CANADIAN BAR ASSOCIATION
ASSOCIATION DU BARREAU CANADIEN

November 17, 2026

Via email: CHPC@parl.gc.ca

The Honourable Lisa Hepfner, M.P.
Chair, Standing Committee on Canadian Heritage
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

Dear Ms. Hepfner,

Re: Bill C-34 - Safe Social Media Act

We write on behalf of the Canadian Bar Association's Child and Youth Law, Privacy and Access Law, Constitutional and Human Rights Law, and Sexual and Gender Diversity Alliance Sections (CBA Sections). While we support the objectives of Bill C-34, the *Safe Social Media Act*, it falls short of emerging international standards on online safety.

The CBA is a national association representing 40,000 legal professionals across Canada. Its objectives include improving the law and administration of justice. Our recommendations address child safety as a distinct regulatory concern, child's rights and participation, child's rights expertise, marginalized populations, and constitutional, privacy and regulatory concerns.

Child safety as a distinct concern

Children's online safety warrants a distinct legislative framework that recognizes children as rights holders. The UK's *Data Protection Act* and Children's Code set a global benchmark; Canada should follow, consistent with its obligations under the United Nations Convention on the Rights of a Child (UNCRC) and the Office of the Privacy Commissioner's (OPC) new Children's Privacy Code (CPC). Combining child and adult online safety under one regime risks diluting children's distinct rights. [1]

Recommendations:

1. Enact stand-alone children's online safety legislation or establish a distinct Part focused on child-protection, recognizing children as rights holders under the UNCRC. This includes a Children's Code on age-appropriate design modelled on s. 123[2] of the UK Data Protection Act 2018.
2. Require the Digital Safety Commission of Canada (Comission) to coordinate with the OPC to ensure consistent standards with the CPC for age assurance, default settings and the collection and use of children's personal information.

---

1 *Data Protection Act 2018* (UK), c 12, s 123, online; ICO, *Age Appropriate Design Code* (2020), online; CRC, General Comment No. 25 (2021), CRC/C/GC/25, paras 23-24, online; OPC, *Children's Privacy Code* (20 October 2026), online.

2 *Ibid*.

Child rights and participation

Any approach should rest on the best interests of the child (UNCRC, art. 3(1)) and meaningful child participation. The European Commission's Child Safety Online report and proposed EU KIDS Act place primary responsibility on providers with graduated age-based and safety-by-design obligations, reflecting children's evolving capacities. [3] In addition, children are entitled to be heard on legislation such as Bill C-34. The process to create the OPC's Code shows meaningful consultation is achievable.[4]

Recommendations:

3. Require the best interests of the child be a primary consideration in all decisions affecting children under the Act. Child-specific obligations should reflect children's age and evolving capacities.
4. Hold dedicated consultations with children's groups, including Indigenous, disabled, newcomer, racialized and 2SLGBTQIA+ youth, children in care, and those in rural and remote communities, before finalizing the Bill.

Child rights expertise in oversight

At least one Commission member needs expertise in child protection and children's rights, including child-rights impact assessments (CRIAs).[5] The risk assessments required under Sections 18(e) and 42(1) are not child-specific. Alternatively, a National Commissioner for Children could strengthen oversight, bringing Canada in line with many peer countries.[6]

Recommendation:

5. Require child protection and children's rights expertise on the Commission or establish a National Commissioner for Children.

Marginalized and vulnerable communities: access to 2SLGBTQIA+ affirming information

Operators must limit access by users under 16 to content not shown to be safe and take measures to reduce harm. Platforms may over-restrict affirming content about 2SLGBTQIA+ identity, relationships, sexual-health education and gender-affirming care by mislabeling it as sexual or harmful. This material is critical support for many youth; restricting it may undermine the child's right to information.[7]

Recommendation:

6. Expressly exclude 2SLGBTQIA+ affirming information from the definitions of harmful and pornographic content. We suggest a statutory carve-out:

> "For greater certainty, content is not harmful content or pornographic content by reason only that it depicts, describes, discusses, or provides education, information, or support relating to sexual orientation, gender identity or expression, gender-affirming care, or 2SLGBTQIA+ relationships or sexual health."

---

3 European Commission, Child Safety Online (13 July 2026), online; *EU KIDS Act* proposal, (2026) 681 (17 September 2026), online; *Supra* note 2.

