

— A Justice Centre Report —

— August 5, 2026

The Safe Social Media Act:

**A threat to our
privacy and
freedom of
expression**

Censorship, mandatory
ID for all, internet
controlled by government

Author: Nigel Hannaford



Justice Centre
for Constitutional Freedoms

We Defend
Freedom
in Canada

Abstract

The Justice Centre supports the goal of protecting children from online harms. Bill C-34, the *Safe Social Media Act*, pursues that goal through measures that unjustifiably limit *Charter* rights and freedoms. An under-16 social media ban will force every Canadian to provide ID or age-verification or both, violating the privacy rights of millions of adults and displacing parental authority. Vague duties to mitigate “harmful content” and to regulate AI chatbots will incentivize over-censorship and undermine freedom of expression. A new Digital Safety Commission, exercising sweeping and largely undefined powers without meaningful accountability to Parliament, will create new rules, order content removal, and impose severe penalties. Parliament should reject Bill C-34 and instead focus on alternative measures to mitigate harms to children online, including better enforcement of existing *Criminal Code* provisions that already protect children and adults from online harms.

Copyright and reprinting

Copyright © 2026 Justice Centre for Constitutional Freedoms.

Licensed under the Creative Commons [CC BY-NC-ND](https://creativecommons.org/licenses/by-nc-nd/4.0/). This license enables reusers to copy and distribute the material in any medium or format in unadapted form only, for noncommercial purposes only, and only so long as attribution is given to the creator.



Acknowledgements

We thank the thousands of Canadians who continue to support the Justice Centre with their donations. Their generosity empowers the Justice Centre to defend freedom in Canada and to shape public policy that respects *Charter* rights and freedoms.

Updates to this report

This is Version 1.0 of this report, which may be updated periodically.

Authorship

The primary author of this report is Nigel Hannaford, a veteran journalist and public policy analyst.

Contents

Executive summary	4
A social media ban for Canadians under age 16	7
<i>Charter</i> section 8 right to be secure against unreasonable search or seizure	9
<i>Charter</i> section 7 right to life, liberty, and security	10
<i>Charter</i> Section 2(b) freedom of expression	10
AI chatbot regulation and content moderation duties.....	11
Monitoring conversations and disclosure to police	12
Regulating AI chatbot outputs	13
The Digital Safety Commission: government surveillance of the internet	13
Composition and responsibilities.....	14
Rules yet to be written, without input from Parliament	14
Recommendations	15
Bibliography.....	16
Appendix A.....	18



Executive summary

The federal government's Bill C-34, the *Safe Social Media Act*, is presented as a measure to protect children from online harms. It would impose identity screening for all Canadians using social media, facilitate extensive monitoring of private AI conversations, and create a powerful new regulator with largely undefined authority to censor speech. These measures unjustifiably limit Canadians' rights to privacy, freedom of expression, and parental authority under the *Canadian Charter of Rights and Freedoms*.

Bill C-34 would:

- Require operators of pornography websites to implement “adequate” age-verification or age-estimation for access, and impose duties to make child sexual abuse material and non-consensual intimate images inaccessible
- Ban Canadians under 16 from having accounts on certain social media platforms, enforced through “adequate” age-verification and age-estimation measures
- Impose unspecified design, safety, monitoring, and crisis-intervention obligations on conversational AI chatbot services; and
- Assign broad, undefined powers to a new Digital Safety Commission of Canada, including the authority to interpret vague standards and impose severe penalties on non-compliant platforms.

Requiring robust age-verification for dedicated pornography websites is a targeted and defensible measure. The under-16 social media ban is not. Experience from other countries, including Australia's under-16 social media ban, shows that preventing minors from accessing regulated social media platforms requires screening all users.

Platforms in Australia have used facial age estimation, behavioural inference, and “optional” stronger checks including government-ID. Even so, most under-16s continued to use social media three months after the ban, and parental awareness of children's use declined for some groups.

An effective ban would almost certainly lead to requiring all Canadians to prove their identity when accessing social media for daily work, leisure, education, and exploration. This regime violates *Charter* section 8 privacy rights for millions of adults: compelling the surrender of highly personal identifying information as a condition of everyday online life constitutes illegal “search or seizure.” It is a blunt, population-wide measure aimed at children but imposed on everyone.

