# David Young Law
# Compliance Bulletin

**June 2026**

## New online harms law – a modern, measured approach or tilting at windmills?

Last Wednesday the federal government introduced its long-awaited proposed revised online harms law – Bill C-34, the *Safe Social Media Act*, and on Monday, tabled its new private sector privacy reform bill, Bill C-36, enacting the *Protecting Privacy and Consumer Data Act* (PPCDA).

The iterative tabling of these two bills, although not entirely in synch,[1] should be seen as revealing the government's coordinated approach to not only its updated framework for addressing online harms, with particular focus on children and youth, but also for a reformed privacy law. To appreciate the alignment of these two areas of regulatory oversight under the new laws, one needs look no further than the role of the proposed Digital Safety and Data Protection Commission of Canada which will have authority not only for protection against online harms but also for protection of personal information.[2]

Bill C-34 might be characterized as having three main thrusts: a more articulated version of the government's previous attempt at passing online harms legislation (Bill C-63) minus the hate speech and inciting violence provisions; provisions aimed at mitigating risks involving chatbots; and a social media ban for individuals under the age of 16.

However, viewed in its entirety, the Bill could be seen as a measured and forward-looking approach to addressing the serious challenges posed by potential online harms to youth and users generally, as well as third parties, emanating from social media platforms and chatbots, challenges that are being grappled with worldwide with, to date, differing approaches and levels of success.[3]

**Online harms and privacy – one regulator**

The Bill, now amended by Bill C-36, enacts two separate legislative documents – the *Digital Safety Act*, which articulates the substantive rules constituting the proposed protective framework for online harms, and the *Digital Safety and Data Protection Commission of Canada Act.* The latter Act establishes the Commission as the regulator tasked with overseeing the framework's substantive protections, as well as enforcing the new privacy reform law.

---

[1] To note, the privacy reform bill amended a number of provisions set out in the as yet not passed online harms bill, most significantly with respect to role of the proposed Digital Safety and Data Protection Commission and the extension of its jurisdiction to private sector privacy oversight.

[2] Under Bill C-36, administration and enforcement of the substantive privacy rules in the new PPCDA will be the exclusive jurisdiction of the Commission – the Office of the Privacy Commissioner's role will be narrowed to oversight of federal government institutions under the *Privacy Act*.

[3] See for example: Australia's social media ban for children under 16, Manitoba's proposed ban and the UK's proposed social media, online gaming and streaming ban.

.

The Commission's powers under the online harms law will include the authority to make regulations including for example, setting out prescribed youth-protective design features for platforms, the approval of platforms' digital safety plans, exempting platforms from the social media ban, ordering take-downs of certain harmful content, and enforcing the protective rules including issuing orders for compliance and imposing monetary penalties.

Concerns have been voiced regarding the extent of the Commission's roles under the *Digital Safety Act* and the PPSDA, suggesting that the Commission will be a new digital super-regulator with significant influence over the daily lives of Canadians.[4]

**Framework for Platform Governance**

Notwithstanding its being touted as the vehicle for imposing a social media ban, the Bill provides for what may be characterized as a more substantive - and likely more expeditious - institution of a framework for protection against online harms – focussing on platform governance. This framework will require, for example, for all regulated platforms,[5] the development and approval by the Commission of a "Digital Safety Plan" – building on that concept first introduced in Bill C-63 - addressing a platform's measures to mitigate risks of exposure to harmful content including risk assessments, mitigation measures, adoption of design features for protecting against such harms in particular for youth, and criteria for assessing the effectiveness of such measures. The Bill also reiterates and articulates in greater detail the duties of platforms to act responsibly and to be transparent, also as originally set forth in Bill C-63.

**Social Media Ban – what is intended?**

While the "headline" moniker of the Bill is the enactment of a social media ban for children, a closer reading of its provisions reveals that such a ban would only come into effect for platforms designated by regulation, requiring them to have age-control protocols also stipulated by regulation once such controls are determined by the Commission as adequate. The issue of age controls, which potentially would apply to all users, not just youth, is the most controversial aspect of any social media ban, involving the collection by the platforms of potentially extensive sensitive personal information.[6] It reasonably can be anticipated that the proper development, approval and institution of such controls will have a longer-term trajectory, given the regulation-making process and likely consultation process, not to mention approval by the yet to be appointed Digital Safety and Data Protection Commission.

Significantly, the Bill provides for the exemption from the social media ban for platforms that can demonstrate that they have instituted adequate safeguards addressing the protection of children. Assuming that all regulated platforms have adopted and are aligned with the Bill's requirements for platform governance, which will come into force presumably following an appropriate transition period,[7] it might be asked, what platforms would not qualify for exemption from the

[4] See: Michael Geist Blog, The Commission: How Bill C-34 Creates an Internet Super-Regulator That Will Touch the Lives of Millions of Canadians, June 15, 2026.