4 OPC, *supra* note 3.

5 Department of Justice, Child Rights Impact Assessment tool (2023), online.

6 S van der Hof & T Liefaard, Digital Play: Children's Rights, Risks and Responsibilities (2025).

7 UNCRC, art 17.

The Bill rightly recognizes that the repeated, highly personalized nature of AI chatbots interactions creates unique risks requiring mandatory safeguards. Safeguards should target escalating suicidal or violent ideation, planning and circumvention efforts, without treating affirming discussions of sexual orientation or gender identity as indicators of self-harm.

Recommendations:

7. Include explicit safeguards in the Bill's chatbot provisions for 2SLGBTQIA+ users.
8. Clarify restrictions on "manipulative engagement techniques" to target exploitative design without restricting supportive, affirming resources.

The “reasonable grounds to suspect” threshold, user flagging and safety-plan obligations may encourage discriminatory algorithmic over-enforcement, restricting 2SLGBTQIA+ content. Indigenous and racialized 2SLGBTQIA+ youth may rely more on online support while facing greater risks of harm. Operators should assess actual risk rather than treating such content as inherently risky.

Recommendations:

9. Require operators to moderate content on a non-discriminatory basis and provide clear guidance distinguishing educational and affirming content from harmful or pornographic material.
10. Require transparency and independent auditing of content-removal and down-ranking decisions.

Proposed statutory language is available on request.

Statutory guardrails and accountability

Bill C-34 leaves key standards to regulations or the Commission, raising concerns about whether limits on expression meet the prescribed-by-law, minimal impairment and proportionality requirements under s. 1 of the *Charter*. The Commission’s broad powers, limited ministerial oversight and restrictions on employee testimony may hinder judicial review and accountability. While the Bill requires a warrant for entry, its other investigative powers are not subject to prior judicial authorization.

Recommendations:

11. Require Governor in Council approval and parliamentary review of Commission regulations that expand the types of regulated content or behaviour, including chatbot behaviours specified under s. 126(1)(v) for the purpose of s. 53(e).
12. Require the Commission to report to Parliament.
13. Appoint the Commissioner as an independent officer of Parliament.
14. Permit Commission employees to testify in judicial review proceedings.
15. Extend the requirement for prior judicial authorization to the Commission’s other search powers, consistent with *Hunter v. Southam*.
16. Require a structural separation of the Commission’s investigative and adjudicative functions for administrative monetary penalties and content orders, such as a separate adjudicative division under s. 8 of the *Digital Safety Commission of Canada Act* and provide a statutory right of appeal from penalty decisions and permanent takedown orders to the Federal Court.
17. Establish clearer statutory standards for key terms such as “adequate” safeguards and “significant risk of harm,” rather than leaving them to the Commission or regulation.

Overbroad definitions

Key definitions require platforms facing significant penalties to assess content and intent, and weigh public interest and free expression values, a task better suited to courts. "Acts of terrorism or violent extremism" extends to property damage and common assault. "Sexual victimization of a child" could capture public interest expression (e.g., documentation of war crimes against children, news reporting or literature) and advocacy about the age of consent. "Content used to bully a child" could capture criticism of a child, and services meeting the "social media service" definition are regulated once they reach a user threshold set by regulation, without any statutory requirement to demonstrate a risk of harm. These definitions raise overbreadth and proportionality concerns. Clear, child-specific obligations (Recommendations 1 to 5) would better protect children without suppressing lawful expression.

Recommendation:

18. Narrow the definitions of "acts of terrorism or violent extremism," "sexual victimization of a child," "content used to bully a child," and "social media service" so that platforms are not left to resolve questions of content and intent and public interest that are properly the role of the courts.

Freedom of expression and intimate content takedowns

The definition of "intimate content communicated without consent" uses a "reasonable to suspect" threshold on consent, a factual question on which platforms have little information. Under ss. 43 to 46, a complaint not dismissed as frivolous, vexatious or made in bad faith triggers interim content removal pending a decision; the Commission must do the same after its own screening. Nothing requires the complainant to be the person depicted or their representative. This risks suppressing lawful adult expression protected by s. 2(b) of the *Charter*, including content the person depicted chose to publish. Permanent removal should require a finding, on a balance of probabilities, that content is prohibited.

Recommendations:

19. Regulate content that sexually victimizes a child separately from intimate content communicated without consent. Address child sexual abuse material through the child-specific framework and age-appropriate design code, with reporting and response procedures allowing rapid intervention.

