Ensuring the Best Interests of Children in Canada's Response to Online Harms

UNICEF Canada Policy Brief: Bill C-63

August 2024

unicef CANADA | for every child

Introduction

As the Government of Canada stated upon tabling Bill C-63 (*Online Harms Act*) on 26 February 2024, "the digital world can pose significant risks. Social media can be used to sexually exploit children, promote self-harm to children, incite violence, put people's safety at risk and foment hate. Online harms have real world impact with tragic, even fatal, consequences." Children and youth have also expressed the need for online spaces where they are safe and freer to engage.

With a goal to cultivate a safer online environment, Bill C-63 acknowledges governments' obligations to safeguard children. It proposes legislative and regulatory measures targeting certain online harms, supported by accountability mechanisms. In so doing, the Bill also addresses the private sector's responsibility to uphold children's rights. UNICEF Canada applauds initiatives outlined in Bill C-63 aimed at reducing children's exposure to significant online harms and enhancing responses to instances of harm. The focus of UNICEF Canada's brief is the potential impacts of the proposed legislation on children (under age 18) and their human rights, and we recommend measures that would optimize positive impacts and avoid or mitigate negative and inequitable impacts. We hope this encourages further deliberation and prioritization of the best interests of the child and consideration of the full expression of their human rights online.

Situation Analysis

The current generation of children in Canada was born at the time of the smartphone and has grown up with access to the Internet. This lifelong "digital immersion" compared to older generations affects the prevalence and nature of their online engagement. For instance, in 2023, young people aged 15 to 24 were more likely to get their news and information from social media (62%) than older Canadians (18%).[1] By the time a child turns 18, tens of thousands of data points will have been collected about them.[2] While for some children this will not lead to harm, for others these are examples of gateways to online harm. Children are exposed to conduct, contact, content and contract risks online. Social media and other forms of Internet use can place younger people at a higher risk of exposure to harmful online content and can facilitate the manipulation of young people to perpetrate online harms including sexual exploitation; self-harm; bullying; cyber-related hate speech; mis/disinformation; commercial exploitation and privacy violation.

Bill C-63 focuses most of its provisions on two types of online harm: online sexual exploitation and exposure to hate speech, with specific attention provided to children. Children are among the most likely to experience or to be exposed to these harms, but young people are also a considerable source of harms against their peers. While reports of such harms are increasing, most online harms to children are unreported and most of the reported incidents do not result in convictions after harm is done. Given this situation, a child rights-based focus on preventing harm is called for along with punishing or remediating harm done.

Children's Rights Online

[1]Government of Canada, Statistics Canada. (2024, February 27). *The Daily — Online hate and aggression among young people in Canada*. https://www150.statcan.gc.ca/n1/daily-quotidien/240227/dq240227b-eng.htm
[2] UNICEF, The Case for Better Governance of Children's Data: A Manifesto.

As children increasingly engage with online content in diverse ways, with diverse impacts on their rights and well-being, there is a role for legislation to equitably prioritize and protect their human rights. The foundation of child-centred governance should be in established international human rights laws and institutions. Having ratified the Convention on the Rights of the Child and the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, the Government of Canada has the duty to respect, protect and fulfil these rights for every child, without discrimination, and ensure that other actors including digital content platforms and providers ("online services") undertake their responsibility and the duty of care to uphold children's rights.

Article 3.1 of the Convention, elaborated in United Nations Committee on the Rights of the Child General Comment No. 16 on the best interests of the child, provides that all decisions made by governments; private actors including business enterprises in the digital environment; and public and private welfare organizations should consider children's best interests. Achieving children's best interests requires recognizing their evolving capacities and fulfilling of all their rights to the greatest possible extent. States also have duties regarding the impact of business activities and operations on children's rights. The United Nations Guiding Principles on Business and Human Rights (2011) and the Children's Rights and Business Principles (2012) call on businesses to "meet their responsibility to respect children's rights".

States and the private sector are also given more specific guidance in relation to children's rights online by the UN Committee on the Rights of the Child General Comment No. 25 (2021) on children's rights in relation to the digital environment. This guidance underscores the role of digital technologies in enabling children to fully exercise their civil, political, cultural, economic and social rights outlined in the Convention on the Rights of the Child. These rights encompass access to diverse information sources; freedom of expression, association, and assembly; privacy; leisure; play; participation; education; and protection from violence and exploitation in the use of digital technologies. While it is readily apparent that children's exposure to the types of online content subject to Bill C-63 is or can be harmful, it is not always recognized that their rights can be subverted online in many other ways:

- Children have the right to **freedom of thought** and relatedly **freedom of expression**, which includes the freedom to seek, receive and impart information and ideas of all kinds; freedom to express themselves; and freedom from manipulation, mis/disinformation and privacy violation. These rights are undermined by persuasive technologies for behavioural modulation and manipulation including non-transparent nudge techniques, algorithms, surveillance, marketing and misinformation.

- Children have **participation and protection** rights to express themselves, choose how they are represented online and explore and experiment safely with ideas and identities as they develop -- without being subjected to surveillance, privacy violation, harmful content or disproportionate legal and other penalties.

