



RIGHT GOAL, WRONG EXECUTION:

Privacy, Age Verification and Gaps in **Bill C-34**

A policy assessment of Canada's
proposed online harms bill

An OpenMedia White Paper

Authored by: Elruma Dixon & Abde Amr

SEPTEMBER 2026

openmedia.org





OpenMedia is a grassroots community of 230,000 people in Canada that work together for an open, accessible and surveillance-free Internet. We work as a civic engagement platform that educates, engages, and empowers Internet users to advance democracy and digital rights across North America.

For more information, visit openmedia.org.

You can also find us on these social media platforms.

Bluesky | [@openmedia.org](https://bsky.app/profile/openmedia.org)

Mastodon | [@OpenMediaOrg](https://mastodon.social/@OpenMediaOrg)

Instagram | [@openmediaorg](https://www.instagram.com/openmediaorg)

LinkedIn | [OpenMedia.org](https://www.linkedin.com/company/OpenMedia.org)

Our Team

Matt Hatfield | Executive Director

Jenna Fung | Policy Engagement Manager

Elruma Dixon | OpenMedia Summer Fellow 2026

Abde Amr | OpenMedia Summer Fellow 2026

Table of Contents

Executive summary	4
Introduction and Background	5
1. A Rights-Based Approach to Online Child Safety	7
2. The Under-16 Account Restriction: Age Assurance, Privacy, Evidence & Alternatives	8
2.1 Age Assurance and Privacy	8
2.2 Evidence Behind Social Media Account Restrictions	10
2.3 The “Adequate Safeguards” Exemption	11
3. Other Gaps in Bill C-34	12
3.1 User Count Thresholds and Measurements	12
3.2 Adult Content Age-Verification Duty	14
3.3 AI Chatbot Duties	15
3.4 Mixed-Function Services and Private Messaging	16
Conclusion	17
References	18

Executive summary

- **A new online framework.** Bill C-34, the *Safe Social Media Act*, introduced on June 10, 2026, is Canada's latest attempt to regulate online harms through new obligations for social media services, chatbot services, and other online services. Among its most consequential provisions is an account restriction for users under 16 on social media services specified by regulation, unless an operator receives an exemption from a new regulator, the Digital Safety Commission.
- **Greater operator responsibility.** The bill rightly shifts greater responsibility for online safety toward operators of regulated services. It introduces child-protection and transparency requirements, tailored duties for social media and chatbot services, and a process requiring regulated social media services to make content that sexually victimizes a child or revictimizes a survivor, and intimate content communicated without consent, inaccessible in Canada, generally within 24 hours.
- **A rights-based approach.** Children should be treated as rights-holders in online safety policy. Bill C-34 should account for their evolving capacities and provide meaningful opportunities for young people to participate in decisions affecting their digital lives.
- **Rethinking the under-16 restriction.** The account restriction and its “adequate safeguards” exemption raise questions about privacy, access, effectiveness and how the framework will operate in practice, while early evidence from Australia illustrates practical enforcement challenges. OpenMedia recommends replacing the restriction with stronger content-neutral, safety-by-design requirements targeting harmful or manipulative features and systems, including autoplay, infinite scroll and engagement-maximizing recommendation systems.
- **Other critical gaps remain.** Important questions remain about user-count thresholds, the reach of the separate adult-content age-assurance duty, aspects of the chatbot regime left to future regulation, and the treatment of private messaging on mixed-function services. Digital policy expert Michael Geist has identified 50 key issues left to future decision-making by the Governor in Council and the Digital Safety Commission.
- **Getting the execution right.** Bill C-34's overarching goal of making online spaces safer is one we support. The question is whether its current mechanisms achieve that goal while protecting privacy, access and digital rights. With the bill still before Parliament, there remains an opportunity to strengthen the framework and get those choices right before it becomes law.

Introduction and Background

The Government of Canada has introduced [Bill C-34, the Safe Social Media Act](#), a successor to the previous Parliament's unpassed [Bill C-63, the Online Harms Act](#). Bill C-34 received its First Reading in the House of Commons on [June 10, 2026](#), and proposes to regulate social media services, chatbot services, and other online services under a proposed *Digital Safety Act*, overseen by a new *Digital Safety Commission of Canada*. With Bill C-34 still before Parliament, there is an opportunity to address these concerns before the framework is finalized. Bill C-34 establishes significant new responsibilities for operators of regulated services and has received support from organizations such as the [Canadian Medical Association](#), [Canadian Centre for Child Protection](#), and grassroots advocacy group, [Unplugged](#), which are optimistic about its possible outcomes.

