaces. Moreover, ensuring that school-based technologies are implemented in a manner that promotes inclusion and respects privacy concerns remains a critical challenge. Tech companies must be held accountable for designing technologies that prioritize youth privacy and participation, as Canadian youth often disregard privacy notices due to their length, complexity, and intentional obscurity.[8] Instances like the Facebook-Cambridge Analytica scandal have heightened awareness of privacy risks but have also underscored the need for clearer and more accessible privacy policies in digital platforms.[9]

Increasing impact of artificial intelligence in digital education: Accessing digital education may involve the use of artificial intelligence technology, including Facial Recognition Technologies (FRTs). Concerns surrounding the use of FRTs in schools include risks and limitations associated with these technologies, especially regarding their accuracy in recognizing children and young people’s faces and the profiling of students. The potential for FRTs to exacerbate racism, normalize surveillance, and institutionalize inaccuracy in schools emphasizes the urgency for regulation of these technologies.[10]

Question 2

What steps is the Government taking to ensure that digital education is accessible and promoted among young people? Please provide examples of specific laws and regulations, measures, policies, and programmes directed at ensuring young people’s universal access to digital education.

The Government of Canada has implemented measures to ensure that digital education is accessible and promoted among young people in Canada. Recognizing the importance of trust in the digital realm, the government has established Canada’s Digital Charter to promote responsible innovation in the digital economy and protection of

---

6 “Digital equity: focusing on every Canadian’s digital future.” Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

7 Zuboff, S. *The Age of Surveillance Capitalism: The Fight for A Human Future at The New Frontier of Power*. (New York: Public Affairs, 2019).

8 Dubois, E. and Martin-Bariteau, F. (eds.), Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa, ON: University of Ottawa Press.https://www.equalityproject.ca/wp-content/uploads/2023/01/Framing-the-Challenges-of-Digital-Inclusion-for-Young-Canadians.pdf

9 “Digital equity: focusing on every Canadian’s digital future.” Deloitte, 2002. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/fcc/digital-equity-2/ca-catalyst-digital-equity2-aoda-en.pdf?icid=de2-report-en.

10 ‘Facial Recognition & Canadian Youth’ (2021), Center for Media, Technology and Democracy. https://www.mediatechdemocracy.com/all-work/facial-recognition-and-canadian-youth

privacy. In addition, specific laws, regulations, measures, policies, and programs have been established to address this goal:

Freedom Online Coalition (FOC):[11] Canada, as a founding member of the FOC, collaborates with 32 other countries to promote internet freedom and uphold human rights online. The Tallinn Agenda, adopted unanimously in 2014 by FOC members, emphasizes the importance of non-discriminatory access to the internet for exercising freedom of information. Members are committed to supporting digital literacy to empower internet users, especially those in vulnerable positions, to make informed decisions, access information and economic opportunities and safeguard their human rights and freedoms.

Broadband accessibility:[12] The government has made efforts to expand broadband infrastructure to rural and remote areas through initiatives like the Universal Broadband Fund. The $3.225 billion Universal Broadband Fund aims to ensure that all Canadians have access to high-speed internet, thereby promoting digital education accessibility, benefiting Indigenous and rural and remote communities. Some provinces and municipalities like Toronto, Ontario provide Wi-Fi hotspot lending programs, Wi-Fi hotspots with unlimited data for six months to 1,000 households and launched a new Internet Connectivity Kits initiative to give a laptop and a Wi-Fi hotspot with two years of unlimited data to those with most the urgent need.

Digital literacy programs:[13] The government has implemented digital literacy programs and initiatives to equip young people with the skills needed to navigate digital environments effectively, and to educate young people about online safety and security. These programs provide resources and training to help young Canadians navigate the digital world safely, recognize online threats, and protect their personal information.

Education policies:[14] Canada's K-12 school systems have increasingly created policies to embrace digital learning, including the adoption of Google Apps for Education (GAFE) across the country. With education responsibilities decentralized to provincial and territorial authorities, the advancement of digital skills and technologies in K-12 education varies widely and remains inconsistent.

Digital inclusion programs and public-private partnerships: Various government programs and initiatives promote digital inclusion among marginalized communities, including young people. Government initiatives like CanCode 3.0**[15]** distribute funds to private sector initiatives to address barriers to digital access, such as affordability and skill gaps. An example is Actua's Digital Skills for Underrepresented Youth and Teachers Across Canada; the project provides inclusive, equitable access to digital literacy opportunities to underrepresented youth including girls, Indigenous youth, Black youth, youth with disabilities and youth residing in rural, remote and northern communities.

---

[11] "Human rights and inclusion in online and digital contexts." Government of Canada, October 20, 2022. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/internet_freedom-liberte_internet.aspx?lang=eng.