The same regime displaces parental authority. The Supreme Court has recognized that the *Charter* section 7 liberty interest includes a parent's interest in making fundamental decisions concerning the care and upbringing of their children. Any state interference with

this right must be carefully tailored, and not arbitrary. Bill C-34, however, imposes a uniform prohibition and verification system on all families, with no individualized assessment and no room for parents to decide that less restrictive methods are sufficient. A law that leaves most teens online while making many parents less informed undercuts both child protection and parental authority.

Bill C-34 also restricts freedom of expression under *Charter* section 2(b). Regulated social media platforms must implement “adequate” measures to mitigate the risk that users will be exposed to “harmful content,” including the vague category of content that “foments hatred.” Existing criminal and human rights laws already grapple with the meaning of “hatred,” and those standards are themselves contested. Bill C-34’s distinctive problem is that a new, unelected Commission – able to impose severe financial consequences – would have the power to interpret and enforce vague standards across social media.

Facing severe penalties, platforms will have incentives to over-remove legitimate expression of opinion by Canadians. Several of the most serious “harmful content” categories, particularly child sexual victimization and non-consensual intimate images, already overlap substantially with *Criminal Code* offences. Where the worst harms are already criminal, a parallel administrative regime with lower thresholds for protecting *Charter* rights and freedoms is hard to justify.

Bill C-34’s rules for AI chatbots require operators to monitor conversations for suicidal ideation, self-harm, or intent to cause serious harm. AI operators must interrupt those chats, and may report them to crisis services or police. Operators must create digital “safety plans” that disclose criteria for referring chats to the RCMP. Meeting that duty requires large-scale monitoring of private conversations. Users who know their chats may be scanned, interrupted, or handed to authorities will avoid sensitive and controversial topics. The bill also regulates chatbot outputs and “harmful behaviour,” with further categories left to future regulations. Unclear standards plus severe penalties will push companies toward sanitized models, and reduced access to information. Some companies will leave Canada.

The Digital Safety Commission (DSC) created by Bill C-34 will combine regulatory, investigative, adjudicative, and advocacy roles. It can compel testimony and documents; its inspectors can demand information without a warrant. Most critically, 50 consequential decisions – including which social media are covered, what age-verification methods are acceptable, and how vague standards are interpreted – are left to the Commission or Cabinet after the bill passes. Parliament is being asked to approve a new legal architecture without knowing what it will look like in practice. Annual reporting provides only minimal accountability. Judicial review exists in theory, but few ordinary Canadians can afford to challenge the Commission’s rules or penalties in court.

Bill C-34 therefore creates a framework that sacrifices *Charter*-protected privacy, expression, and parental authority for uncertain gains. Child protection is a legitimate objective. It does not require mandatory identity screening of the adult population, open-

ended duties to mitigate “hatred,” monitoring the AI conversations of all Canadians, or the transfer of core policy choices from Parliament to an unelected body with weak safeguards.

Existing *Criminal Code* prohibitions already address the most serious online harms involving children and non-consensual intimate images. Those laws should be enforced more effectively. Clearer civil accountability for platform design choices that foreseeably harm children, and targeted age-verification for pornography, are more tailored tools than population-wide verification and a new Commission with open-ended powers.

The Justice Centre urges Parliament to reject Bill C-34. Canadians should contact their Member of Parliament and demand that the protection of children be pursued through better enforcement of existing laws, and measures that respect *Charter* rights, parental authority, and parliamentary control over lawmaking.

A social media ban for Canadians under age 16

Bill C-34, the *Safe Social Media Act*, creates a legal duty on certain social media platforms to protect children and reduce users' exposure to online harms. Without input from Parliament, the federal Cabinet will decide which social media platforms (e.g., X, Facebook, YouTube, etcetera) will be affected.

Section 27 bans Canadians under age 16 from being able to have an account with, or be otherwise registered with, regulated social media platforms through age-verification or age-estimation measures.¹ Age-verification and age-estimation measures must be “effective,”² and collected information must be protected, limited to age-verification or age-estimation purposes, and destroyed once verification or estimation are completed.³

Section 28 allows Cabinet to impose additional regulations – to be created only *after* the passage of Bill C-34 – to ensure that Canadians under 16 cannot access regulated social media platforms. In effect, this gives Cabinet a blank cheque to add stricter rules post-passage of the bill, without Parliamentary scrutiny. Under section 29, a social media platform may be exempted from some requirements if the Digital Safety Commission is satisfied the platform already provides “adequate safeguards” for the protection of children.