- Children have the right to **privacy and identity** in the digital environment, which includes the protection of their personal data. Without the ability to think, write and communicate in private, children will choose to self-censor rather than experiment with ideas that bring the risk of social, legal or physical consequences. Children have the right to privacy from governments, private companies, civil society actors, and to some extent, from their own parents.

The violation of children's rights online can contribute to children's self-harm, impair their development and increase the risk that some children will come into contact with the justice system and face serious and lifelong consequences for online activity. The repercussions of online harms extend beyond the digital realm, sometimes resulting in tragic outcomes including loss of life.

The Committee on the Rights of the Child has affirmed that States should regularly review, update and enforce robust legislative frameworks 'to protect children from recognised and emerging risks of all forms of violence in the digital environment'.[3] Legislative measures for safeguarding children online should encompass procedures for electronic evidence investigation and preservation; regulation of digital businesses; independent monitoring of children's rights protection; access to redress for affected children; and online provision of child protection services for victims.[4] Bill C-63 addresses these measures to varying extents. In so doing, it attempts a difficult balancing act between children's rights to freedom of expression and their rights to protection. But it must further consider the full scope of children's rights, including their evolving capacities and the different situations of diverse children, to achieve an overall understanding of their "best interests".

UNICEF Canada recommends amendments to optimize the positive impacts of Bill C-63 on children and mitigate potential negative and inequitable impacts.

Prioritizing and Protecting Children from Online Harms in Legislation

72% of UNICEF Canada U-Reporters said there should be stricter regulations for online services to ensure the safety of users, especially young people.[5]

Aims of Legislation

Bill C-63 defines a child as "a person under 18 years of age", which is in accordance with the Convention on the Rights of the Child. The Bill states that a primary objective is children's protection and safety, particularly concerning their physical and mental well-being. Online services will be required to have a "duty to protect children" and, relatedly, a "duty to act responsibly" and a "duty to make certain content inaccessible".

The Bill's objectives should also explicitly recognize relevant, internationally agreed standards and principles including upholding the Convention on the Rights of the Child and the principle of the best interests of the child. Determining and prioritizing children's best interests is a legal and administrative duty enshrined in international and domestic law. This principle requires comprehensively considering children's interconnected rights outlined in the Convention on the Rights of the Child. These rights include not *only* mental and physical health and safety but also protection from exploitation and

[3] CRC General Comment No. 25 (2021), para. 82.
[4] Legislating for the digital age. (2022, May 1). UNICEF. https://www.unicef.org/reports/legislating-digital-age

[5] https://canada-en.ureport.in/opinion/6971/

privacy violation; access to information; participation; play and leisure; non-discrimination; and access to justice, tailored to children's evolving capacity. Children's best interests need to have greater strength and validity among other legal bases for regulating online activities, pursuant to article 3 of the Convention on the Rights of the Child.

To assist in realizing the best interests of children, the UN Guiding Principles on Business and Human Rights affirm that all businesses have a responsibility to identify, prevent, mitigate and, where appropriate, remediate their potential or actual negative impacts on human rights. To this end they should conduct human rights due diligence (HRDD), including impact assessments. Globally, a growing number of laws and regulations make aspects of HRDD mandatory for the technology sector. The Children's Rights and Business Principles provide explicit guidance on what it means for business to respect and support children's rights. Companies can assess how well they are meeting their responsibilities to children in particular by carrying out Child Rights Impact Assessment (CRIA). General Comment No. 25 also calls on States to promote the use of CRIA by businesses relating to the digital environment. CRIA are an important element of a company's overall human rights due diligence to understand systemic risks to children relating to the company's operations.

Bill C-63 should expressly require the application of CRIA to the safety assessments and plans that online services would be required to implement. This child rights due diligence is more comprehensive than a focus on safety and risk. It should enable online services to identify, prevent and mitigate potential impacts on children's rights; extend this consideration across their business relationships; and engage in "meaningful consultation with potentially affected groups", according to the Guiding Principles on Business and Human Rights.

While Bill C-63 is essentially an effort to compel online service providers to undertake due diligence for children, it is likewise appropriate that the Government of Canada employ its own process of due regard for children and apply a fulsome CRIA of the Bill. The Department of Justice has a CRIA process (as of July 2023) to ensure proposed legislation considers the full scope of children's interdependent rights to determine to what extent it may achieve their best interests; to avoid or mitigate potential negative impacts; to optimize positive impacts; and to ensure equitable impacts.

UNICEF Canada recommends that:

- **The best interests of children is stated as an explicit principle and purpose of Bill C-63, recognizing the goal to protect, respect and fulfil the full spectrum of children's rights, beyond physical and mental health, that are affected by online harms and by the proposed legislation.**
- **The results of the Child Rights Impact Assessment of Bill C-63 are provided to Parliamentarians.**
- **Child Rights Impact Assessment is applied to any regulations developed pursuant to Bill C-63, and this assessment includes children's views of the potential efficacy and impacts of the proposed measures.**
- **The duty to protect children established in s. 65 includes "respecting the human rights of children in the Convention on the Rights of the Child".**

- **The terminology in the Bill related to the sexual exploitation and abuse of children consider the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse (the Luxembourg Guidelines).**

Types of Harmful Content

The Bill focuses on seven categories of harmful content: three that directly address child-specific forms of harm and four that involve children as well as other populations:

1. Content that **sexually victimizes** a child or re-victimizes a survivor;
2. Content used to **bully** a child;
3. Content that induces a child to **harm themselves;**
4. Content that incites violent extremism or terrorism;
5. Content that incites violence;
6. Content that foments hatred; and
7. Intimate content communicated without consent, including deepfakes.