[12] "High-speed Internet for all Canadians." Government of Canada, March 15, 2024. https://ised-isde.canada.ca/site/high-speed-internet-canada/en.

[13] "Programs and initiatives innovation." Science and Economic Development Canada. Government of Canada, April 19, 2024. https://ised-isde.canada.ca/site/ised/en/programs-and-initiatives.

[14] Bennett, P. W. "Digital Learning in Canadian K-12 Schools: A Review of Critical Issues, Policy, and Practice." In *Handbook on Digital Learning for K-12 Schools.* Eds. A. Marcus-Quinn & T. Hourigan. (Springer, 2016). 293–315. https://www.researchgate.net/publication/310952338_Digital_Learning_in_Canadian_K-12_Schools_A_Review_of_Critical_Issues_Policy_and_Practice.

[15] "CanCode 3.0 Project Descriptions." Government of Canada, June 2023. https://ised-isde.canada.ca/site/cancode/en/funded-cancode-initiatives.

Overall, these measures demonstrate the government's commitment to ensuring that digital education is accessible and promoted among young people through a combination of policy, engagement in coalition for digital inclusion and programmatic interventions.

Question 3

What steps is the Government taking to ensure that young people can realize their human rights online in a safe, empowering, and inclusive way?

Bill C-63, the Online Harms Act (February 26, 2024)[16]

On February 26, 2024, the Government of Canada introduced legislation aimed at combating harmful content online, particularly addressing the sexual exploitation of children. Known as Bill C-63, or the Online Harms Act, this legislation aims to establish stronger online protections for children and enhance the safety of all individuals in Canada by addressing online hate and other forms of harmful content. The Bill proposes a new framework for fostering safer and more inclusive online participation. It seeks to hold online platforms, including social media services, accountable for their design decisions that contribute to the dissemination and amplification of harmful content on their platforms. Furthermore, it ensures that platforms implement mitigation strategies to reduce users' exposure to such content. Recognizing the significant risks associated with the digital world, including the potential for sexual exploitation of children, promotion of self-harm, incitement of violence, endangerment of safety and propagation of hate, the legislation underscores the real-world impact of online harms, which can have tragic, and even fatal, consequences.

Bill-63 introduces a "duty to protect children", which would compel social media services to incorporate into any regulated service they operate specific design features aimed at safeguarding children. These features, such as age-appropriate design, would be mandated by regulations. These requirements would be detailed in regulations respecting child protection design features, such as account options for children, parental controls, privacy settings for children and other age-appropriate design features. Under this legislation, platforms would be mandated to minimize exposure to explicitly defined categories of harmful content and to be forthcoming and transparent regarding the measures they are implementing to achieve this goal. They would also be obligated to promptly remove content that sexually victimizes a child and re-victimizes a survivor, as well as intimate content shared without consent. Platforms would be required to be transparent with Canadians about their efforts to safeguard users, particularly children and survivors. Every user should have the freedom to express themselves without fear of harm and to have access to convenient methods for flagging harmful content in order to better curate their online experience.

The Online Harms Act proposes the establishment of a new Digital Safety Ombudsperson of Canada. This individual would serve as a primary contact and a support resource for users and victims, advocating for their needs and interests regarding online safety issues. Appointed for a five-year term, the Ombudsperson's responsibilities would include:

- continuously gathering information from users and issuing calls for written submissions to gather perspectives on specific matters.
- conducting consultations with users and victims.
- directing users to appropriate resources, such as law enforcement or support hotlines; and

[16] "Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children." Government of Canada, February 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html.

- providing guidance, publishing public reports, and advocating to the Commission, the government and online platforms to address frequent, severe, or systemic issues from a user perspective.

Resolution on Best Interests of Young People (October 5, 2023)[17]

The Office of the Privacy Commissioner of Canada recommends that both public and private sector organizations adopt privacy practices that align with principles that should also guide legislative reforms. Highlighted privacy practices to address online harm include:

Prioritize the privacy and best interests of young people through proactive design

To effectively mitigate digital privacy risks for young individuals, organizations should identify and address potential concerns at the earliest stages of development. It is crucial that privacy considerations and the welfare of young people are integrated into the product or service right from the initial design phase.

Organizations should:

- conduct privacy impact assessments (PIAs) for projects involving the data of young individuals or to assess potential impacts on them specifically.
- customize their standard PIA process to comprehensively consider the perspectives and experiences of young people, both as individuals and as a collective, prior to the collection, utilization, or disclosure of their information.
- actively engage young individuals, their parents or guardians, educators, or child advocates in this assessment process; and
- perform an intersectional analysis to address the unique privacy risks faced by vulnerable groups of young people, such as those with disabilities, First Nations, or individuals within the 2SLGBTQI+ community.