Under section 32, regulated social media platforms must implement adequate measures to mitigate the risk that all social media users will be exposed to harmful content,⁴ almost all of which is already prohibited by the *Criminal Code*. Bill C-34 defines harmful content as:

- a) intimate content communicated without consent;
- b) content that sexually victimizes a child or revictimizes a survivor;
- c) content that induces a child to harm themselves;
- d) content used to bully a child;
- e) content that foments hatred;
- f) content that incites violence; and
- g) terrorism or violent extremism content⁵

Bill C-34 does not specify how age-verification or estimation will be accomplished. Common methods include:

¹ Bill C-34 empowers the federal Cabinet to decide (without input from Parliament) which social media will or will not be regulated under the *Safe Social Media Act*.

² Bill C-34, 1st Sess., 45th Parl., 2026, s. 22(2). <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>.

³ Bill C-34, 1st Sess., 45th Parl., 2026, s. 27(2)(c).

⁴ Bill C-34, 1st Sess., 45th Parl., 2026, s. 32(1).

⁵ Bill C-34, 1st Sess., 45th Parl., 2026, s. 2(1) (definition of “harmful content”).



- Requiring users to submit government-issued identification, banking information, or health records;
- Using government-operated digital ID systems;
- Capturing biometric data (such as facial recognition) to estimate age; or
- Inferring age from users' behaviour and activity patterns on the platform.

Any effective system will almost certainly require screening every Canadian who uses social media, not only those who appear to be under 16.

Australia's *Online Safety Act* came into effect in December 2025, banning minors under age 16 from holding accounts on social media platforms such as *X*, *TikTok*, *Facebook*, *Instagram*, *Snapchat*, and *Reddit*. Social media platforms have used a mix of age-assurance tools (including facial age-estimation and behavioural inference) and sometimes stronger checks. While 4.7 million ineligible accounts were deleted from these platforms, the ban still fell far short of its objective.

Australia's eSafety Commissioner reported in March 2026 that around seven in ten parents whose children had accounts before the ban said those children still had accounts on major platforms.⁶ The Commissioner found implementation inadequate and pressed platforms toward more robust and continuous measures, such as better inference models and escalation to more reliable checks (including bank-based or "optional" ID checks).⁷

A July 2026 update from the Commissioner found under-16s' social media use had only edged down from 85.9% to 81.5%.⁸ Parents' awareness of their children's use also declined for some cohorts, particularly girls and children aged 10 to 12.⁹

A regime that leaves most teens online while making some parents less aware of what their children are doing undercuts both child protection and parental authority.

⁶ eSafety Commissioner. "Social Media Minimum Age: Compliance Update." March 2026. <https://www.esafety.gov.au/sites/default/files/202603/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf>.

⁷ Australian law prohibits platforms from strictly requiring government-issued ID or a government digital ID; however this method may be offered if accompanied by a "reasonable alternative."

⁸ This update focused on the same reporting period but provided additional data. "Social media use" is different than "social media account."

⁹ eSafety Commissioner, "Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow-up," July 2026, <https://www.esafety.gov.au/sites/default/files/2026-07/Early-days-early-insights-SMMA-evaluation-three-months-July-2026.pdf>.

The *Charter* right to be secure against unreasonable search or seizure

Compelling individuals to provide government ID, facial images, or other biometric information constitutes search or seizure under section 8 of the *Charter*. In *Hunter v. Southam Inc.* (1984), the Supreme Court held that section 8 protects a reasonable expectation of privacy wherever it exists – including in personal data, devices, and communications – and that searches must be reasonable and, as a general rule, authorized in advance.¹⁰ In *R. v. Duarte* (1990), the Court held that secret electronic surveillance by the state violates section 8, and that government cannot circumvent that protection by relying on intermediaries to obtain information it could not legally access itself.¹¹ In *R. v. Spencer* (2014), the Court ruled that police require a warrant to obtain subscriber information from an internet service provider, even if the provider would disclose it voluntarily.¹² In *R. v. Marakah* (2017), the Court held that the sender of a text message retains a reasonable expectation of privacy even when the message is stored on another person’s device.¹³ A regime that requires millions of adults to surrender identifying or biometric data as a condition of using everyday social media is a broad, indiscriminate seizure imposed on every Canadian.

