Canada moves to regulate online safety: Understanding the Safe Social Media Act (Bill C-34)

June 17, 2026

What Canadian companies need to know (if enacted):

- Bill C-34 is broader than previously proposed online safety legislation and targets regulated social media services, certain online services, and AI chatbot services, with a focus on protecting children and supporting victims of online harms.
- Regulated services, as applicable, have a duty to act responsibly, a duty to protect children, a duty to be transparent, and a duty to make certain content inaccessible.
- Regulated services will have to implement and publish a digital safety plan.
- A new regulator is created, the Digital Safety Commission,[1] which will administer and enforce the new act.
- Non-compliance may result in administrative monetary penalties of up to the greater of $10 million or 3 per cent of global revenue, and penal sanctions of up to the greater of $20 million or 5 per cent of global revenue.
- The majority of the operational requirements remain to be determined and will depend on future regulations and guidance.
- Early governance and risk-readiness planning is important.

The introduction on June 10, 2026, of Bill C-34, *An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts* (Bill C-34 or the Safe Social Media Act), marks a significant and long-awaited development in Canada's evolving regulatory framework for online safety.

Bill C-34 is broader than previously proposed legislation (Bill C-63), which focused on regulating social media service providers. By contrast, Bill C-34 proposes a regime aimed at addressing online harms, particularly those affecting children, while introducing new (and ongoing) disclosure obligations for social media platforms, online services, and artificial intelligence (AI) chatbot services. It also reflects a broader effort toward increased accountability for service operators, although many key elements remain to be defined through future regulations, resulting in a degree of uncertainty as to the final contours of this new legal framework.

Overview

The federal government's backgrounder emphasized the rapid development of AI and new challenges in online environments, particularly where children are at risk. The Tumbler Ridge tragedy is one of too many examples of the underestimated risks of AI and online services, as we know that voluntary actions by digital services cannot always keep pace with the scale, speed and severity of online harms.

Bill C-34 establishes a dual legislative framework by enacting the *Digital Safety Act* and the *Digital Safety Commission of Canada Act*. Together, these instruments create both the substantive obligations applicable to regulated services and a new institutional body in charge of enforcement, the Digital Safety Commission (DSC), with a mission to promote safety in online environments for children under 18, reduce exposure to harmful content, and ensure that operators of regulated services are accountable and transparent in the design and operation of their platforms.

General obligations under Bill C-34

The proposed regime organizes operators of regulated services (such as social media services, chatbot services or online services) obligations around a series of core duties, which are applicable to all operators or specific to the service provided, as described below.

Operators have a general duty to protect children, notably by implementing adequate minimum-age verification or estimation measures to mitigate children's exposure to pornographic material, and implementing prescribed design features respecting the protection of children.

The operators will also have a general duty to be transparent. The transparency obligation in Bill C-34 is operationalized by the publication and submission of a digital safety plan to the DSC, and the requirement to keep records of their compliance with the Act. The digital safety plan must be adapted to the regulated service, and must be made publicly available in an accessible and easy-to-read format. Uncertainty remains with respect to the updating requirements of the plan.

Regulated social media services

A regulated social media service is a social media service with a specific number of users to be determined by regulation, or designated as a social media service by regulation.

Duty to protect children

Beyond the general duty to protect children for each of the social media services it operates, operators of a regulated social media service must implement adequate age-verification or age-estimation measures designed to prevent children under 16 years old from having an account with a regulated social media service. This is subject to potential exemptions that may be granted if the operator establishes and maintains sufficient safeguards for children.

Duty to act responsibly

Operators of regulated social media services will be required to integrate design and safety measures prescribed by regulation to mitigate the risk of exposure to harmful content. The proposed law defines “harmful content” to include content that:

1. is intimate and shared without consent;
2. sexually victimizes a child or a survivor of childhood sexual victimization;
3. induces child self-harm;
4. is used to bully a child;
5. foments hatred;
6. incites violence; and
7. includes terrorism or violent extremist.

Safety measures include providing tools that enable users to block other users, flag harmful content, and an obligation to label AI-generated content and harmful content through adequate mechanisms. The operator will have to make user guidelines accessible, publicly available on the service, and easy to use. They shall include a standard of conduct applicable to users with respect to harmful content, as well as the description of the measures implemented with respect to harmful content on the service.