Most of the Bill's requirements focus on the first category of harmful content: the *sexual victimization of children* ("content that sexualizes children or victims of sexual violence and sexual content shared without consent"). A secondary focus is *content that promotes hate speech.* The Bill also gives regard to other specific types of online content particularly harmful to children including content that is used to cyberbully and to encourage self-harm in certain ways.

Categories of harm that are not a focus of the Bill but are implicated in the harm to children it seeks to mitigate include:

- **Privacy violation** including surveillance of children, data collection, confidentiality breaches and personal information/identity theft; and

- **Commercial exploitation** of children through data collection and marketing of/exposure to harmful products such as alcohol, drugs, tobacco and nicotine products, gambling and other unhealthy and age-inappropriate products and content.

Hate speech or "content that foments hatred*"* is an increasingly difficult area to regulate, based on experiences across jurisdictions. The proposed changes to the *Criminal Code, Youth Criminal Justice Act* and *CHRA* have the stated intent to combat hate speech and hate crimes; provide improved remedies for victims; and hold individuals accountable for the hatred they spread. Amendments to the *Criminal Code* and by extension the *YCJA* would address hate-motivated conduct as a distinct crime rather than an aggravating factor and increase penalties for spreading hate online. Changes to the *CHRA* would mean that posting hate speech online constitutes discrimination and introduce a new process for handling hate speech complaints. The proposed changes empower the Canadian Human Rights Tribunal to adjudicate disputes and order the removal of hate speech; compensate victims up to $20,000; and protect the confidentiality of complainants, victims and witnesses to prevent reprisals while maintaining openness in proceedings.

Considering these particular types of online harms, it is important to recognize that children and youth are not only victimized as targets of sexual abuse, bullying or hatred, but also that they can be more

easily influenced and manipulated to perpetrate harms due to their developmental stage and the nature of the online environment. Childhood, the period from birth to 18 years of age, is a time when attitudes, preferences and identity are fluid and under formation. Children's developing capacities, including cognitive capacities such as the ability to discern true from false information, predispose them to engage with others; explore different belief systems; discover and experiment with identity; and take risks. This can make children more vulnerable both to exploitation and to engaging in behaviours that are not well-understood for their potential harms and consequences.

Contrary to popular tropes, some studies have concluded that young people are no more "savvy" than older people at determining what online content is factual and what is false. Children can be more likely to believe disinformation and misinformation and to be manipulated to spread it. This can occur not only on social media platforms but also in online games and other seemingly benign content platforms. Content that manipulates children and promotes their engagement in harms is relentlessly served to them through popular influencers, algorithms, bots and troll factories, and even from trusted sources including relatives and friends. Children's data can be used to manipulate and influence their behaviour through microtargeting of content to shape their beliefs. Many digital services have developed comprehensive profiles on children including their online actions, interests and behaviours. This allows for the development of algorithms that predict the types of content that will keep children engaged in scrolling, clicking, watching and sharing digital content.

The same kinds of sophisticated behavioural science and data analytics that companies use to push children to consume products and media are sometimes used to influence behaviours and beliefs that come under the scope of Bill C-63. Mis/disinformation, malinformation, propaganda and even hate can be disguised as humour, novelty or scholarly fact, packaged as compelling clickbait that captures attention. This content appears alongside editorial material that individuals trust, blurring the lines of what is true and what is not and between what is funny and edgy and what is harmful and dangerous. Opaque algorithms and non-transparent nudge techniques immerse children in an echo chamber affecting their abilities to make independent choices and to access high quality, credible information. These techniques may also be used by groups with harmful goals such as pushing youth towards joining extremist organizations or spreading conspiracy theories and disinformation. By manipulating amplification metrics on social media platforms these groups ensure that their content gains traction.

Children are highly susceptible to these techniques. Their rights to privacy, protection of their identity, information and freedom of expression are violated, and this in turn facilitates the kinds of harms that Bill C-63 aims to mitigate: a compounding of harms due to failures in governance and corporate responsibility online. The Committee on the Rights of the Child recognized that the digital environment "may open up new ways to perpetrate violence against children, by facilitating situations in which children experience violence and/or may be influenced to do harm to themselves or others."[6][7] In fact, the delineation of children as victims and perpetrators can be blurred, since some children who are targets for online harms are also involved in perpetuating harms. Bill C-63 proposes measures that could protect children from abuse, violence and exploitation, and these measures may further reduce children's risk of involvement in perpetuating online harms. However, the increased criminal and financial penalties proposed in Bill C-63 might criminalize more children for engaging in harmful online behaviour; particularly boys. While Bill C-63 places more responsibility on online services and introduces fines for violations, legal and financial penalties are also increased for

[6] Committee on the Rights of the Child (CRC Committee), General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021 (CRC General Comment No. 25 (2021)), para. 3.
[7] CRC General Comment No. 25 (2021), para. 80.

individuals. For instance, section 27 (14) (2) introduces the crime of "hate propaganda" as well as "hate crime" to the *Youth Criminal Justice Act* among existing *Criminal Code* violations subject to summary conviction.