At the same time, civil society organizations including [OpenMedia](#) and the [Canadian Civil Liberties Association](#) have raised a number of concerns about the bill's implications for privacy, freedom of expression and access to online spaces. Questions regarding the under-16 account restrictions' compatibility with Charter rights have also been raised by [Michael Geist](#), [Michael Karanicolas](#), an associate law professor at Dalhousie University's Schulich School of Law, and civil liberties experts [Tamir Israel](#) and [James Turk](#). At its core, the legislation rightly shifts responsibility for online safety away from parents and users, and towards operators of regulated services. All regulated services are subject to child-protection and transparency requirements, while additional duties apply depending on the type of regulated service. For regulated social media services, these include requirements to mitigate users' risk of exposure to seven specific categories of harmful content. The bill also establishes age-appropriate design requirements and allows operators of regulated social media services to seek an exemption from the under-16 account restriction if they can demonstrate "adequate safeguards" for children. A dedicated oversight body armed with the power to impose financial penalties would enforce these rules.

The bill establishes [four main categories of duties](#), although their application varies depending on the type of regulated service:

1. **Duty to protect children:** Operators of regulated services are subject to child-protection requirements, including requirements concerning child protective design features that will be further specified by regulation. For specified regulated social media services, this includes age-verification or age-estimation measures designed to prevent users under the age of 16 from holding accounts, unless the service receives an exemption.
2. **Duty to act responsibly:** Operators of regulated social media services must assess and mitigate risks associated with seven categories of harmful content: 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 terrorism or violent extremism content.

3. **Duty to be transparent:** Operators of regulated services must comply with record-keeping requirements and submit Digital Safety Plans describing their compliance with the Act. Public versions of those plans must also be made available, subject to specified exceptions.
4. **Duty to make certain content inaccessible:** Regulated social media services must make content that sexually victimizes a child or revictimizes a survivor, and intimate content communicated without consent inaccessible in Canada, generally within 24 hours after it is reported, subject to the statutory process.

While many of these duties may advance online safety, the framework presents several operational and regulatory gaps. One major concern highlighted is the bill's requirement for specified regulated social media services to verify or estimate users' age to actively prevent individuals under 16 from holding accounts. As noted above, the bill allows exemptions for operators that can demonstrate "adequate safeguards" for children, although what constitutes "adequate safeguards" has yet to be defined. Concerns have also been raised about the [privacy risks](#) associated with potentially requiring a much broader group of users to provide sensitive personal information as part of the age-assurance process.

Beyond the under-16 social media restriction, Bill C-34 would also create a separate age-assurance requirement. Under [section 22\(1\)](#), operators that have "reasonable grounds to suspect" a regulated service provides access to pornographic content must use age verification or age estimation measures to reduce children's exposure to that content. Depending on how future regulations define which services are covered and how these rules operate, this requirement could extend beyond traditional adult websites to other regulated services that host or provide access to user-uploaded material.

Moreover, in a [direct response](#) to the tragic Tumbler Ridge shooting in February 2026 in British Columbia, where an AI chatbot functioned as an unmonitored "[trusted confidant](#)" to the shooter, the bill introduces new important duties for chatbots. Operators of these services would be subject to a tailored Duty to Act Responsibly. Operators would be required to take measures to reduce the risk that their chatbots communicate harmful content or engage in specified harmful behaviours, including misleading users into believing they are interacting with a human, posing as a licensed professional and giving advice based on that deception, and using manipulative engagement techniques that may encourage harmful emotional attachment or social withdrawal. As part of this duty, operators must also implement measures for specified crisis situations that cause the chatbot to interrupt the interaction and direct the user to an appropriate and available crisis-intervention service where they can interact with a human.

Taken together, Bill C-34 marks a significant shift in how Canada approaches online safety by placing greater responsibility on operators of regulated services. Many of its measures could make online spaces safer, particularly for young people. Nonetheless, important questions remain about how some of these requirements will work in practice, particularly where measures

intended to improve safety may also affect privacy, access to online spaces and other digital rights.

1. A Rights-Based Approach to Online Child Safety

Children's rights do not just disappear when they go online. The [UN Committee on the Rights of the Child's General Comment No. 25 \(2021\)](#) recognizes that protecting children in digital environments must go hand in hand with respecting their rights, which includes their ability to access information, participate and express themselves. It also emphasizes the principle of evolving capacities, thus recognizing that children's needs and abilities change as they develop.