20. For intimate content involving adults:
    - Limit complaints to persons depicted or their representatives.
    - Ensure that uncertainty about consent does not automatically favour removal.
    - Require a substantive preliminary finding before operators or the Commission must make disputed content inaccessible; screening out frivolous, vexatious or bad faith complaints is insufficient.
    - Require disputed facts to be established on a balance of probabilities before permanent Commission takedown orders, with written reasons.
    - Establish expedited restoration where interim removal is reversed.

Social media ban and age assurance

Sections 27 to 29 require age assurance to bar persons under 16 from holding accounts. Social media supports young people's expression, association and political engagement. A categorical ban, applied across all regulated services regardless of risk or maturity, is a *prima facie* infringement of s. 2(b) of the *Charter*. France's constitutional court recently found its ban disproportionately infringed young people's expression, and that requiring all users to prove their age without legal safeguards violated privacy.[8]

---

8 Conseil constitutionnel, *Décision n° 2026-911 DC* (14 August 2026), paras 17-21, online.

Despite limits on use and retention, concerns remain about age-assurance technologies, government identification, biometrics, error rates and alternatives. Data minimization should govern, preferably through an age or eligibility signal, and exclusion should not begin before exemption processes are operational. Unlike the graduated EU KIDS Act model, the Bill imposes a single threshold of 16 and leaves age-appropriate design to permissive guidance, weighing against minimal impairment.

Recommendations:

21. Reconsider the necessity and proportionality of a categorical ban on social media accounts for persons under 16 and whether binding age-appropriate design and graduated access could mitigate risks less intrusively.
22. If the minimum-age regime is retained:
    - Require the least privacy-intrusive age-assurance method reasonably available, using only information necessary to verify eligibility;
    - Ensure consistency with the OPC's CPC;
    - Expressly exclude age-assurance identity information from the record-keeping duty in s. 25 and require its destruction within a fixed period; and,
    - Include a five-year sunset provision.
23. Prohibit mandatory government-issued identification where less intrusive methods can establish eligibility and discourage centralized databases of identity or age-verification information.
24. Delay implementation until regulations, exemption criteria and Commission guidance are in place, with reasonable time for operators to seek exemptions.

Regulatory and inspection powers

We support the warrant requirement for entry without consent, which also covers remote access. Section 80 gives inspectors broad power to demand documents. Compelled disclosure of data to researchers raises confidentiality, intellectual property, privacy, re-identification and cybersecurity risks, particularly for children, with protections largely left to regulations.

Recommendations:

25. Amend s. 80 to require that information demands be reasonably necessary and proportionate to a specified compliance purpose; expressly preserve legal privilege and permit prompt review of disputed demands.
26. Establish statutory safeguards for compelled researcher access, including necessity and proportionality, data minimization, de-identification where reasonably possible, security standards, meaningful operator representations and an effective mechanism to challenge access orders.

The Bill does not set out how the Commission must assess Digital Safety Plans, or what supervisory steps must precede a finding of non-compliance, yet the Commission may impose administrative monetary penalties of up to the greater of $10 million or 3% of gross global revenue (s.88). Penalties should follow a structured process, as in the EU *Digital Services Act*.

Recommendations:

27. Set out statutory duties for Commission review of Digital Safety Plans, including assessment criteria, scrutiny of risks to children informed by CRIA, written feedback to operators and reasonable opportunities to remedy deficiencies.

28. Require regular compliance audits under Commission standards for auditor independence and methodology, with transparent findings.

29. Before imposing monetary penalties, require preliminary findings, access to the file and an opportunity to be heard. Where appropriate, require independently verified remedial action plans. Penalties should reflect the nature, gravity and recurrence of non-compliance.

Conclusion

The CBA Sections support the stated objectives of Bill C-34 but recommend necessary amendments to:

(a) Give children's online safety its own legislative framework;

(b) Pair binding age-appropriate design and graduated access rather than a relying on a single categorical age ban; and

(c) Set out stronger statutory, procedural, privacy and expression safeguards.

Yours truly,

(*Signed by Yasmin Khaliq for the CBA Chairs*)

Christian Whalen
Chair, Child and Youth Law

Brent Arnold
Chair, Privacy and Access Law

Errol P. Mendes
Chair, Constitutional and Human Rights Law

Anastacia L. DesLauriers
Chair, Sexual and Gender Diversity Alliance Sections