Children are already more likely than older people to be involved in and accused of the online harms that are the focus of Bill C-63. Most incidents of online sexual offences against children from 2014 to 2022 involved an accused person similar in age.[8] The median age of victims of online sexual offences was 15 years for girls and 14 years for boys, while the median age of accused persons was 15 years for boys and 14 years for girls. The most common accused-victim relationships were casual acquaintances, dating partners and friends.[9] Although men and women aged 15 to 24 are fairly equally likely to see content that may incite hate or violence, those accused of cyber-related hate crimes reported to police are typically young males.[10] More than one-third (35%) of those accused of cyber-related hate crime from 2018 to 2022 were aged 12 to 17.

Considering all children involved in online harms, in different ways, is necessary to protect their rights and their futures. It is imperative that new legislation and regulations require robust prevention efforts and afford comprehensive protection to all children. While Bill C-63 seeks to mitigate online harms in important ways, it must also avoid increasing the criminalization of children for their online behavior to the maximum extent possible. The UN Committee on the Rights of the Child states in General Comment No. 25 that "States parties should ensure that policy-makers consider the effects of such laws on children, focus on prevention and make every effort to create and use alternatives to a criminal justice response" to children. Children should not face extreme consequences for mistakes that are made at a developmental stage of evolving capacity, for acts in which manipulation and persuasion easily trump insufficient prevention and education measures.

Preventive measures should also be regarded as protection measures, just as legal prohibitions and consequences can increase child protection. For victims, the low proportion of crimes resulting in court convictions, and for youth involved in perpetuating harms, the serious and potentially lifelong consequences, emphasize the need for prevention strategies to avoid harm in the first place, including robust education together with private sector implementation of CRIA (which should encompass child rights by design, risk assessment and transparent safeguarding plans). Many organizations consulted by the Standing Committee on Justice and Human Rights stressed the importance of prevention when combatting online hate. Their recommendations included "raising awareness regarding online hate, promoting dialogue and engagement, and increasing education on 'responsible usage of social networking sites and websites'."[11]

63% of UNICEF Canada U-Reporters say they have learned about online safety at school.[12]

UNICEF Canada recommends that:

---

[8] Government of Canada, Statistics Canada. (2022, May 12). *The Daily — Online child sexual exploitation and abuse in Canada, 2014 to 2020*. https://www150.statcan.gc.ca/n1/daily-quotidien/220512/dq220512a-eng.htm

[9] Government of Canada, Statistics Canada. (2024d, March 12). *The Daily — Police-reported online child sexual exploitation in Canada, 2022*. https://www150.statcan.gc.ca/n1/daily-quotidien/240312/dq240312b-eng.htm

[10] Government of Canada, Statistics Canada. (2024a, February 27). *The Daily — Online hate and aggression among young people in Canada*. https://www150.statcan.gc.ca/n1/daily-quotidien/240227/dq240227b-eng.htm

[11] Report of the Standing Committee on Justice and Human Rights, Taking Action to End Online Hate, June 2019, 42nd Parliament, 1st session.

[12] https://canada-en.ureport.in/opinion/6971/

- **Bill C-63 establish a strong focus on prevention of online harms, recognizing the importance of robust and effective information/digital literacy and antiracist education.**
- **Legislative amendments ensure that children and youth are not disproportionately or inequitably criminalized by new legal sanctions, recognizing that they may be victims of persuasion and manipulation.**
- **The identities of all children are safeguarded throughout procedures conducted by the Digital Safety Office, the Canadian Human Rights Commission and the Canadian Human Rights Tribunal.**
- **Bill C-63 require online services and public authorities to adhere to internationally agreed standards that minimize the use of surveillance and algorithms to profile children's behaviours; and regular public audits of the algorithms used by online services.**

Online Services' Responsibilities to Prevent and Respond to Harm

Bill C-63 provides that certain online services, particularly social media and live streaming platforms, have responsibilities ranging from preventing to responding to harms. These include:

- proactively and continuously assess and mitigate risks and publishing digital safety plans;
- minimize users' exposure to harmful content; and
- provide users with flagging and blocking tools and remove offensive material.

Digital safety plans:

Respect for children's rights must reside within a company's core operations and how it carries out its daily business activities. The UN Committee on the Rights of the Child, in General Comment No. 25, calls on States to require the private sector to undertake a high standard of privacy by design and safety by design in digital services and products. To assess risks and create digital safety plans as provided for in Bill C-63, online services should be required to apply a comprehensive CRIA process encompassing safety by design; privacy by design; security by design; and inclusive design. For children, these considerations should be "designed in" by default. CRIA should be undertaken to assess positive and negative impacts of proposed digital products and services on children's rights across different age groups and among diverse groups of children. It is much more effective to proactively build features respecting children's rights into products and services than to try to react to the consequences of rights infringements and associated impacts on children.

Product and service design features:

Bill C-63 would mandate online services to prioritize children's interests in product design, adopting age-appropriate features similar to those in the UK, Australia and the EU. These include parental controls; content warnings; safe search settings; restrictions on targeted ads; and default settings for minors' interactions. Regulations issued by the Digital Safety Commission would outline these requirements, allowing for adaptation to emerging risks.