This approach is particularly relevant to Bill C-34's proposed under-16 account restriction. While digital spaces can expose children and youth to serious harms, they are also important spaces for learning, community building, accessing resources as well as self-expression. A framework intended to protect young people therefore has to account for both realities.

That balance also requires recognizing that children are not a single, uniform category. The risks, needs and capacities of a seven-year-old are not the same as those of a fifteen-year-old, for example. Yet, Bill C-34's under-16 account restriction applies a single age threshold across those differences. In doing so, it leaves little room to account for young people's evolving capacities as they develop. A rights-based approach would instead consider whether a blanket restriction adequately accounts for those evolving capacities and whether the risks young people face could be addressed through less restrictive protections that preserve their ability to participate in digital life.

Consistent with this approach, UNICEF Canada in its [June 10, 2026 statement](#), which welcomed Bill C-34's introduction as an important step towards protecting children online, nevertheless argued that the duties to protect children, act responsibly and make certain content inaccessible should be accompanied by a duty to consult young people. It also called for young people to remain involved as Bill C-34's framework is implemented and reviewed. Their participation matters because many of its details will be determined through regulations, Commission guidance and other implementation decisions. Young people should have a role in shaping those choices rather than being consulted only after the central rules have been established.

The recommendations throughout this paper therefore build from the principles that protections should respond to risk without unnecessarily restricting participation, and young people should have a meaningful role in shaping the rules that govern their digital lives.

POLICY RECOMMENDATION #1

Adopt a rights-based, evolving capacities approach to online child safety and give young people a real, funded and ongoing role in shaping the rules that affect them. The government and Digital Safety Commission should establish an ongoing youth-advisory mechanism and consult young people when developing and reviewing child-safety regulations, guidance and major implementation policies. That participation should include young people of different ages and backgrounds and should be structured to meaningfully inform decisions that affect their digital environments.

2. The Under-16 Account Restriction: Age Assurance, Privacy, Evidence & Alternatives

Bill C-34's proposed under-16 account restriction represents one of the most consequential elements of its approach to child safety. Although it is intended to reduce young people's exposure to online harms, enforcing the restriction requires some means of distinguishing users under 16 from those aged 16 and over. This raises questions about the privacy and access implications of age assurance, as well as whether exclusion is necessary where some of the underlying risks can instead be addressed through the design and operation of online services.

This section first considers those implications, then examines the early evidence on how minimum-age restrictions operate in practice and, finally, Bill C-34's "adequate safeguards" exemption as an alternative to the account restriction.

2.1 Age Assurance and Privacy

An under-16 account restriction requires a mechanism for distinguishing users who are under 16 from those who are not. This creates an immediate tension between Bill C-34's child-safety objective and the privacy implications of the mechanism used to enforce it.

Section 27(1) requires operators of specified regulated social media services to implement adequate age-verification or age-estimation measures designed to prevent people under 16 from holding accounts or otherwise registering with the service. Importantly, the obligation does not automatically apply to every regulated social media service. The Governor in Council must specify by regulation the services or classes of services to which it applies. The bill also builds privacy safeguards into the assessment of whether those measures are adequate, including restrictions on using personal information for unrelated purposes and requirements concerning its protection and destruction after the age-assurance process.

These are important safeguards. However, widespread age assurance still raises two separate questions.

The first is whether age assurance is necessary to achieve the safety objective at all. The risks Bill C-34 seeks to address are shaped in part by the systems and features built into online services. The bill already provides for child-protective design requirements that can address features and systems contributing to those risks. Safety-by-design measures can target those systems directly without requiring users to establish or have their age estimated. Greater reliance on those protections could, in turn, reduce the need to extend age-assurance processes to people who are not themselves subject to the under-16 account restriction.

In fact, this approach is consistent with the [guidance](#) from the Office of the Privacy Commissioner of Canada (OPC). The OPC recognizes that age assurance can play a role in protecting children online, but warns against its use as a default requirement for accessing the Internet. Its guidance advises organizations to first determine whether there is a need to differentiate users by age and, where appropriate, consider reasonable alternatives to age assurance that could address the potential harm.

Even where age assurance is used, a second question remains: whether the privacy safeguards surrounding it will be sufficient in practice. As discussed earlier, age assurance may extend to users who are not themselves subject to the under-16 account restriction. Its privacy implications may therefore extend to those users as well.