[5] Meaning a "regulated service" defined as a regulated social media service, a regulated chatbot service or other regulated online service, all as meeting criteria or specification as set out in regulations.

[6] See: Protecting children online – age verification concerns and social media bans, Compliance Bulletin, May 2026.

[7] See: Michael Geist Blog June 11, 2026, The Law to Be Named Later: Bill C-34 Punts 50 Key Decisions to Cabinet and a Digital Safety Commission That Does Not Yet Exist,

ban? It may be surmised that the likely lead candidates for designation to be governed by a ban – such as Facebook, Instagram, X, WhatsApp - will make major efforts to be exempted, rather than institute potentially controversial age controls for all their users.

Understanding this broader context, one could hypothesize that the contemplated social media ban is really intended to be seen as a last resort, to be operationalized only in exceptional circumstances and once fully articulated privacy-protective protocols have been developed. However, media reports of the government's plans suggest a different trajectory, with the ban coming into effect immediately on passage of the Bill, without waiting for privacy-protective requirements to be in place, or allowing platforms time to align their practices with the new governance duties laid down by the Bill and potentially seeking exemption from the ban. [8]

**Regulated Services**

The thrust of the new law will be to regulate social media platforms with the particular focus on protecting children and youth. However, the law will have broader application – to chatbots as well as potentially any other online service that may be accessed by children. Inclusion will be determined by criteria set out in regulations (number of users) or if otherwise deemed warranted, by regulation stipulating included categories of platforms (e.g. pornography sites).

All "regulated services" will be subject to a general duty to protect children and to this end must incorporate into their platforms design features set out in regulations prescribed by the Commission. Furthermore, all regulated services, if they provide access to pornographic content, must establish measures to mitigate the risk of such access by children, including age-based access controls meeting adequacy and reasonableness criteria set out in the Act. These criteria include privacy-protective measures such as destruction of personal information collected for purpose of age estimation once that estimation is completed.

**Children's Design Code?**

A significant rule applicable to all regulated services is the requirement to adopt platform design features for the protection of children, in accordance with regulations prescribed by the Commission. It may be noted that notwithstanding urging by privacy activists for the reformed privacy law to include provision for a mandatory code of practice for the protection of children's personal information,[9] no such privacy protective rules are contained in the proposed PPCDA.[10]

However, the federal Office of the Privacy Commissioner is preparing a children's privacy code building on the responses that it received during a consultation with respect to the adoption of such a code. The goal of the consultation was informing the development of a children's privacy code that would clarify obligations under applicable privacy law and

[8] Michael Geist Blog June 12, 2026, The Exemption Illusion: Why the Government's Plan to Fast Track Bill C-34's Kids' Social Media Ban Means No Standards, No Privacy Review, and No Enforcement.
[9] See, for example, Centre for Digital Rights, Not Fit For Purpose - Canada Deserves Much Better, Centre for Digital Rights' Report on Bill C-27 Canada's Digital Charter Implementation Act, 2022, October 2, 2023.
[10] As noted by the OPC, codes of practice and special protections contained in privacy legislation can empower children to exercise their privacy rights and protect against potential harms experienced by children as they navigate online spaces.

set out the OPC's expectations regarding protection of children's personal information and protection against online harms.[11]

The requirement under the *Digital Safety Act* for platforms to adopt child-protective platform design features may be seen as a vehicle for the Commission to articulate in effect a mandatory design code that addresses not only online harms but also the related protection of children's online privacy. In the context of the projected transfer of the OPC's private sector oversight role to the Commission, it might be surmised that the OPC's work on an online privacy code could inform the development of the regulations setting out requirements for such a children's online design code.

**Digital Safety Plans**

A key rule applicable to all regulated services, is a "duty to be transparent" - which resolves to a requirement to submit a *digital safety plan* to the Commission in respect of each platform that they operate. The digital safety plan must include detailed information addressing a comprehensive list of items set out in the Act including how the platform complies with each of the protective rules provided for in the legislation, the platform's experience in implementing such measures, its research related to improving such measures, whether any reporting of incidents to law enforcement authorities was made and its criteria for such notification, whether any incidents of child exploitation were reported under the relevant legislation, and an electronic record of data used to prepare the information required for the plan document.