If Bill C-34 passes in its current form, it could entail government-issued documents or permanent biometric data (whatever the unelected and largely unaccountable Commission approves as “adequate”). *Charter* section 8 is violated by a broad, indiscriminate requirement on millions of adults to surrender highly sensitive identifying information in order to access the social media platforms they use every day for work, leisure, and exploration.

As currently written, Bill C-34 requires social media platforms to “provide for the protection of personal information that is collected for age-verification or age-estimation purposes until that information is destroyed.” Including this provision is an implicit recognition that compelled age-verification measures entail privacy risks to Canadians. It is a risk-mitigating measure – not a preventative one. Absent the disaster of a serious and irreversible privacy breach, nobody will know whether or not the private information was actually destroyed (or properly protected prior to its destruction).

¹⁰ *Hunter et al. v. Southam Inc.*, [1984] 2 SCR 145, 1984 CanLII 33 (SCC).

<https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Retrieved on 2026-06-18.

¹¹ *R. v. Duarte*, [1990] 1 S.C.R. 30, 1990 CanLII 150 (SCC). <https://canlii.ca/t/1fszz>. Retrieved on 2026-06-18.

¹² *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, 2014 CanLII 43 (SCC).

<https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html>. Retrieved on 2026-06-18.

¹³ *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, 2017 CanLII 59 (SCC).

<https://www.canlii.org/en/ca/scc/doc/2017/2017scc59/2017scc59.html>. Retrieved on 2026-06-18.



No company is entirely protected from data breaches. For example, despite having data-protection measures in place, Bell Canada has suffered four breaches since 2016, Rogers Communications has had three breaches since 2015, LifeLabs had one, and other examples abound.¹⁴

The *Charter* section 7 right to life, liberty, and security of the person

By imposing a blanket under-16 social media ban enforced through mandatory age-verification on every social media user, Bill C-34 places the federal government in the role of parent. In *B.(R.) v. Children's Aid Society of Metropolitan Toronto*,¹⁵ a majority of the Supreme Court held that the liberty interest protected by section 7 includes a parent's interest in making fundamental decisions concerning the care and upbringing of their children. While that interest is not absolute and must yield where a child's life or health is demonstrably and imminently at risk, the Court insisted that any state interference on this interest must be "carefully crafted, adaptable to a myriad of different situations and far from arbitrary."¹⁶

Bill C-34 meets none of those requirements. It imposes a uniform prohibition and surveillance regime on all Canadian families, regardless of the child's maturity, the parents' capacity, or the actual risks present in a particular household. There is no opportunity for a family to demonstrate that less restrictive measures are sufficient, such as parental controls, device restrictions, education, and closely supervised access to the internet.

This is the opposite of the carefully tailored, case-by-case intervention required by *B.(R.)*. Bill C-34 is a pre-emptive, population-wide displacement of parental authority, enforced through privacy-invasive technology that has not yet been established, while its necessity and effectiveness remain unproven. Parents who know their own children's vulnerabilities, developmental stage, and online habits are far better positioned to make these decisions than a distant federal regulator.

The *Charter* section 2(b) right to freedom of expression

Bill C-34 also fundamentally limits the freedom of children and teens under 16 to access information and to express themselves via social media. This violates freedom of expression as protected by section 2(b) of the *Charter*, which protects both the right to speak as well as the right to hear, read and receive information.

¹⁴ Corbado. "11 Biggest Data Breaches in Canada [2026]." April 14, 2025.

<https://www.corbado.com/blog/data-breaches-canada>.

15 B. (R.) v. Children's Aid Society of Metropolitan Toronto, [1995] 1 S.C.R. 315.

<https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1220/index.do>. Retrieved on 2026-07-18.

¹⁶ Ibid. at 383 (per La Forest J.).