The privacy implications will also depend heavily on the methods used and the entities involved in carrying them out. Depending on the system, establishing or estimating a user's age may involve processing identity information, facial images or other personal information. Operators may also rely on third-party age-assurance providers, which raises additional questions about how restrictions on collection, use, retention and destruction will operate across verification systems that are outsourced. As Law professor [Robert Diab](#) has argued, requiring information to be destroyed after verification does not, on its own, resolve all of the privacy risks that can arise from the age-assurance process.

These risks also make it important to distinguish between establishing privacy requirements and ensuring that age-assurance systems comply with them in practice. Even though Bill C-34 establishes requirements governing age-assurance information, those protections should be accompanied by mechanisms capable of demonstrating that age-assurance systems comply with them in practice. The Office of the Privacy Commissioner has similarly identified independent review, including third-party audits or conformity assessments, as one means through which organizations can demonstrate compliance with privacy requirements when implementing age-assurance systems.

These concerns make the justification for widespread age assurance especially important. If an account restriction may require age-assurance processes extending beyond the young people it targets, there should be strong evidence that the restriction itself is likely to achieve its intended objective in practice.

2.2 Evidence Behind Social Media Account Restrictions

The empirical evidence for broad minimum-age social media restrictions is still developing, and Australia provides an early example of the implementation challenges involved with age-based social media restrictions.

An observational study published by [The BMJ](#) followed 436 Australian adolescents aged 12 to under 17 recruited before the country's under-16 social media restrictions took effect, with 408 participating in the follow-up approximately 3 months later. More than 85% of under-16 participants reported continuing to use platforms subject to the restrictions. The researchers cautioned that it was still too early to determine the policy's longer-term effects.

The study points to incomplete implementation by platforms and efforts by some adolescents to circumvent the restrictions as factors that may have contributed to these early results. The findings also show that, at least during the early implementation period, the account restriction did not prevent some young people from continuing to access restricted services in practice. At the same time, the researchers stressed that longer-term evaluation will be necessary to determine the policy's full effects.

For Bill C-34, the significance of these early findings is not that they settle the debate over minimum-age restrictions. Rather, they reinforce the need to ask whether an account restriction that requires age assurance across a broader group of users can reliably deliver sufficient benefits to justify the privacy and access implications associated with enforcing it.

POLICY RECOMMENDATION #2

Amend Bill C-34 to remove the under-16 account restriction. Instead, strengthen its content-neutral, safety-by-design requirements to address harmful and manipulative design features, including infinite scroll, autoplay and engagement-maximizing recommendation systems. This would place greater responsibility on operators to address risks through the design of their services without broadly excluding young people from online spaces.

POLICY RECOMMENDATION #3

Alternatively, if Parliament still retains the under-16 account restriction and its age-assurance requirements, the Digital Safety Commission should establish a framework for acceptable age-assurance methods in consultation with the Office of the Privacy Commissioner. Those

standards should address necessity, privacy, security, accuracy, accessibility and data minimization, with specific safeguards for biometric information where it is used. Future mandatory age-assurance requirements should not be introduced unless they are demonstrated to be necessary and proportionate to the identified risk and can be implemented in accordance with those standards.

Bill C-34 already requires a statutory review of the minimum-age framework. Under section 129, the Minister must cause a review of sections 27 to 29 and their operation no later than three years after that section comes into force. Building on that requirement, the framework should also be subject to regular, independent, evidence-based assessments of effectiveness under the under-16 account restriction and its impact on privacy and access. The results should be published and used to inform future decisions on whether the restrictions should be maintained, modified or repealed.

2.3 The “Adequate Safeguards” Exemption

Bill C-34 provides an [alternative](#) to the under-16 account restriction. Under [section 29\(1\)](#) of the proposed Digital Safety Act, an operator may apply to the Digital Safety Commission for an exemption where the Commission is satisfied that the social media service provides “adequate safeguards” for the protection of children. The Commission may also make an exemption subject to any conditions it considers appropriate.

In principle, this exemption could allow services with sufficient child-safety protections to continue serving users under 16 rather than excluding them altogether. However, how viable this alternative will be depends on what ultimately counts as an “adequate safeguard” and what a service must demonstrate to qualify.

The bill allows the Governor in Council to establish criteria that the Commission must consider when determining what safeguards are adequate, and it allows the Commission to issue guidelines on what constitutes adequate safeguards. Neither step is mandatory, and the bill itself does not otherwise specify what safeguards will be sufficient to qualify for an exemption.