Be transparent

Transparency is crucial for informed decision-making and obtaining consent.

Organizations should:

- provide privacy information to young individuals (and their parents or guardians when necessary) in a succinct, prominent, and easily understandable format tailored to the young person's level of maturity.
- inform young individuals about who to reach out to if they have any questions regarding the provided information; and
- be transparent about the privacy risks associated with the usage of their product or service. This may encompass details regarding their specific measures to safeguard young individuals from such risks, such as content moderation efforts or potential harms.

Allow for deletion or deindexing and limiting retention

Young individuals often have limited understanding of how companies collect, utilize, and disclose their personal information. Moreover, they are prone to making decisions in the present that could have adverse consequences in the future, often persisting for extended periods.

[17] "Putting best interests of young people at the forefront of privacy and access to personal information." Office of the Privacy Commissioner of Canada, October 2023. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/.

Organizations should, and in certain instances, are obligated to:

- provide young individuals with the ability to rectify errors in their personal information or to retract information they previously shared but now regret; and
- implement a data retention policy that prioritizes the well-being of young individuals, ensuring that personal information is retained only for the duration necessary to deliver a product or service. This approach reduces the likelihood of breaches and minimizes the potential for information to be reused beyond its original intent.

Question 4

What are the main gaps and challenges to young people's protection from online threats in law, policy, and practice in your country and the impacts on young people's human rights? Please consider the specific situation of marginalized young people and those in vulnerable situations in your response.

The below gaps and challenges exist for Canadian young people's protection as it impacts people's human rights.

Implement an age-appropriate design code[18]

The most effective approach to safeguarding children's online interactions is integrating privacy and safety principles into product and service designs from the beginning. Establishing standards and guidance for children's online safety and privacy can offer a cohesive set of principles to assist companies in evaluating their services in order to guarantee a secure environment for children. Moreover, these standards can serve as a foundation for regulatory assessment and labeling, aiding parents and young individuals in assessing whether a product or service aligns with these principles without needing to scrutinize every setting individually.

Utilize age-appropriate categories when establishing standards and regulations for online activities[19]

When it comes to ensuring children's safety and privacy online, the Internet often operates within strict age distinctions: whether users are above or below 13, or above or below 18. While this mirrors the simplistic binary understanding of childhood and adulthood in legal frameworks, it overlooks more nuanced approaches used to promote age-appropriate development and safety in policy and standards. Standards crafted to support and safeguard children typically employ "fenced" or categorized approaches based on age or developmental stage. For instance, safety guidelines for sports and playgrounds or content ratings for television, movies and video games are tailored to specific age groups, considering typical physical and psychosocial developmental milestones. While recognizing that every child is unique, these benchmarks provide a useful reference point for parents and children to make informed decisions. While few online standards currently incorporate this level of granularity, and implementing such measures may pose enforcement challenges, there remains considerable merit in devising tools and standards for children's online safety and privacy that align with developmental stages.

[18] "Children's Safety and Privacy in the Digital Age." CSA Group, May 2020. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Childrens-Safety-and-Privacy-in-the-Digital-Age.pdf.

[19] "Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children." Government of Canada, February 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html.

Engage children in crafting solutions[20]

Incorporating the perspectives of young individuals in both design and policymaking endeavors not only anchors initiatives in children's digital rights but also ensures that solutions resonate with the realities faced by children. Several governments have implemented consultations and co-development programs to solicit input from youth.

Mechanisms for accountability[21]

Robust policies and standards are impactful only when supported by effective and accessible enforcement mechanisms. The enforcement of online safety measures, whether conducted by a public authority or a platform enforcing its Terms of Service agreements, heavily relies on users lodging complaints. However, the processes for submitting complaints are frequently complex and may lack user trust, particularly if users doubt that the platform or regulatory body will take action. These obstacles are especially formidable for children, and even more so for those experiencing online harm.

Question 5

What steps is the Government taking to ensure that young people are protected from online threats? Please provide examples of specific laws and regulations, measures, policies, and programmes.

The Canadian government is implementing multiple measures to safeguard young individuals from online dangers.

Canada's Digital Charter:[22] The Digital Charter initiative outlines principles to ensure that privacy is protected and that organizations act responsibly in the digital space. By promoting transparency, control and consent over personal data, the Digital Charter aims to safeguard young people's privacy and mitigate online threats such as data breaches and unauthorized use of personal information.