Charter Section 2(b) is further violated by the broad duty on social media operators to mitigate the risk that users will be exposed to “harmful content,” which includes the vague and subjective category of material that “foments hatred.”¹⁷ Recent public controversies illustrate how easily this standard can capture legitimate opinion. Whether questioning the unsubstantiated narrative of murders at Indian residential schools¹⁸ should be called a hate crime, or the justice of a \$750,000 fine imposed on a Chilliwack school board trustee for criticizing the board’s policy of promoting transgender ideology to children,¹⁹ are two examples.

As written, Bill C-34 empowers the Digital Safety Commission to create, interpret and enforce standards, giving it effective power to deem certain viewpoints “harmful” and pressure platforms to suppress them. Facing massive fines for non-compliance, platforms will have strong incentives to over-remove or algorithmically downrank the legitimate expression of opinion. This chilling effect will inevitably restrict *Charter*-protected freedom of expression for all Canadians (of all ages) who use social media.

Furthermore, most of the “harmful content” categories of Bill C-34, particularly those involving child sexual victimization and non-consensual intimate images, are already prohibited by the *Criminal Code*. In a recent Toronto case, for example, a man was charged with 68 offences arising from alleged online child luring and exploitation across platforms including *Snapchat*, *Instagram*, and *Discord*, including child sexual abuse.²⁰ Where criminal law already prohibits the most serious harms, the additional restriction on freedom of expression is not easily justified as a “reasonable” limit on *Charter* rights and freedoms.²¹

AI chatbot regulation and content moderation duties

Bill C-34 regulates both inputs and outputs for Artificial Intelligence chatbots: what may be said to a chatbot, and what a chatbot may say in response.

¹⁷ Section 2 (3) “For greater certainty and for the purposes of the definition *content that foments hatred*, content does not express detestation or vilification solely because it expresses disdain or dislike or it discredits, humiliates, hurts or offends.”

¹⁸ National Post. “AFN chiefs want residential school denialism to be hate speech crime.” July 15, 2026. <https://nationalpost.com/news/residential-school-denialism-hate-speech-crime-afn-chiefs>.

¹⁹ The Epoch Times. “Former Trustee to Challenge \$750K Tribunal Fine Over Anti-SOGI Remarks in BC Supreme Court.” February 2026. <https://www.theepochtimes.com/world/former-trustee-to-challenge-750k-tribunal-fine-over-anti-sogi-remarks-in-bc-supreme-court-5989949>.

²⁰ CityNews. Toronto Police Service / news report: “Toronto man facing 68 online child exploitation charges with alleged victims in multiple countries.” July 29, 2026. <https://toronto.citynews.ca/2026/07/29/toronto-man-charged-online-child-exploitation/>.

²¹ Under *Charter* section 1, the onus is on government to justify “demonstrably” with cogent and persuasive evidence that its violation of a *Charter* right or freedom is reasonable in a “free and democratic society.”



The *Safe Social Media Act* defines a “chatbot service” as a publicly accessible artificial intelligence system that communicates over the internet and uses natural language to provide adaptive, human-like responses in a conversational format. Chatbot services must also be capable of simulating a sustained human-like relationship through multiple interactions or sessions. The Bill C-34 definition is broad enough to potentially capture services such as OpenAI’s ChatGPT, xAI’s Grok, and Google’s Gemini.

Bill C-34 regulates how AI companies manage chatbot conversations involving fantasies of violence. Presumably this is a response to the Tumbler Ridge school shooting in February 2026.

Monitoring conversations and disclosure to police

Increasingly, Canadians use AI chatbots not merely for conversation but for research, education, and discovery. The more Canadians rely on AI systems, the more consequential government control over chatbot outputs becomes.

Section 51 of the *Safe Social Media Act* will require regulated chatbot services to immediately interrupt chats where users express suicidal ideation, an intention to self-harm, or an intention to commit an act that could cause death or serious bodily harm to an individual.

Section 51 requires chatbot services to refer such conversations to “crises intervention services that are appropriate to the situation.” Bill C-34 provides no framework for understanding what “service” (the RCMP?) may be appropriate.

A system cannot reliably identify every problematic conversation without scrutinizing all conversations. Canadians will be watched when legitimately exploring history, politics, literature, terrorism, extremist ideologies, crime, and mental health issues. When Canadians know that their chats may be scanned and interrupted (and potentially handed over to police) they will lose their ability to search freely for information, and will often avoid sensitive topics altogether.