Operators will also have to designate a resource person, whose contact information must be easily accessible, to assist users with respect to harmful content on the service, and preserve certain harmful content for a period of one year after content is made inaccessible. The operators of social media services will eventually also have to comply with additional measures provided by regulations, which have yet to be determined.

Duty to be transparent

For regulated social media services, the digital safety plan must describe:

- the operator’s risk assessment;
- mitigation measures against harmful content and, on the service, the operator’s public user guidelines with respect to harmful content;
- measures to protect children against exposure to pornographic content;
- child-protection design features;
- age-related measures implemented;
- law-enforcement notification processes;
- allocated human or automated resources;
- content moderation data;
- tools and processes in place to flag harmful content;
- a summary of the findings and conclusions with respect to harmful content on the service, or risk of significant psychological or physical harm;
- mandatory reporting compliance;
- supporting electronic data; and
- any other information prescribed by regulation.

Duty to make certain content inaccessible

The new legislation requires social media platforms to make certain categories of content inaccessible in Canada, including content that sexually victimizes a child, revictimizes survivors, or consists of intimate content shared without consent. Notably, this includes a 24-hour take-down requirement triggered by operators identifying or receiving reports about nonconsensual distribution of intimate images, or child sexual abuse material.

Regulated chatbot services

A regulated chatbot service is defined as a chatbot service with a specific number of users to be determined by regulation, or being designated as a chatbot service by regulation, but which does not include an artificial intelligence system that exclusively serves a purpose specified in the future regulations.

Duty to act responsibly

A particularly notable feature of Bill C-34 is its explicit regulation of AI chatbot services. Operators must implement adequate safeguards to reduce the risk that chatbots will communicate harmful content or engage in harmful behaviours. The legislation identifies specific prohibited behaviours, including posing as a human in a deceptive manner, impersonating licensed professionals such as lawyers or physicians, and using manipulative engagement techniques that encourage users to form emotional dependencies.

Operators will have to make user guidelines accessible, publicly available on the service, and easy to use. These must include a description of the measures implemented by the operator to mitigate the risk that the service will communicate harmful content; address situations regarding suicidal ideation and an intention to encourage self-harm, or cause death or serious bodily harm to an individual; and, mitigate the risk that the chatbot service will engage in any type of previously indicated prohibited behaviours. Other obligations include ensuring intervention in crisis situations, such as where a user expresses suicidal ideation or intent to harm others.

Additionally, operators of regulated chatbot services will have to provide easy-to-use reporting tools and a dedicated resource person for users. The tools will help users flag harmful chatbot content, failures to respond to self-harm, suicide or serious-harm risks, and other harmful chatbot behaviours covered by Bill C-34. They will also have functionalities of acknowledgement of receipt to the user. The designated resource person, whose contact must be easily accessible, will assist users with respect to harmful content arising through chatbot interactions.

Some aspects of the regulatory framework applicable to AI chatbot services also remain to be defined through future regulations, with which operators will ultimately be required to comply.

Duty to be transparent

For regulated chatbot services, the digital safety plan must especially address:

- the operator's safeguards against harmful chatbot communications and harmful behaviours;
- crisis intervention and emergency measures;
- child-protection design features;
- age-verification measures;
- measures to reduce children's exposure to pornographic content;
- law-enforcement notification processes;
- tools and processes in place to flag harmful content;
- related notifications;
- allocated human or automated resources;
- compliance with mandatory reporting obligations and the electronic data used to support this information; and
- any other prescribed information.

Regulated online services

A regulated online service is defined as an online service having a specific number of users to be determined by regulation, or being in a category of online services that could pose a significant risk of harm to children in Canada, also to be determined by regulation. However, it does not include a website or application designed to facilitate the sale, listing or advertisement of goods or services, or to provide directories, search results, maps or navigation tools. Duties under the proposed legislation do not apply to private messaging features on online services.

Duty to be transparent

Operators of regulated online services would have a duty of transparency to be complied with by preparing, publishing and submitting a digital safety plan to the DSC. For regulated online services, the digital safety plan must particularly address:

- the operator's child-protection design features;
- age-verification measures;
- safeguards against children's exposure to pornographic content;
- law-enforcement notification processes;
- allocated human or automated resources to address risk prevention;
- compliance with mandatory reporting obligations and supporting electronic data; and
- any other prescribed information.