Digital Charter Implementation Act, 2022:[23] This draft legislation modernizes the framework for the protection of personal information in the private sector and introduces new rules for the development and deployment of artificial intelligence (AI). It includes provisions to increase control and transparency over personal information and ensure that consent is obtained for data use, which contributes to protecting young people's privacy online. If passed, it will impose significant fines for privacy violations, and serve as a deterrent against irresponsible data practices that could harm young Canadians' privacy.

Bill C-63, Online Harms Act (mentioned above in Question 3)

Bill C-13, the Protecting Canadians from Online Crime Act: Canada ranked 21st out 29 industrialized nations in the incidence of bullying according to UNICEF's report card on child well-being.[24] In response, the Canadian

---

[20] "Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children." Government of Canada, February 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html.

[21] "Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children." Government of Canada, February 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html.

[22] "Canada's Digital Charter." Government of Canada, March 2023. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world.

[23] "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Bill C-27)." Parliament of Canada, June 16, 2022. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

[24] "Child well-being in rich countries: A comparative overview." UNICEF. https://www.unicef.ca/en/child-well-being-rich-countries-comparative-overview.

government introduced Bill C-13 to address cyberbullying, which came into effect on March 10, 2015.[25] The Act includes amendments to Canada's Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act to criminalize online behaviours such as online bullying and "sexting."

Digital Literacy Exchange:[26] The Digital Literacy Exchange program provides resources and training to educators and community organizations to enhance digital literacy among youth and to develop knowledge required to use the Internet safely, securely and effectively. "Safe" means how to avoid online risks like cyberbullying, scams, and phishing. "Secure" focuses on keeping personal information protected through measures like strong passwords. "Effective" involves using online resources and tools to learn, communicate, and collaborate. Launched in 2018, and in its first phase, it supported training of more than 400,000 participants from under-represented groups

Please provide any relevant statistical or disaggregated data based on age, gender, disability, ethnicity, religion, sexual orientation and gender identity, migration status, or other categories.

Online hate and aggression among young people in Canada:[27]

- More than 7 in 10 young people have been exposed to online hate and violence.
- Seeing online hate was more common among young Canadians with a disability. Young people aged 15 to 24 with a disability (29%) were over 2.5 times as likely as young people without a disability (11%) to have seen content on a daily basis that may incite hate. There were, however, no differences in the overall volume of exposure to online hate by gender or racialized groups among young people aged 15 to 24, though the same content can have a different impact on different viewers.
- Based on data from the UCR Survey, the overall number of cyber-related hate crimes, directed at any age group, has increased from 2018 to 2022, from 92 reported incidents in 2018 to 219 incidents in 2022. Of the cyber-related hate crimes that took place from 2018 to 2022, 82% were violent and 18% were non-violent.
- Uttering threats (36%) was the most common type of cyber-related violent incident from 2018 to 2022, followed by indecent or harassing communications (29%).
- Among non-violent cyber-related hate crimes, public incitement of hatred (52%) accounted for more than half of the incidents.
- From 2018 to 2022, cyber-related hate crimes targeting Black people and those motivated by a person's sexual orientation were the most common types of cyber-related hate crimes reported to police, representing 17% each. These were followed by hate crimes targeting the Jewish population (12%).
- Nearly one-quarter of victims of cyber-related hate crimes are youth aged 12 to 17.
- Teenage boys aged 12 to 17 are six times more likely than teenage girls to be charged with or accused of a cyber-related hate crime.
- Young women are most often the victims of online harassment.

Cyber victimization and mental health:[28] Experienced by one in four Canadian youth, cybervictimization is associated with multiple indicators of mental ill health, including suicidal ideation and attempt. While certain

[25] "Protecting Canadians from Online Crime Act." Government of Canada, April 25, 2024. https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/page-1.html.

[26] "Digital Literacy Exchange Program." Government of Canada, June 7, 2023. https://ised-isde.canada.ca/site/digital-literacy-exchange-program/en.

[27] "Online hate and aggression among young people in Canada." Statistics Canada, February 27, 2024. https://www150.statcan.gc.ca/n1/daily-quotidien/240227/dq240227b-eng.htm.

[28] Kingsbury, M., & Arim, R. "Cybervictimization and mental health among Canadian youth." *Health Reports* 34, no. 9. (September 20, 2023): 3–13. doi: 10.25318/82-003-x202300900001-eng. https://pubmed.ncbi.nlm.nih.gov/37729061/.

population groups (transgender and non-binary youth, females attracted to the same gender, and those living with chronic conditions) appear to be at a higher risk of experiencing cybervictimization, results suggest that cyber victimization is associated with similar mental health indicators for all adolescents.

Submission prepared by

Melanie Selvadurai
Management Consultant in Data Protection and Privacy
Toronto Canada

Diana Rosemberg
Management Consultant in Data Protection and Privacy
Toronto Canada