Regulated chatbot companies will also have to submit a “digital safety plan” to the Digital Safety Commission disclosing the service’s criteria and processes for escalating to the RCMP any chats where “there is a risk that an individual will commit an act that would cause death or serious bodily harm to another individual.”

This, in turn, may provide police with access to private communications they would otherwise require judicial authorization to obtain, contrary to Supreme Court of Canada rulings that individuals maintain a reasonable expectation of privacy in their electronic communications.²²

²² *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608.

Regulating AI chatbot outputs

Bill C-34 also regulates what chatbots may say to users.

Sections 49, 50, and 53 require regulated chatbot services to implement measures mitigating the risk of harming users. Harmful behaviour includes posing as a human being or as a medical, legal, or other licensed professional, manipulating users to form emotional attachments to the chatbot, and encouraging self-harm, suicide, or acts that could cause death or serious bodily harm to others. Importantly, section 53(e) extends that duty to “any other type of behaviour specified in the regulations.”²³ Those regulations do not yet exist.

What the federal Cabinet or the Digital Safety Commission determine in the future to be “any other type” of harmful chatbot output will have profound implications for Canadians’ access to information.

Section 53(e) boils down to “trust the government.” It empowers a future Commission to regulate an increasingly important gateway to information without placing clear limits on that Commission’s authority.

Faced with severe penalties and unclear obligations, AI companies will have powerful incentives to retain more, monitor more, disclose more, and implement increasingly cautious generative models. Alternatively, they may simply exit the Canadian market.

If Bill C-34 passes in its current form, the rational response for Canadians will be to assume their AI conversations are being monitored by AI companies or by police. The rational response for AI companies will be to err on the side of caution at the expense of Canadians’ autonomy, freedom of expression, access to information, and privacy.

The Digital Safety Commission: government surveillance of the internet

Bill C-34 would establish a new government body, the Digital Safety Commission of Canada, to enforce compliance with the *Digital Safety Act*. The Commission would exercise substantial control and censorship powers over social media platforms, AI chatbot services, age-verification and identity-verification systems, content-mitigation practices, and the design features used to protect children online.

²³ Bill C-34, 1st Sess., 45th Parl., 2026, ss. 49, 50 and 53. <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>.



Composition and responsibilities

Operators of social media services, chatbot services, and other online services to be regulated under Bill C-34 will be required to submit digital safety plans explaining their risk assessments, safeguards, compliance practices, and allocation of resources. The Commission will review this information to assess compliance, investigate possible violations, grant certain exemptions, issue orders, and impose monetary penalties.

When enforcing the *Safe Social Media Act*, the largely unaccountable Commission will assess whether measures adopted by companies are “adequate,” including measures intended to mitigate exposure to harmful content, restrict access based on age, and address harmful chatbot behaviour. The Commission will issue guidelines and make regulations that have the force of law. While the Commission must submit an annual report to Parliament, that reporting requirement provides only very limited accountability.

Bill C-34 would give the Commission many of the investigative and enforcement powers ordinarily associated with a court or major regulatory tribunal. Under section 73, the Commission itself may summon witnesses, compel them to give testimony under oath, and require the production of documents. Under section 80, an inspector appointed by the Commission may require any person in possession of a document or information to provide such for the purpose of verifying compliance. Neither power requires a warrant.

If the Commission believes that an operator of a regulated online service is violating the legislation, the Commission can order that company to take – or refrain from taking – measures necessary for compliance. The Commission’s orders can be registered with the Federal Court, and enforced as court orders. In theory, the Commission’s orders can be challenged in court, but most companies will not have the money required to start a very expensive legal process that will drag on for years.

Violating a provision of the *Safe Social Media Act* will result in penalties of up to the greater of \$10 million and three percent of the offender’s gross global revenue. These penalties create powerful incentives for regulated companies to interpret vague requirements in the most censorious manner possible, with little or no consideration given to the privacy rights and freedom of expression of Canadians.

Rules yet to be written, without input from Parliament

Ottawa University law professor Michael Geist estimates that approximately 50 consequential questions are left to future regulations or administrative decisions by the Commission or by the federal Cabinet.²⁴ These include user thresholds, regulated services,

²⁴ Michael Geist. “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.” Michael Geist (blog), June 11, 2026.
<https://www.michaelgeist.ca/2026/06/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/>.

age-assurance requirements, design features for children, additional measures addressing chatbot conduct, and numerous standards by which corporate compliance will be assessed.²⁵

In the context of a very large federal government whose annual spending exceeds \$500 billion per year,²⁶ Parliament will have limited practical influence over the detailed rules and enforcement decisions made under Bill C-34.

