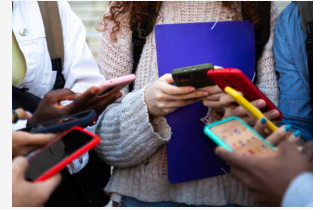


Bill C-34 at a glance: Canada's new Digital Safety Act

JUNE 11, 2026 11 MIN READ



Related Expertise

- [Privacy and Data Management](#)
- [Technology](#)

Authors: [John Salloum](#), [Sam Ip](#), [Maryna Polataiko](#), [François Joli-Coeur](#), [Tina Saban](#), CIPP/C

Key Takeaways

- Bill C-34 would enact a new *Digital Safety Act* (DSA) that covers three “regulated services”: social media, chatbot and online services.
- Duties across operators include duties to protect children, to act responsibly and to be transparent.
- Child-protection measures would include safety-by-design features and age-based restrictions.
- Social media operators would be required to take down child sexual abuse material (CSAM) and non-consensually distributed intimate images (NCDII) within 24-hours.
- The DSA would be among the first Canadian statutes to impose direct safety duties on operators of AI “chatbot services.”
- Administrative Monetary Penalties (AMPs) up to the greater of \$10 million or 3% of gross global revenue, and offences carry the potential for the greater of up to \$20 million or 5%.

The Government of Canada has introduced a comprehensive legal framework intended to govern online safety, reduce harms resulting from online content, and establish transparency and accountability requirements for operators of regulated services such as social media sites, chatbots and other online services. Bill C-34, the *Safe Social Media Act*, creates two new statutes: the *Digital Safety Act* (the DSA or the Act), which imposes duties on the operators of regulated services, and the *Digital Safety Commission of Canada Act*, which establishes the regulator that administers and enforces those duties.

Regulated social media, chatbot and online services

The Act's duties apply to “regulated services.” A service is generally “regulated” when it falls within a defined service type and either meets a user number threshold set by regulation or is designated as regulated by the Governor in Council. The Act's duties apply to three types of “regulated services”:

- **Social media services:** Websites or applications whose primary purpose is to facilitate communication among users by enabling them to access and share content. Social media services include adult content and live streaming services. Duties under the Act do not

apply to private messaging features on social media services.

- **Chatbot services:** Artificial intelligence (AI) systems that (i) communicate over the Internet; (ii) are publicly accessible via websites or applications; (iii) use natural language interfaces to provide adaptive, human-like responses in a conversational format; (iv) can simulate sustained human-like relationships through multiple interactions or sessions; and (v) generate content or responses that are not fully predetermined by system developers or operators. Chatbot services do not include AI systems that exclusively serve purposes specified in the regulations. Notably, the Act does not appear to include a standalone definition of “artificial intelligence system”.
- **Online services:** Websites or applications other than social media or chatbot services that allow users to interact with them. Online services do not include websites or applications whose primary purpose is either to facilitate the sale, listing or advertisement of goods or services, or to provide directories, search results, maps or navigation tools. Duties under the Act do not apply to private messaging features on online services. Online services must first fall within a “category of online services” established by the Governor in Council that pose a significant risk of harm to children in Canada in order to be “regulated”.

Telecommunications service providers that provide basic Internet connectivity would be exempt from the duties under the Act. Nothing in the Act would not require operators to proactively search for harmful content on their services, though regulations may require use of technological means to prevent child sexual abuse material (CSAM)^[1] from being uploaded.

Because the Act leaves key details to be determined by the regulations, the precise scope of application of the Act will not be known until draft regulations are circulated.

Digital Safety Commission of Canada

Bill C-34 proposes the Digital Safety Commission of Canada. The Commission’s mandate would be to promote online safety in Canada and contribute to the reduction of harms caused to persons in Canada as a result of harmful content online by, among other things, ensuring the administration and enforcement of the Act.

Harmful, pornographic and synthetic content

The Act would target seven categories of harmful content: NCDII,^[2] CSAM, content that induces a child to harm themselves, content used to bully a child, content that foments hatred, content that incites violence, and terrorism or violent extremism content. The Act would also establish requirements specific to pornographic content and synthetic content.