General Comment No. 25 calls for age-based or content-based systems to protect children from age-inappropriate content, balancing content moderation and controls with children's rights to freedom of expression and privacy. It also calls for protection from data exploitation, a harm not fulsomely addressed in Bill C-63, by prohibiting the profiling or targeting of children for commercial purposes, automated processing of children's data and digital surveillance (which should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver).

The Australian eSafety Commissioner's Safety by Design principles include providing tools for users to block and report problematic people and content; implementing technical solutions to minimize exposure to content risks; ensuring strong privacy settings by default; and promoting user empowerment. They emphasize taking preventative steps to ensure that known and anticipated harms have been evaluated in the design and provision of an online service; that user empowerment and autonomy are secured as part of the in-service experience; and that organizations take ownership and responsibility for users' safety and well-being and are clear about the steps required to address any issues.

The UK Information Commissioner's Age Appropriate Design Code (AADC) has a specific focus on children. It is grounded in the Convention on the Rights of the Child and reflects a risk-based and proportionate approach, calling for companies to: create an open, transparent and protected place for children online; follow a set of standards for design and development of online services likely to be accessed by children; consider the best interests of the child when processing their personal data; implement high privacy settings by default; and use language that is clear and easy for children at different development stages to understand. Companies will have to demonstrate that they are complying with the AADC, otherwise they may be fined.

These measures recognize the power imbalance between online service providers' push to capture greater user and data volume, and the capacity of families and children to protect themselves in an increasingly complex digital world. For too long, the focus of responsibility has rested unfairly on individuals and particularly on parents to shield their children from the harms that online providers create or amplify. Bill C-63 rightly aims to hold online services more accountable for their design choices and content.

The Bill's provisions and subsequent regulations must focus on the responsibility of online service providers rather than defaulting to parents to use controls. There is a clear role for parents in supervising their children's use of the Internet. Parental controls include device settings that allow children to download age-appropriate apps and games; filters that block age-inappropriate web content; and password controls that disable in-app purchasing to prevent large bills being run up at parents' expense. But this approach is most suitable for younger children and is largely ineffectual on personal devices and for older children who are able to circumvent parental controls. Furthermore, parental controls may infringe on children's rights to access information and to freedom of expression where their access is censored at an older age. Some features enable parents (and in some cases, teachers) to use more invasive types of surveillance to monitor children including location tracking; Internet search logs; websites visited and time spent on each; and monitoring of calls and texts. This raises ethical questions regarding the child's right to privacy, especially as they get older. Moreover, the data collected and monitored by these applications on behalf of parents is often processed by the commercial entities that operate them and may be shared with third parties including online advertising and analytics services.

Children – often for clear and justifiable reasons – are subject to other people's decision-making and consent governing their online activity. Efforts to support child safety online should also support children's resilience to confront issues online with confidence, seek support of adults when needed and support other children as peer educators. Different approaches will be appropriate for different ages and maturity levels. Online services should ensure that all control features intended for use by children are easy for diverse children to understand, trust, access and use. Relying on children to use the avenues of recourse provided by legislation may be ineffective without consulting them on the efficacy of these measures. For instance, research in Canada has found that children may feel that reporting hate speech or applying a peace bond may provoke their harasser and create more problems for them.[13] Research shows that younger children tend to be more vigilant about interpersonal privacy violations and less about corporate or government privacy violations, and often struggle to manage privacy settings.

63% of UNICEF Canada U-Reporters said they are very or somewhat confident in their ability to manage their online privacy and protection 68% use online privacy and protection settings.[14]

Privacy violation is a gateway for online harms. A limited understanding of or concern about the nuances of privacy risks makes children more vulnerable to online exploitation. While their capacity and understanding may expand as they grow, there is no specific age at which children and youth are fully and automatically capable of managing their privacy, which is unsurprising given how much adults struggle to do the same. Yet the legal bases that have been offered to children for online access or collection of their data largely rely on consent. Legislation in some jurisdictions sets an arbitrary age, usually of 13 or 16, at which a child is judged to be capable of giving their own consent.

As per the definition of a child in Bill C-63, children should be entitled to special protection and consideration by online services until they reach the age of maturity (at 18) irrespective of the age of consent. This protection should extend to the right of rectification and erasure (often referred to as the right to be forgotten) and protection from profiling based on automated processing. The UK Age Appropriate Design Code offers this additional protection to all children, without changing the existing age of consent.