A more detailed summary of the Commission's deferred and as-yet-undefined powers, prepared by Professor Geist, is attached as an Appendix to this paper.²⁷

Recommendations

The Justice Centre recommends that Parliament:

1. **Reject Bill C-34** in its present form.
2. **Enforce existing *Criminal Code* prohibitions** more effectively rather than layering a parallel administrative regime that violates *Charter* rights and freedoms with the threat of enormous penalties.
3. **Preserve targeted age-verification for accessing pornography**, which is a narrower and more defensible measure than an under-16 ban on general social media platforms enforced through screening of all users.
4. **Explore civil-law tools** that would impose liability on companies that directly or indirectly facilitate access to pornography and other online harms, rather than expanding government control over the internet.
5. **Equip parents** with support tools, education, and family-level controls instead of a uniform federal prohibition and surveillance regime that treats every household the same.
6. **Keep core rules of online expression, privacy, and age assurance in the hands of elected legislators**, not under the control of a largely unaccountable government Commission.

Canadians should contact their Member of Parliament and demand that the protection of children be pursued through measures that respect freedom of expression, access to information, privacy, parental authority, and parliamentary control over lawmaking.

²⁵ Geist, "The Law to Be Named Later," supra note 24.

²⁶ Treasury Board of Canada Secretariat. 2025–26 Estimates. <https://www.canada.ca/en/treasury-board-secretariat/services/planned-government-spending/government-expenditure-plan-main-estimates/2025-26-estimates.html>.

²⁷ See Geist, "The Law to Be Named Later," supra note 24. A summary of deferred decisions is attached as Appendix A.



Bibliography

Legislation

Canada. Parliament. House of Commons. *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*. 45th Parliament, 1st Session. First reading, June 10, 2026.
<https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>.

Jurisprudence

B. (R.) v. Children's Aid Society of Metropolitan Toronto, [1995] 1 S.C.R. 315. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1220/index.do>. Retrieved on 2026-06-18.

Hunter et al. v. Southam Inc., [1984] 2 S.C.R. 145, 1984 CanLII 33 (SCC).
<https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Retrieved on 2026-06-18.

R. v. Duarte, [1990] 1 S.C.R. 30, 1990 CanLII 150 (SCC). <https://canlii.ca/t/1fszz>. Retrieved on 2026-06-18.

R. v. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608.
<https://www.canlii.org/en/ca/scc/doc/2017/2017scc59/2017scc59.html>. Retrieved on 2026-06-18.

R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212.
<https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html>. Retrieved on 2026-06-18.

Secondary sources

Geist, Michael. "The Commission: How Bill C-34 Creates an Internet Super-Regulator That Will Touch the Lives of Millions of Canadians." *Michael Geist* (blog), June 15, 2026.
<https://www.michaelgeist.ca/2026/06/thecommission/>.

CityNews. "Toronto man facing 68 online child exploitation charges with alleged victims in multiple countries." July 29, 2026. <https://toronto.citynews.ca/2026/07/29/toronto-man-charged-online-child-exploitation/>.

Corbado. "11 Biggest Data Breaches in Canada [2026]." April 14, 2025.
<https://www.corbado.com/blog/data-breaches-canada>.

eSafety Commissioner. "Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow-up." July 2026.
<https://www.esafety.gov.au/sites/default/files/2026-07/Early-days-early-insights-SMMA-evaluation-three-months-July-2026.pdf>.

eSafety Commissioner. "Social Media Minimum Age: Compliance Update." March 2026.
<https://www.esafety.gov.au/sites/default/files/202603/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf>.

The Epoch Times. “Former Trustee to Challenge \$750K Tribunal Fine Over Anti-SOGI Remarks in BC Supreme Court.” February 2026. <https://www.theepochtimes.com/world/former-trustee-to-challenge-750k-tribunal-fine-over-anti-sogi-remarks-in-bc-supreme-court-5989949>.