Baseline duties

The DSA would impose two baseline duties on all operators of regulated services: (1) a duty to protect children, including through safety-by-design features and age measures for pornographic content, and (2) a duty to be transparent through compliance record-keeping:

Duty to protect children

- safety-by-design features set out in regulations
- age verification or age estimation measures “adequate” to mitigate the risk of children’s exposure to pornographic content where an operator has “reasonable grounds” to suspect its service provides access to such content
- any measures prescribed by regulations to mitigate the risk of children’s exposure to pornographic content

Duty to be transparent

- record-keeping necessary to determine compliance with duties under the Act

Social media duties

For operators of regulated social media services, the DSA would supplement both baseline duties — adding a minimum-age regime to the duty to protect children and digital safety plans to the duty to be transparent — and impose two additional duties: a duty to act responsibly through systems-based safety measures, and a duty to make NCDII and CSAM inaccessible:

Duty to protect children

- where a regulated social media service is designated by regulation as subject to minimum age requirements, age verification or age estimation measures “adequate” and “designed to prevent” persons under 16 from having accounts with, or being registered with, the service, along with any measures prescribed by regulations
- the Commission may exempt an operator that provides “adequate safeguards” for the protection of children

Duty to act responsibly

- measures “adequate” to mitigate the risk of users’ exposure to harmful content, and any measures to mitigate such risk as prescribed by regulations
- user guidelines setting out a standard of conduct regarding harmful content and describing the operator’s compliance measures
- tools enabling users to block other users and to “easily” report harmful content, with notice requirements for reporting and reported users
- “adequate” measures to label synthetic content that meets prescribed criteria where it is “reasonable” to do so, and any prescribed measures regarding synthetic content labelling
- labelling harmful content the operator has “reasonable grounds to believe” was artificially amplified through automated third-party programs
- an “easily identifiable” resource person with “easily accessible” contact information to receive users’ concerns, direct users to internal and external resources, and provide guidance on internal resources
- compliance with specific preservation and destruction requirements following take-downs of content that incites violence, or terrorism or violent extremism content

Duty to be transparent

- submission of a digital safety plan to the Commission that includes:

- volume, type and timing of harmful content moderation and user reports, child safety-by-design features and their effectiveness, age measures for pornographic content and minimum-age measures for under-16 registration, resources allocated to compliance, relevant research and mandatory child-exploitation reporting measures, together with an inventory of the electronic data used to prepare the plan
- criteria and processes, if any, for notifying the RCMP or another law enforcement agency of content giving rise to reasonable grounds to suspect a risk of death or serious bodily harm, with statistics on any such notifications made
- publication of the digital safety plan in an “accessible and easy-to-read format”

Duty to make certain content inaccessible

- 24-hour take-down requirement triggered by operators identifying or receiving reports about NCDII or CSAM, paired with due process requirements (i.e., notice and appeal processes)

Chatbot duties

For operators of regulated chatbot services, the DSA would supplement the baseline duty to be transparent with digital safety plans and impose one additional duty, a duty to act responsibly, including crisis-intervention and harmful-behaviour measures:

Duty to act responsibly

- measures “adequate” to mitigate the risk of communicating harmful content to a user, and any prescribed measures to mitigate such risk
- emergency measures that, where a user expresses suicidal ideation, an intention to self-harm, or an intention to commit an act that could cause death or serious bodily harm, immediately interrupt the interaction and direct the user to crisis intervention services that are appropriate, available at that moment, and permit interaction with a human being, along with any prescribed measures to address emergency situations
- measures “adequate” to mitigate the risk of the service engaging in harmful behaviour, and any prescribed measures to mitigate the risk of the service engaging in such behaviour, namely:
 - posing as a human being in a manner likely to lead users to mistake it for a human or otherwise being deceptive about being an AI system
 - posing as a licensed professional and giving advice that could reasonably be expected to be relied on
 - using “manipulative engagement techniques” to encourage emotional attachment that may encourage social withdrawal or disconnection from reality
 - encouraging self-harm, suicide or acts that could cause death or serious bodily harm and
 - any other prescribed behaviour
- publicly available, accessible and easy-to-use user guidelines describing measures to mitigate the communication of harmful content, address emergency situations and

mitigate harmful behaviour

- tools and processes enabling users to “easily” report the communication of harmful content, failure to address an emergency situation or engagement in harmful behaviour, with notice of receipt to the reporting user and
- an “easily identifiable” resource person with “easily accessible” contact information to receive users’ concerns, direct users to internal and external resources, and provide guidance on internal resources