This uncertainty also raises a related question: how will the exemption interact with Bill C-34’s existing child-protection obligations? Operators of regulated services are already required to implement child-protective design features that will be specified in regulations, and operators of regulated social media services are subject to additional obligations to mitigate the risk of users’ exposure to harmful content. Nonetheless, the bill does not specify how compliance with these existing obligations will factor into the Commission’s assessment of “adequate safeguards,” whether additional protections will be required to qualify for an exemption or how the sufficiency of those safeguards will be assessed.

These details will determine whether the exemption operates as a genuine alternative in practice or remain an uncertain exception whose availability operators cannot reasonably predict. If safety-by-design measures can provide adequate protection for children, the framework should give operators a clear path to demonstrate that protection rather than making exclusion the only predictable outcome.

If the under-16 account restrictions are to be retained, operators should know what protections they need to provide before the minimum-age requirements take effect. Equally, the public should be able to understand the principles underlying the Commission's decisions. Clear criteria can provide that certainty without requiring the disclosure of confidential commercial or security information.

More broadly, the uncertainty surrounding the exemption reflects a recurring issue with Bill C-34: several important questions about the scope and operation of the framework remain to be settled after the legislation is enacted.

POLICY RECOMMENDATION #4

Establish clear criteria for the “adequate safeguards” exemption before the under-16 account restriction takes effect. The criteria should explain how a service's design features, risk-mitigation measures and other child-protection safeguards will be assessed, whether additional protections beyond the bill's existing child-protection obligations are required, and how the Commission will determine whether those safeguards are sufficient to justify an exemption.

3. Other Gaps in Bill C-34

Beyond the under-16 account restriction, several other elements of Bill C-34 warrant closer attention. These include the rules determining which services fall within the regulatory framework, the separate age-assurance duty for pornographic content, the application of new duties to regulated chatbot services, and the treatment of services that combine private and public communication features.

In each case, the concern goes beyond the fact that further details will be established through regulation or guidance. The decisions left to implementation can affect who is regulated, when users may be required to undergo age assurance, what conduct falls within the chatbot rules and where the boundary between regulated public spaces and private communications is drawn. These choices will shape the practical reach of the legislation and its effects on users.

3.1 User Count Thresholds and Measurements

Before many of Bill C-34's duties can apply, it must be determined which services fall within the regulatory framework.

For social media services and chatbot services, [sections 6 and 7](#) provide two main routes into regulated status. A service may become regulated because it reaches a significant number of users prescribed by regulation. A service below that [threshold](#) may also be specifically designated by regulation if the statutory conditions relating to risk are met. Other online services are treated differently; [sections 5 and 8](#) require the relevant type of service first to fall within a category established by regulation before the threshold or designation mechanisms apply.

The numerical thresholds have not yet been established. Nor have the rules governing how users will be counted. These details are consequential because the threshold does more than determine the scale of an operator's obligations. It can determine whether a service enters the regulatory framework in the first place. A service counted just below the applicable threshold may fall outside obligations that apply to an otherwise comparable service counted just above it, unless it is separately designated. The methodology used to count users can therefore shape the practical reach of Bill C-34 alongside the numerical threshold itself.

Setting the number is only part of the issue. Who counts as a user? Over what period should users be counted? How should inactive, duplicate, suspended or deleted accounts be treated? Different approaches could determine whether a service falls above or below the regulatory threshold.

The European Union (EU)'s Digital Services Act (DSA) shows how these questions can arise in practice. Under the DSA, online platforms can be designated as Very Large Online Platforms (VLOPs) when they reach at least [45 million average monthly active recipients](#) in the EU and become subject to additional regulatory obligations. The designation of several adult content platforms has already led to disputes over how user numbers should be calculated and verified. Popular pornography website Pornhub, for example, initially [reported](#) a user count below the 45 million threshold, but the European Commission's investigation concluded that the platform met the threshold and designated it as a VLOP. More broadly, the Commission has confirmed that it [relied on third-party data providers](#) where necessary to determine whether services met the DSA threshold. Adult website Stripchat, meanwhile, was later [de-designated as a VLOP](#) after its average monthly active recipients fell below 45 million. These are cases that demonstrate the issue is not only where the threshold is set but also how platforms are determined to have reached it.

Bill C-34 anticipates further rules concerning user counts and gives the Commission authority to request prescribed information for the purpose of determining the number of users of a service. The eventual methodology should be sufficiently clear and verifiable for operators and the Commission to determine consistently whether the applicable threshold has been met.