Geist, Michael. “The Commission: How Bill C-34 Creates an Internet Super-Regulator That Will Touch the Lives of Millions of Canadians.” Michael Geist (blog), June 15, 2026. <https://www.michaelgeist.ca/2026/06/thecommission/>.

Geist, Michael. “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.” Michael Geist (blog), June 11, 2026. <https://www.michaelgeist.ca/2026/06/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/>.

National Post. “AFN chiefs want residential school denialism to be hate speech crime.” July 15, 2026. <https://nationalpost.com/news/residential-school-denialism-hate-speech-crime-afn-chiefs>.

Additional cited government documents

Treasury Board of Canada Secretariat. 2025–26 Estimates. <https://www.canada.ca/en/treasury-board-secretariat/services/planned-government-spending/government-expenditure-plan-main-estimates/2025-26-estimates.html>.



Appendix A

BILL C-34 · THE SAFE SOCIAL MEDIA ACT

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

$$19 \text{ cabinet decision points in the Digital Safety Act} + 31 \text{ Commission regulation-making powers in s. 126(1)} = 50 \text{ key issues left to be decided after the bill becomes law}$$

Cabinet Decides

19 GOVERNOR IN COUNCIL DECISION POINTS

New categories of regulated online services	s. 5(1)
User thresholds: which social media services are regulated	s. 6(2)
Designating below-threshold social media services	s. 6(3)
User thresholds: which chatbot services are regulated	s. 7(2)
Designating below-threshold chatbot services	s. 7(3)
User thresholds: regulated online services	s. 8(2)
Designating below-threshold online services	s. 8(3)
Designating the responsible minister	s. 13
Requiring Commission hearings or reports on any matter	s. 19
Which services face the under-16 ban	s. 27(5)
Which services face prescribed under-16 measures	s. 28(3)
Criteria for exemptions from the under-16 ban	s. 29(2)
Enforcement mechanics: penalty factors, revenue, undertakings	s. 112
Cost-recovery charges to fund the Commission	s. 125(1)
AI systems excluded from the chatbot definition	s. 127(1)(a)
Defining "significant psychological or physical harm"	s. 127(1)(b)
Replacing the 24-hour takedown period (operator-identified)	s. 127(1)(c)
Replacing the 24-hour takedown period (user-flagged)	s. 127(1)(d)
Coming into force of the entire Act	s. 130

AND THAT'S NOT ALL

Not counted: seven more cabinet decisions under the Digital Safety Commission of Canada Act — appointing the members, designating the chair, fixing the head office and remuneration, and bringing both Acts into force.

Also not counted: the Commission's four guideline powers (ss. 16, 17, 24, 30), its rules of procedure, and its case-by-case adequacy determinations, exemption rulings, and orders.

The Commission Decides

31 HEADS OF REGULATION-MAKING POWER · S. 126(1)

Information required for user-threshold determinations	(a)
Child-protection design features and parental controls	(b)
Adequate age verification requirements	(c)
Measures limiting children's exposure to pornography	(d)
Record-keeping scope and retention	(e)
Measures preventing under-16 accounts	(f)
Factors for adequacy assessments	(g)
Additional adequacy and complaint-screening factors	(h)
Mandated mitigation measures (incl. upload prevention)	(i)
User guidelines	(j)
User blocking tools	(k)
Flagging tools and processes	(l)
Synthetic content labelling criteria	(m)
Bot-amplified content labelling	(n)
The mandatory resource person role	(o)
Preserving removed terrorism and incitement content	(p)
Digital safety plans: timing and reporting period	(q)
Digital safety plans: required information	(r)
Digital safety plans: additional information	(s)
Digital safety plans: publication	(t)
Takedown, representations, and reconsideration process	(u)
New types of prohibited chatbot harmful behaviour	(v)
Electronic data inventories in chatbot safety plans	(w)
Researcher accreditation	(x)
Researcher access to data inventories	(y)
Researcher data access requests	(z)
Data access conditions: privacy, IP, security	(z.1)
Revoking or amending data access orders	(z.2)
Complaint case management	(z.3)
Operator duties after Commission orders	(z.4)
Publication of violation notices by violators	(z.5)

Source: Bill C-34, the Safe Social Media Act (Digital Safety Act, enacted by s. 2)

michaelgeist.ca