Duty to be transparent

- submission of a digital safety plan to the Commission that includes:
 - risk assessments regarding the communication of harmful content and engagement in harmful behaviour, mitigation measures and their effectiveness, volume and type of user reports and resulting measures, child safety-by-design features and their effectiveness, age measures for pornographic content, resources allocated to compliance, relevant research and mandatory child-exploitation reporting measures, together with an inventory of the electronic data used to prepare the plan and
 - criteria and processes, if any, for notifying the RCMP or another law enforcement agency of content giving rise to reasonable grounds to suspect a risk of death or serious bodily harm, with statistics on any such notifications made
- publication of the digital safety plan in an “accessible and easy-to-read format”

Online services duties

For operators of regulated online services, the DSA would supplement the baseline duty to be transparent with digital safety plans.

Duty to be transparent

- submission of a digital safety plan to the Commission that includes:
 - child safety-by-design features and their effectiveness, age measures for pornographic content, resources allocated to compliance (including to automated decision-making), and mandatory child-exploitation reporting measures, together with an inventory of the electronic data used to prepare the plan and
 - criteria and processes, if any, for notifying the RCMP or another law enforcement agency of content giving rise to reasonable grounds to suspect a risk of death or serious bodily harm, with statistics on any such notifications made
- publication of the digital safety plan in an “accessible and easy-to-read format”

Access to inventories and electronic data

The Act would establish a researcher access regime, empowering the Commission to accredit persons whose primary purpose is research or education related to the Act’s purposes, grant them access to the inventories of electronic data included in operators’ digital safety plans, and order operators to give researchers identified in an accredited person’s request access to the data for related research projects. The Commission may publish a list of accredited persons and a description of the research projects for which it has made access orders.

Remedies

The Act would empower persons in Canada to:

- make submissions to the Commission respecting harmful content on a regulated service, harmful behaviour by a regulated chatbot service, or an operator's compliance with the Act and
- make complaints to the Commission that content on a regulated social media service is NCDII or CSAM and seek a take-down order

Administration and enforcement

The DSA would grant the Commission extensive enforcement powers, including to:

- investigate complaints by, among other things, summoning persons to give evidence on oath and produce records, and receiving evidence without regard to whether it would be admissible in a court of law
- hold hearings in connection with complaints relating to NCDII or CSAM, as well as any other matters relating to an operator's compliance with the Act
- enter any place for a purpose related to verifying compliance or preventing non-compliance If where authorized by a warrant under the Act and
- make compliance orders requiring operators to take, or refrain from taking, any measure to ensure compliance with the Act, where the Commission has reasonable grounds to believe that an operator is contravening or has contravened the Act

Under the Act, orders made by the Commission could be enforced by the Federal Court.

AMPs and offences

The DSA would also introduce significant penalties for operator non-compliance (subject to a due diligence defence):

- administrative monetary penalties of up to the greater of 3% of gross global revenue or \$10 million, for violations such as contraventions of the Act or the regulations or of an order of the Commission and
- fines of up to the greater of 5% of gross global revenue or \$20 million on indictment, and the greater of 4% or \$15 million on summary conviction, for offences such as contravening an order of the Commission or an undertaking, obstructing an inspector, or making false or misleading statements

Where an operator is part of an affiliated group, "gross global revenue" would mean the group's gross global revenue. The Commission could also publish notices of violations and undertakings, naming the applicable parties and require the named party to publish the notice itself.

Osler Online Harms Series: This Update is the fourth installment in Osler's Online Harms Series, tracking Canada's evolving framework for online safety, platform regulation and children's privacy. Read earlier installments: [Bill C-16: updates to Canada's federal child](#)

sexual abuse and exploitation material reporting regime (December 18, 2025) and Canada's new Online Harms Act (C-63): what you need to know (March 1, 2024).

^[1] The Act uses the term "content that sexually victimizes a child or revictimizes a survivor," commonly known as child sexual abuse material (CSAM).

^[2] The Act uses the term "intimate content communicated without consent," commonly known as non-consensually distributed intimate images (NCDII).