POLICY RECOMMENDATION #5

Clearly define the user-count threshold and how it will be calculated, including who counts as a user, the period over which users are counted, and how inactive, suspended or deleted accounts are treated. The regulations should also require operators to provide sufficient information for the Digital Safety Commission to independently verify whether an applicable threshold has been met.

3.2 Adult Content Age-Verification Duty

The bill also creates a separate age-assurance duty. Under [section 22\(1\)](#), an operator that has “reasonable grounds to suspect” a regulated service provides access to pornographic content must implement age-verification or age estimation measures to reduce the risk of children being exposed to that content.

Protecting children from access to pornographic content is an important policy objective. Extending age assurance to these services, however, raises many of the same privacy concerns discussed earlier above, while creating a different implementation question: what circumstances are enough to give an operator “reasonable grounds to suspect” that its services provides access to such content?

Bill C-34 does not clearly answer that question. A service may prohibit pornographic content and actively remove it when detected, but still have users occasionally upload it. That is different from a service whose primary purpose is providing access to pornographic content.

Treating those situations alike could significantly expand the use of age assurance. If the presence of prohibited or incidental user-uploaded content is enough to trigger the duty across a general-purpose regulated service, users could face age checks on services that are not principally designed to provide access to adult content. Building on the privacy concerns discussed in [Section 2.1](#) of this paper, this would extend the privacy implications associated with age assurance into a broader range of online services.

The potential reach of the duty could also depend on the broader scope of the regulatory framework and this could be particularly difficult for general-purpose services that host user-generated content. Section 22 applies to regulated services, but the rules that will determine which online services fall within the broader regulatory framework, which includes the applicable categories of online services and the applicable user thresholds, remain to be established through regulation. Depending on how those rules are ultimately defined, the pool of services potentially subject to the duty could extend beyond traditional adult content services to include forums, image-sharing services, community discussion sites and other services that host user-generated content.

Without further clarity, services in these very different situations could face similar age-assurance obligations, which would extend the associated privacy implications to a much broader range of online spaces.

POLICY RECOMMENDATION #6

The regulatory framework should provide clear guidance on what constitutes “reasonable grounds to suspect” that a regulated service provides access to pornographic content and identify the factors that will be considered when assessing compliance, including the role of content moderation practices. The framework should also distinguish between services whose primary purpose is providing access to pornographic content and services that actively prohibit and remove such content, with compliance requirements that reflect those differences.

3.3 AI Chatbot Duties

Bill C-34 introduces [new safety obligations](#) for regulated chatbot services in light of growing concerns about AI systems that can appear increasingly human and persuasive. Operators would be required to reduce the risk that their chatbots communicate harmful content or engage in certain harmful behaviours. These include presenting themselves as human in a way that could lead users to mistake them for a person, posing as a licensed professional in specified circumstances, and using manipulative engagement techniques that may encourage harmful emotional attachment or social withdrawal.

In addition, the bill requires chatbots to intervene in specified crisis situations (such as when a user expresses an intention to harm themselves or seriously harm another person) by interrupting the interaction and directing the user to an appropriate and available crisis-intervention service where they can interact with a human.

Some elements of how these duties will operate are left to future regulations. [Sections 50, 52 and 54](#) allow regulations to add to the measures operators must take to meet the chatbot duties concerning harmful content, specified crisis situations and harmful behaviour. Section 53 also identifies the harmful behaviours operators must address and allows additional types of harmful behaviour to be specified by regulation. In this way, the bill establishes the basic duties but leaves important aspects of their implementation, and some of their future scope, to regulation.

The concern here is the nature of the decisions being delegated. These rules can shape what regulated chatbots are permitted to communicate and how they may interact with users, and section 53 allows the category of harmful behaviour itself to expand through regulation. Future rules could therefore affect the boundary between genuinely harmful chatbot conduct and [lawful conversations involving sensitive or controversial subjects](#).

Clear limits and contextual guidance become especially important where regulatory choices can affect that boundary.

The objective should be to regulate the harmful behaviour or interaction at issue rather than treating the subject of a conversation itself as harmful. Educational, journalistic, research and support-related discussions, for example, can involve sensitive or difficult subjects without creating the kinds of harms the legislation is intended to address. Clear guidance should focus on the behaviour and circumstances that create the relevant risk rather than the subject of a conversation alone.