**Regulated Social Media Services**

Within the category of regulated services, the class of "regulated social media services" is subject to additional, specific rules, with a particular focus on children and youth but with broader application to preventing access to harmful content by all potential users.[12] A regulated social media service is again defined by criteria prescribed by regulation (number of users) or if not otherwise falling within such criteria, specifically designated by the Commission in a regulation.

Firstly, all regulated social media services specified by regulation or falling within a class of such service specified by regulation must establish age control measures designed to prevent persons under the age of 16 from accessing the platform. Such measures must meet the adequacy and reasonableness criteria set out in the Act including privacy-protective measures such as destruction of personal information collected for the purpose of age estimation once that estimation is completed. In addition, such measures must comply with any other requirements if set forth in regulations.

As noted, an overriding rule provides for the Commission to exempt from the age ban any social media platform that has established, to the satisfaction of the Commission, "adequate safeguards" for the protection of children. To this end,

[11] See: Consultation on the Development of a Children's Privacy Code – What We Heard, OPC, May 4, 2026
[12] Harmful content is defined to mean: intimate content communicated without consent; content that sexually victimizes a child or revictimizes a survivor; content that induces a child to harm themselves; content used to bully a child; content that foments hatred; content that incites violence; and content that incites violent extremism or terrorism.

the Commission is empowered to make regulations setting out criteria for such adequacy and to establish guidelines setting out what such adequacy may look like.

The second key rule, applicable to all regulated social media services, is a "duty to act responsibly" in implementing measures to mitigate the risk that users of the service will be exposed to harmful content. The Act sets out criteria that must be addressed in determining whether such measures are adequate, including the effectiveness of such measures, the size of the service, the technical and financial capacity of the operator, and whether the measures are designed or implemented in a manner that is discriminatory on the basis of a prohibited ground of discrimination within the meaning of the *Canadian Human Rights Act*. The Commission is empowered to publish regulations setting out more specific criteria of adequacy for such measures.

With respect to potential harmful content, platforms are required to publish guidelines for users setting out their policies regarding harmful content, make tools available for users to flag and report harmful content, and must implement processes for addressing any such content including potentially, flagging, removing access and reporting to law enforcement authorities.

The third specific rule applicable to all regulated social media services is a duty to implement measures to label any "synthetic content" – meaning essentially *deepfake content* - accessible on the service that meets the criteria provided for by regulations. Criteria for assessing whether such measures are adequate and reasonable are set out in the Act, including whether or not they are accurate in labelling them as such, the extent to which it is technically feasible to identify such content, the size of the service, and the technical and financial capacity of the operator.

Finally, as with other regulated services, a regulated social media service is required to develop and submit to the Commission for approval a digital safety plan, including the information listed in the detailed items set out in the Act.

**Regulated Chatbot Services**

A significant inclusion in the proposed law, in light of the Tumbler Ridge tragedy, are duties imposed on "regulated chatbot services" again defined by criteria stipulated in regulations or specifically identified by regulation. As with other regulated services, regulated chatbot services will have a "duty to act responsibly" in this case to take measures to mitigate the risk that the service will communicate harmful content to a user. In addition, significantly, the service must have in place emergency measures to intervene in the event that a user expresses any intention of harm whether to themselves or to others, including any measures set out in regulations. Other requirements include measures to mitigate the risk of the service posing as an advisor or otherwise posing as a human being, guidelines for users to respond to the communication or expression of harmful content, and providing tools to enable users to flag any such communication or expression.

As with the digital safety plans required for other regulated services, regulated chatbots must include in such plans detailed information addressing a comprehensive list of items set out in the Act, including their criteria for notifying law enforcement authorities of circumstances involving potential risk that an individual will cause death or serious bodily harm to another individual as well as an account of any such notifications.

**Conclusions**

As noted, viewed in its entirety, the proposed framework under Bill C-34 could be seen as a measured and forward-looking approach to addressing the challenges posed by potential online harms to youth and users generally, as well as third parties, emanating from social media platforms and chatbots.

The framework focusses on platform governance notwithstanding its bright line media call-out as imposing a social media ban for children. However, it is not clear whether the government's intention is actually to have such a ban in place for the mainline social media platforms, at least before those platforms have had the opportunity to align their practices with the protective governance rules set out in the Bill.

It is recognized that any such ban involves the collection by the platforms of potentially sensitive personal information of any intended user - meaning likely from a wide swath of Canadians. While not evident from the text of the Bill or the government's pronouncements to date, a more considered ultimate approach could be to move forward and prioritize operationalizing the platform governance protocols contemplated by the Bill, thus obviating the need for a ban, or at least punting it down the road until technologies are developed that avoid the need for any significant personal information collection by the platforms.

*For more information please contact:* David Young 416-968-6286 david@davidyounglaw.ca