Bill C-34 enforcement and sanctions

Enforcement of Bill C-34 obligations is entrusted to the newly created Digital Safety Commission of Canada (or the "Digital Safety and Data Protection Commission of Canada" under Bill C-36), which would be granted broad oversight and enforcement powers, not only in the online area, but also in the privacy and data protection area.

The DSC may receive complaints from individuals regarding harmful content, conduct hearings and inspections, and issue orders requiring platforms to make certain content inaccessible. It can also request access to relevant data and records in order to verify compliance. In addition to complaints, the regime provides for a "commentary"

mechanism allowing individuals to make submissions regarding a platform's compliance measures.

Bill C-34 is supported by a sanctions framework. Administrative monetary penalties (AMPs) may reach the greater of $10 million or 3 per cent of global revenue, with the amount taking into account factors such as the nature and scope of the violation, the operator's history of compliance, and any benefit derived from the violation. Penal sanctions may reach the greater of $20 million or 5 per cent of global revenue. These provisions are clearly intended to ensure that the regime has a meaningful deterrent effect, particularly for large multinational technology companies.

Uncertainties and open questions

Bill C-34 raises important questions regarding its practical implementation. A defining feature is the extent to which key obligations are left to be specified in future regulations: numerous provisions explicitly require operators to implement "any measures that are provided for by regulations." As well, several central elements, such as the scope of regulated services, the nature of age-verification mechanisms, and the specific standards applicable to chatbot behaviour, remain to be determined. This structure is reminiscent of the previously proposed *Artificial Intelligence and Data Act* (AIDA), which similarly relied on an extensive regulatory framework to operationalize broad legislative principles.

While reliance on future regulations introduces a degree of uncertainty for businesses, Bill C-34 is not final. There will be a second and third reading in the House of Commons, and consultation opportunities once regulations are proposed; we will continue to monitor and report on these developments.

Bill C-34 must also be understood within the broader context of the federal government's evolving digital policy, including its recently released national AI for All strategy. As discussed in BLG's recent Insight, Canada's new AI for All strategy: A business outlook on AI governance, adoption, and data sovereignty (June 9, 2026), the government has signalled a move toward establishing expectations around the development and deployment of trusted and compliant AI systems, relying on a combination of legislation and future regulatory development.

AI for All's first pillar (Pillar 1—Protecting Canadians and safeguarding our democracy**)** is now under construction with Bill C-34, as well as the very fresh privacy reform, *An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts* (Bill C-36), which was just introduced on June 15, 2026 (publication in progress).

With respect to the timeline for implementation, the adoption of detailed regulations may take significant time, although a stable parliamentary majority could accelerate this process. In the meantime, companies must operate in an environment characterized by evolving expectations and limited regulatory clarity.

What businesses should pay attention to ahead of the Safe Social Media Act

Organizations should begin mapping whether their services could become “regulated services” once thresholds and exemptions are prescribed. They should also start reviewing what happens behind the scenes of their operations, either to plan for the drafting of a potential digital safety plan, if applicable, or to review the agreements in place between them and regulated services, from a liability and reputational risk perspective.

Organizations should also evaluate existing risk-mitigation measures, including content moderation processes, transparency practices, and safety-by-design features. Particular attention should be given to AI systems, especially those capable of interacting directly with users, as these will be subject to heightened scrutiny.

Given that Bill C-34’s key compliance requirements will depend on forthcoming regulations, to accommodate for the significant uncertainty in determining the precise scope of their obligations, a proactive and flexible approach focused on governance and risk assessment will be essential. At this stage, the full operational impact of the regime will only become clear as Bill C-34 progresses through the legislative process.

The authors would like to thank Sirine Abdi, student-at-law, for her contributions to this article.

Footnote

[1] Notably, Bill C-36 (introduced days after C-34) renamed this body the Digital Safety and Data Protection Commission of Canada.

By

Claire Feltrin, Candice Hévin

Expertise

Information Technology, Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Government & Public Sector, Artificial Intelligence (AI), Technology

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749