POLICY RECOMMENDATION #7

Provide clear operational guidance on how the duties applying to regulated chatbot services should operate in practice, particularly when conversations involve sensitive subjects. The guidance should distinguish between conversations that present the risks the legislation is intended to address and legitimate educational, journalistic, research and support-related discussions, so that safeguards targeting specific harms do not result in unnecessarily broad restrictions on lawful conversations.

3.4 Mixed-Function Services and Private Messaging

A final implementation question concerns the boundary between private and public communications. [Section 11](#) excludes private messaging features of regulated social media and regulated online services from the duties that would otherwise apply to those services. It defines a private messaging feature by reference to communication with a limited number of users determined by the sender, rather than communication to a potentially unlimited number of users not determined by them. This is an important protection for private communications.

The distinction is relatively straightforward at either end of the spectrum. A private message between two users is clearly different from a public post available to an unlimited audience. The boundary becomes less obvious for services that combine different forms of communication within the same product. Direct messages, group chats, invite-only communities, larger community spaces and public feeds can all exist alongside one another.

How the private-messaging exclusion applies to these mixed-function services has implications for both privacy and the reach of Bill C-34's obligations. An interpretation that reaches too far into genuinely private or limited communications could weaken an important privacy safeguard. At the same time, the presence of a private-messaging feature should not determine how the bill applies to separate public-facing features offered by the same service.

The objective should therefore be to preserve a clear boundary around genuinely private communications while providing enough certainty about how the exclusion applies to features that sit between private messaging and fully public social media.

POLICY RECOMMENDATION #8

Provide clear guidance on how Bill C-34's private-messaging definition applies to mixed-function services, including direct messages, group chats, invite-only communities, larger community spaces and public feeds. The guidance should preserve strong protection for genuinely private communications while clarifying how the bill applies to more public-facing features offered by the same service.

Conclusion

Bill C-34 certainly sets the stage for a new regulatory framework for platform oversight in Canada. Its shift toward a more proactive model could rightly improve online safety and make platforms more accountable for the environments they create. However, in its current form, the bill also risks creating new challenges for privacy and digital rights.

The concern is not with the goal of protecting young people online, but with how that goal is achieved. Bill C-34 already requires platforms to introduce child-protective design requirements, but it also layers an under-16 account restriction and broader age-assurance requirements onto that framework. Relying too heavily on restricting access or requiring users to establish their age risks treating the symptoms of online harm without sufficiently addressing the platform features and systems that contribute to it.

The same principle applies to the bill's broader implementation. Decisions about which services are regulated, when age assurance is required, how chatbot duties develop and where private communications remain protected are not merely technical details. They will determine how far the framework reaches and how its obligations affect users in practice. Those decisions should be guided by clear rules, meaningful accountability and a commitment to addressing specific risks without unnecessarily expanding restrictions on users.

For that reason, the recommendations in this paper would move Bill C-34 toward a more rights-based and safety-by-design approach. This means placing greater responsibility on platforms to create safer online environments, protecting privacy when age assurance is considered, and ensuring that young people have a voice in decisions that affect their digital lives. It also means clearer rules around the scope and implementation of the framework will be essential so that its protections can operate effectively in practice.

Ultimately, Canada can pursue stronger online safety without sacrificing privacy and digital rights in the process. Bill C-34 gets much of the goal right. The challenge is ensuring that its execution gets the balance right too.

References

- Barnes, C., Hall, A., Mantach, S., Oldmeadow, C., Attia, J., Backholer, K., Williams, C., Tefera, Y., Kay, F., & Wolfenden, L. (2026). Assessing early effects of Australia's Social Media Minimum Age Act on adolescents' social media use: Observational study. *BMJ*, 393, e363695.
<https://doi.org/10.1136/bmj-2026-363695>
- 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, 1st Sess., 45th Parl., 2026 (first reading June 10, 2026).
- Black, R., Macek, A., & McDonald, M. (2026, June). *An overview of Canada's Safe Social Media Act*. DLA Piper.
<https://www.dlapiper.com/en-ca/insights/publications/2026/06/an-overview-of-canadas-safe-social-media-act>
- Bussi res McNicoll, A. (2026, June 11). *CCLA warns against risks to freedom of expression and privacy posed by Bill C-34, the Safe Social Media Act*. Canadian Civil Liberties Association.
<https://ccla.org/press-release/ccla-warns-against-risks-to-freedom-of-expression-and-privacy-posed-by-bill-c-34-the-safe-social-media-act/>
- Canadian Centre for Child Protection. (2026, June 10). Statement: New made-in-Canada online safety bill an important step towards safeguarding children online [Press release].
<https://www.protectchildren.ca/en/press-and-media/news-releases/2026/safe-social-media-act>
- Canadian Medical Association. (2026, June 10). Feds prioritize kids over big tech profits [Press release].
<https://www.cma.ca/about-us/press-room/feds-prioritize-kids-over-big-tech-profits-cma>
- Cheng, M. (2026, June 12). *Canada's move to rein in AI chatbots, spurred by school shooting, faces doubts over loopholes*. Reuters.
<https://www.reuters.com/legal/litigation/canadas-move-rein-ai-chatbots-spurred-by-school-shooting-faces-doubts-over-2026-06-12/>