Limiting exposure to harmful content:

One potential measure to protect children from exposure to certain types of harmful content that is not contemplated in Bill C-63 is digital age assurance and age verification tools to prohibit access based on age. The UN Committee on the Rights of the Child General Comment No. 25 states that to protect children from exploitation in the digital environment, "robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements". Policy-makers are considering or applying mandatory age assurance tools to a range of online content, contact, conduct and contract categories – mostly focused on pornography, gambling, gaming and certain apps (e.g., online dating). Restricting children's access to certain kinds of pornography online

[13] See research by Dr. Valerie Steeves and Jane Bailey: http://www.equalityproject.ca

[14] https://canada-en.ureport.in/opinion/6971/

has been considered a legitimate aim by certain governments. The UK Government introduced the first legislation to mandate the use of age verification to restrict children's access to online pornography, followed by France, Germany, some US states and Australia. In Canada, a Senate public bill focuses on age verification for accessing online pornography. The focus of such measures has been on commercial sites and much of the choice of verification methods is left to the content platforms. This approach depends on adults verifying age (so at least the privacy risks for children are circumvented). Criticisms with these laws have included the capacity – and possibly increased proclivity - for children to access pornography elsewhere such as on social media or sites in other jurisdictions. Objections have also centred on adults' rights to privacy and data protection. Supporters have argued that age verification is still likely to reduce children's exposure, even if it is not the sole or even principal firewall, and to hold providers more accountable for their conduct, consistent with offline content regulation. It has been noted that care is needed to avoid excluding children from sexual and reproductive health information and education.

Measures contemplated by policy-makers to regulate online services may involve balancing rights and risks. They can be considered with the proportionality test which involves three criteria: (1) any interference with a human right must set be set out in a clear legal provision detailing the restriction, (2) it must be in pursuit of a legitimate aim, and (3) the response should be proportionate and necessary. A relevant principle is the primacy of the best interests of children, and a relevant premise is that the more harmful specific content could be, the more restrictions are likely to be required.

UNICEF Canada recommends that:

- **Regulations and the Digital Safety Commission require online services to adopt a transparent process of comprehensive children's rights by design, inclusive of child-specific digital risk assessments and safety plans that are informed by: the Child Rights Impact Self-Assessment Tool for Mobile Operators (MO-CRIA); the UNICEF/ITU Guidelines for Industry on Child Online Protection; the Responsible Data for Children (RD4C) Principles; and the Manifesto on children's data governance in assessing and mitigating risks and developing digital safety plans. These plans should be re-assessed and updated frequently (s. 62(4)).**
- **Digital safety plans apply to product design, engineering, development, operation, distribution and marketing (s. 62).**
- **Digital safety plans identify research on forthcoming features, staying ahead of the curve (s. 62(1)(j)).**
- **Protective and reporting mechanisms put in place by online providers are designed with and for children, to ensure diverse children can easily understand and use these mechanisms and that children are treated safely and sensitively. This includes:**
    - **User guidelines (s. 57) and tools to block users (s. 58) are child-sensitive and provide for age-appropriate access and use in child-friendly language.**
    - **Tools and processes to flag harmful content (s. 59(1)(b)) specify a reasonable time limit for the operator's notifications and resolutions in response to a user's report. Children's notifications and take-down requests should be accessible by them and treated with a "low bar" for the erasure of content or data. The identity of any child user who has flagged/reported content to an online service must be**

protected so that notification to the person who communicated the flagged content does not reveal the child's identity, directly or indirectly.

- **Service operator resource persons (s. 61(2)) provide contact information, a complaint mechanism, guidance and responses that are child-sensitive, age-appropriate and available in child-friendly language.**

- **Protective measures and user reporting mechanisms do not unfairly shift responsibility for protecting children from online service providers to parents and children themselves; users should be empowered to easily use such mechanisms, but it is the responsibility of the providers to protect children from exposure to online harms through their design and content.**
- **Online services produce regular update reports, audited by an independent third party such as the proposed Digital Safety Office. These should be specific and transparent about how they respond to children's requests while protecting children's identities and confidentiality.**
- **The Bill address notable exclusions such as transparency in algorithm use to ensure comprehensive protection. The UN Committee on the Rights of the Child General Comment No. 25 recognizes that digital algorithms, data collection and analytics affect children even when they are not online. Algorithms used in relation to children such as safety and monitoring tools, health apps and behavioural analytics tools should be subject to regulation, and profiling and nudging of children's behaviour strictly prohibited. Services that use algorithms should provide a transparent explanation of the ways in which they are used to make decisions, and about the data used to train such algorithms.**

Scope of Online Service Providers

Bill C-63 specifically encompasses certain "online services": social media services with a broad public (rather than user-controlled private contacts and content); live-streaming services that exceed a certain user threshold; and "user-uploaded adult content services." Encrypted messaging services will be excluded, such as direct messaging or emails (e.g., instant-messaging apps like Snapchat). The exclusion of Snapchat is an example of a platform that is appealing to children and has been used to harm them. Children regularly migrate to new platforms, often to escape the company or surveillance of adults. Therefore, the initial, narrow focus of providers in Bill C-63 may address some of the sources of greatest risk but will still leave children exposed to online harms.

68% of UNICEF Canada U-Reporters said they feel safe when using social media.[15]

The Committee on the Rights of the Child has advised that all companies, irrespective of their size or industry, bear the duty to uphold children's rights and facilitate the resolution of any adverse impacts on these rights, whether online or offline. Regulatory requirements imposed on small and medium-sized enterprises should be proportionate to their size, although when carrying out CRIA, the measures taken should be proportionate to the risks to children that are identified rather than

[15] https://canada-en.ureport.in/opinion/6971/

proportionate to the size of the company. Smaller companies may require support from the State or from industry collectives to meet their due diligence requirements.