- Diab, R. (2026, July 7). *Why safety measures for social media and AI in Bill C-34 cannot be made effective without harming privacy*. Robert Diab. <https://www.robertdiab.ca/posts/bill-c34-privacy/>
- European Commission. (2025, November 17). *Commission staff working document accompanying the document report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts* (SWD(2025) 368 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025SC0368>
- European Commission. (2026, August 31). *Supervision of the designated very large online platforms and search engines under DSA*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>
- Geist, M. (2026, June 11). *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. <https://www.michaelgeist.ca/2026/06/the-law-to-be-named-later-bill-c-34-punts-50-key-decisions-t-o-cabinet-and-a-digital-safety-commission-that-does-not-yet-exist/>
- Geist, M. (2026, July 16). *Why the government's plan for a social media ban in Bill C-34 is unconstitutional*. Michael Geist. <https://www.michaelgeist.ca/2026/07/why-the-governments-plan-for-a-social-media-ban-in-bill-c-34-is-unconstitutional/>
- Joannou, A. (2026, March 9). *Mother of wounded Maya Gebala sues OpenAI over mass shooting in Tumbler Ridge, B.C.* CTV News Vancouver. <https://www.ctvnews.ca/vancouver/article/family-sues-openai-over-mass-shooting-in-tumbler-ridge-bc/>
- Office of the Privacy Commissioner of Canada. (2026, May 4). *Age assurance – Policy note*. <https://www.priv.gc.ca/en/privacy-topics/age-assurance/aa-policy-note/>
- OpenMedia. (2024, March 9). *Explaining Bill C-63, The Online Harms Act: An OpenMedia FAQ*. <https://openmedia.org/article/item/explaining-bill-c-63-the-online-harms-act-an-openmedia-faq>

OpenMedia. (2026, June 10). *The Safe Social Media Act needs major fixes*. [Press release]

<https://openmedia.org/press/item/new-digital-safety-act-needs-major-fixes>

Pírková, E., & Fuchs, J. (2023, May 4). *VLOPs or flops: Is Big Tech dodging accountability in the EU?*

Access Now.

<https://www.accessnow.org/vlops-or-flops-is-big-tech-dodging-accountability-in-the-eu/>

Pozza, D. C., Stewart, J., Scott, K. E., Garriott, B., & Rigzadeh, S. (2026, March 24). *Injunction on California AADC partially vacated—Key provisions may take effect on April 2*. Wiley.

<https://www.wiley.law/alert-Injunction-on-California-AADC-Partially-Vacated-Key-Provisions-May-Take-Effect-on-April-2>

Salloum, J., Ip, S., Polataiko, M., Joli-Coeur, F., & Saban, T. (2026, June 11). *Bill C-34 at a glance:*

Canada's new Digital Safety Act. Osler, Hoskin & Harcourt LLP.

<https://www.osler.com/en/insights/updates/bill-c-34-at-a-glance-canadas-new-digital-safety-act/>

The Canadian Press. (2026, August 17). *Canada's social media ban for under-16s likely to face Charter challenge, experts say*. CP24.

<https://www.cp24.com/news/canada/2026/08/17/canadas-social-media-ban-for-under-16s-likely-to-face-charter-challenge-experts-say/>

UN Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations Human Rights Office of the High Commissioner.

<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

UNICEF Canada. (2026, June 10). *Canada's Safe Social Media Act is a promising start, but how will young people be consulted?* [Press release].

<https://www.unicef.ca/en/press-release/canadas-safe-social-media-act-promising-start-how-will-young-people-be-consulted>

Unplugged Canada. (2026). *National advocacy: Delay harmful social media access*.

<https://www.unpluggedcanada.com/national-advocacy>