The UK Age Appropriate Design Code (AADC) applies to online services including apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news and educational websites, and websites offering other goods or services to users over the Internet. Businesses providing mobile devices and data, search services, digital advertising and entertainment including gaming are also integral to protecting children from online harms. Online service providers rely on a wide range of third parties to develop and deliver products and services. The business partners, clients (which may include public services and civil society organizations) and suppliers of online service providers should also come under risk assessment, as provided for in the UNICEF Child Rights Self-Assessment Tool for Mobile Operators (MO-CRIA).

Because technologies are entwined with almost all areas of children's lives, including public services, governments have an opportunity to support the corporate responsibility to respect children's rights through their engagement with the sector, such as procurement. For example, where governments procure technology for public health, education or social welfare services, a CRIA could be required. Governments and public authorities themselves must also put in place rules to govern the use of children's data held by the public sector, and to impose obligations on data intermediary services for the use of children's data.

UNICEF Canada recommends that:

- **Regardless of size or sector, all online service operators and providers implement a CRIA (such as the UNICEF MO-CRIA) and digital safety plans and child-sensitive protection and reporting mechanisms**.
- **Children be regularly consulted about the online services they use and the nature of their experiences with these services to ensure regulations encompass sources of harm as they evolve.**

Accountability Mechanisms

Bill C-36 introduces the Digital Safety Commission of Canada and a Digital Safety Ombudsperson, supported administratively by a Digital Safety Office. Additionally, individuals can file hate speech complaints with the Canadian Human Rights Commission. The right to remedy is a core tenet of the international human rights system. Remediation refers to both the processes of providing a remedy for an adverse human rights impact and to the substantive outcomes that can counteract or make good the adverse impact.

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography provides that States shall ensure that all child victims have access to adequate procedures to seek compensation for the offences committed against them. The UN Committee on the Rights of the Child in General Comment No. 25 calls on States to ensure that agencies with oversight powers relevant to children's rights investigate complaints and provide adequate remedies for violations or abuses of children's rights. Furthermore, children who face accusations are entitled to child-sensitive justice including protection of their identities, even in quasi-judicial tribunals. The UN Guiding Principles on Business and Human Rights calls on States to take

“appropriate steps to prevent, investigate, punish and redress” business-related human rights abuses within their jurisdiction and ensure that children whose rights have been adversely impacted by digital technologies have access to effective remedy. Where a business has caused or contributed to an adverse impact on human rights, it should provide for or cooperate in remediation through legitimate processes, including effective operational level grievance mechanisms or judicial mechanisms, as appropriate.

Operational level mechanisms for remediation provided by online services should be accessible to children, their families and those who represent their interests, and meet the effectiveness criteria for non-judicial grievance mechanisms set out in the UN Guiding Principles for Business and Human Rights. Effective grievance mechanisms should be both directly accessible by and tailored to children and to those acting on behalf of children who may not have the capacity to represent themselves. Effective reporting mechanisms are:

- Displayed prominently in a place where children can easily find them;
- Available in languages spoken by the children who are using the products, and phrased in age-appropriate ways using relatable and readily understandable language;
- Responsive and informative about what will happen when children make a report, including whom their information will be shared with and what kind of remedy they can expect;
- Capable of providing appropriate redress; and
- Created in consultation with children, parents and communities to ensure they meet users’ needs and provide a remedy that children consider to be effective.

In cases related to children’s rights and data, companies should ensure that they have child-friendly mechanisms in place that allow children to make data and deletion requests.

Within operational grievance mechanisms, there should be child-appropriate processes for receiving, handling, investigating and responding to children’s complaints. Those receiving reports from or about children must have the competence to handle them or know where to escalate them; investigation processes must protect the privacy of all children involved; and outcomes and remedies must adequately address any harms identified without creating additional harm. Specialized staff must be trained in child safeguarding, the company’s child-sensitive procedures and local legal requirements. The staff must be able to connect children to appropriate supportive services, social and legal, available in their communities.

Children must have access to available judicial mechanisms even if engaging with a company’s grievance mechanism, and companies should not impede children’s right to seek access to a remedy elsewhere. Where remedial mechanisms are provided by a company, children should be informed if they have a concurrent right to seek a remedy through other available state and judicial mechanisms.

Similarly, the Digital Safety Office should have a distinct, age-appropriate protocol to coordinate the receipt and resolution of children’s complaints while safeguarding them. It should coordinate responses to complaints related to data with the Privacy Commissioner of Canada. Meaningful consultations with children and their caregivers are necessary to understand and address the informational, legal, practical and procedural barriers that children may face in seeking a remedy and the risks they may face in accessing a remedy, such as the fear of reprisals.

Finally, there must be a “substantive” outcome that is effective for the child. Notably, Bill C-63 provides for monetary fines for online services who breach certain duties, but no financial compensation to child victims. The fines collected for violation of children’s rights should be invested by the federal government in prevention and support services for children related to online harms.

UNICEF Canada recommends that:

- **The Digital Safety Commission create a complaints mechanism that is child-friendly: known to children, easy and safe to access and use, and resolved by a dedicated children’s digital safety commissioner. One of the 3-5 Commission members should have a child-focused mandate and skills (s. 12).**
- **The Digital Safety Commission mandate (s. 11 e and f) and requirements (s. 27) expressly include the requirement to uphold children’s human rights, including priority afforded to their best interests and children’s right to participate in decisions affecting them, when making regulations and issuing guidelines, codes of conduct and other documents.**
- **Submissions (s. 78) and complaints (s. 81) functions of the Digital Safety Commission include child-friendly formats and protection of children’s identities.**
- **Children who make complaints to the Digital Safety Commission must not be requested to make representations (s. 82) unless safeguarded and with free and informed consent and participation, to avoid perpetuating trauma and potential privacy violation.**
- **Any hearings conducted by the Digital Safety Commission (s. 88) involving children must protect their identities.**
- **The Digital Safety Ombudsperson dedicates staff who have the skills to engage with children and ensure child-sensitive, confidential and safe engagement processes (s. 37 and 38) and design services such as helplines that are child-friendly.**
- **The Digital Safety Ombudsperson mandate (s. 31) includes specific reference to children as a sub-category of 'users'.**
- **Any type of information (defined in s. 127) received by the Commission and/or the Ombudsperson from or about a child is by default designated as confidential, whether or not the child so designates it, unless the disclosure of this information is determined to be in the best interests of the child. The best interests of the child should supersede public interest.**
- **All complaint and complaint resolution mechanisms operated by service providers and the Digital Safety Office apparatus are child-sensitive and child-friendly to guarantee full accessibility to all children; protect their identities and privacy; and provide appropriate remediation and support for harms experienced by them.**
- **Operational-level grievance mechanisms provided by online service providers are child-rights based and consistent with UNICEF’s guidance on “Operational-level Grievance Mechanisms Fit for Children”.**

Conclusion

Children are at disproportionate risk of a range of online harms in Canada. Bill C-63 represents a commendable step forward in enhancing their digital safety. The Bill recognizes the duty of governments to fulfil children's rights by legislating and regulating online harms and creating new enforcement and accountability mechanisms. It also recognizes the responsibility of the private sector to uphold children's rights. As such, it takes a systemic approach to online harms. UNICEF Canada welcomes the proposals in Bill C-63 to lower children's risks of certain, substantial online harms and to raise the response when harm occurs. These measures should increase children's protection, the remediation of harm and the accountability to which they are entitled.

The Government of Canada should apply a robust Child Rights Impact Assessment to ensure that potentially positive impacts of Bill C-63 are optimized, and potentially negative and inequitable impacts are avoided or mitigated. Children should be consulted to ensure a fulsome consideration of these impacts and corresponding amendments. Their perspectives and experiences can provide valuable insights into the scope and efficacy of proposed measures. UNICEF Canada's recommendations aim to help ensure that the legislation adequately considers and prioritizes the best interests of children, achieving the best balance of their human rights. A focus of our recommendations is to require online services to proactively undertake a comprehensive approach to children's rights by design (beyond "safety" and "risk" assessments and plans) and to ensure the protective mechanisms and recourses proposed in law and regulation are relevant to and easily used by children. UNICEF Canada also outlines the need to consider potential negative and inequitable impacts of heightened criminal sanctions on children and calls for a strong preventive focus to ensure all children can be safe and supported online. The proposed periodic review of legislation will be critical in this quickly evolving space if Canada is to keep "legislating for the digital age".

About UNICEF Canada

UNICEF is the world's farthest-reaching humanitarian organization for children. With a presence in more than 190 countries and territories, we work tirelessly in the world's most complex situations to bring life-saving aid and long-term support to children and their families. From our role as the world's largest provider of vaccines, to supporting child health, nutrition and education, we are determined to create a better world for every child. And we won't give up.

UNICEF Canada works to address and advance children's rights in Canada and around the world. Our life-saving work for every child is funded entirely through voluntary donations. Visit unicef.ca and follow us on Facebook, X/Twitter and Instagram to learn more.

www.unicef.ca @UNICEFCanada

For more information, please contact:

Lisa Wolff, Director of Policy and Research: lwolff@unicef.ca

Selected UNICEF Resources

Legislating For the Digital Age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse (2022)

The Case for Better Governance of Children's Data: A Manifesto

Child Rights Impact Self-Assessment Tool for Mobile Operators (MO-CRIA) (2021)

Rapid Analysis: Digital Misinformation/Disinformation and Children (2021)
Guidelines for Industry on Child Protection (2014)

Responsible Data for Children (R4DC): https://rd4c.org/

Industry Toolkit on Children's Online Privacy and Freedom of Expression

Operational-level Grievance Mechanisms Fit for Children

Discussion Paper Series: Children's Rights and Business in a Digital World

Children and Digital Marketing Industry Toolkit

Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper

Policy Guidance: AI and children (https://www.unicef.org/innocenti/reports/policy-guidance-ai-children)

Draft Paper: Taking a Child Rights Approach to Implementing the UNGPs [United Nations Guiding Principles for Business and Human Rights] in the Digital Environment

International Telecommunication Union (ITU)/UNICEF e-learning course for professionals in the technology sector:

- Understanding children's rights in the digital environment: Core frameworks and implications for business
- Respecting children's rights: Understanding and addressing online risks and harms
- Deep-dive: Online child sexual exploitation and abuse
- Supporting children's rights and well-being in the digital age

Available via: https://agora.unicef.org/course/info.php?id=46925

UN Committee on the Rights of the Child General Comment No. 25 (2021) on children's rights in relation to the digital environment