



Bearing Institute

BearingInstitute.ca

Safe passage for good policy.

Delegating First, Defining Later: The Structural Risks of Bill C-34, the Safe Social Media Act

A Policy Analysis of Canada's Proposed Digital Safety Framework

Bearing Institute

June 2026 | Matthew Trenholm, MSc | Bearing Institute

Executive Summary

Bill C-34, the Safe Social Media Act, was introduced in the House of Commons on June 10, 2026, the third attempt in five years to legislate a federal online safety framework, following a 2021 consultation paper and Bill C-63, the Online Harms Act, which died on the order paper in two successive Parliaments. The bill enacts two new statutes: the Digital Safety Act, which sets out duties for operators of social media services, AI chatbot services, and certain online services, and the Digital Safety Commission of Canada Act, which creates the regulator that will administer those duties.

Bearing Institute does not oppose the objectives of Bill C-34. Protecting children online, requiring platforms to remove child sexual abuse material and non-consensually shared intimate images within 24 hours, and increasing platform transparency are not partisan goals. An Angus Reid Institute poll conducted in March 2026 found that three-quarters of Canadians support a full ban on social media accounts for those under 16.

The problem is not the objectives. The problem is the structure. The Digital Safety Act (the primary statute enacted by Bill C-34) establishes institutions, fixes penalty ceilings, and writes the number 16 into the statute — then leaves almost everything else to regulations that do not yet exist, written by a Commission that does not yet exist. University of Ottawa law professor Michael Geist has counted 19 distinct decision points reserved for the Governor in Council and a further 31 separate heads of regulation-making power handed to the Commission under section 126(1) alone — roughly 50 major questions Parliament is being asked to resolve by delegation rather than by vote.

Canada is not alone. The United Kingdom announced its own under-16 social media ban on June 15, 2026, five days after Bill C-34 was tabled. Australia's ban came into force in December 2025. The global experiment is accelerating. Its outcomes remain genuinely uncertain, and its unresolved tension — that verifying who is under 16 requires checking everyone — is one that no jurisdiction has yet solved.

This "delegate now, define later" structure raises four concerns this brief examines in detail: Parliament approves a framework whose real shape will be determined after the vote; the powers created will be available in identical form to every future government regardless of ideology; the penalties applied to vaguely defined "harmful content" categories will push AI chatbots and social media platforms to avoid entire categories of lawful but contested questions; and a law sold as protecting children under 16 necessarily requires verifying the age of every adult in Canada.

This brief identifies five structural problems in Bill C-34 that require amendment before it can become law consistent with its stated goals. It recommends five specific amendments, ready to be tabled, that would

preserve the bill's legitimate safety objectives while removing the provisions that create the greatest constitutional, privacy, and free-expression risks. On the harmful content question specifically, Bearing Institute recommends striking "foments hatred" and "incites violence" from the definition entirely — leaving the five remaining categories, which are precisely defined, legally tested, and command broad consensus, intact. On age verification, Bearing Institute recommends replacing the population-wide adult identity verification mechanism with device-based age verification, the parent-set, operating-system-level age check proposed by Jonathan Haidt in *The Anxious Generation*, supported by a complementary duty on platforms to provide effective parental control tools. This approach enforces the under-16 restriction without requiring a single adult to prove their identity online, which is both the more rights-protective path and closer to what a clear majority of Canadians say they prefer.

Part 1: The AI Chatbot Problem — What Happens When Nobody Knows Where the Line Is?

Begin with a question a Canadian teenager might put to an AI chatbot tonight — the kind of general-purpose assistant that millions of Canadians, including the under-16s this bill is built around, already use for homework help, research, and casual conversation:

"Why do some researchers disagree about outcomes from gender-transition treatment?"

"What are the arguments for and against Canada's current immigration levels?"

"Why are birth rates declining across most developed countries?"

"Can you explain the different positions in the Israeli-Palestinian conflict?"

"Why is affirmative action controversial?"

None of these questions is inherently hateful, violent, or unusual. They are the kind of questions a curious teenager, or a curious adult, might ask while trying to understand the world. Under Bill C-34, however, the operator of a regulated chatbot service answering them is not operating in a vacuum. Section 2(1) of the Digital Safety Act defines "harmful content" to include "content that foments hatred" and "content that incites violence," and section 49 imposes on every regulated chatbot service a duty to implement measures "adequate to mitigate the risk that the service will communicate harmful content to a user." The penalty for getting that wrong is the greater of \$10 million or 3 per cent of global revenue for a violation, rising to 5 per cent on indictment.

The statutory definitions matter here because they are broader than they might first appear. "Content that foments hatred" is defined as content expressing detestation or vilification of a person or group on a prohibited ground of discrimination and that, in context, is likely to foment such detestation. "Content that incites violence" is content that actively encourages or threatens physical violence and that, in context, could cause a person to act on it. Both definitions turn on context and likelihood — judgments difficult enough for courts applying them to a single piece of human speech after the fact, but that Bill C-34 now asks chatbot operators to make in real time across every output their systems generate for every user in Canada.

The bill includes one explicit legitimate purpose exclusion: section 2(6) exempts from the "terrorism or violent extremism content" definition any communication that has a legitimate purpose, including journalism, education, or art. No equivalent exclusion appears in the definitions of "foments hatred" or "incites violence." The only carve-out for the hatred category is the narrower section 2(3) clarification that content expressing mere disdain

or causing offence does not qualify. That clarification helps a human rights tribunal weighing a specific statement years after the fact. It does little to tell a chatbot operator where the line falls before the Commission has issued guidance on what “adequate” measures look like under section 50.

Greg Lukianoff — president of FIRE and co-author of *The Coddling of the American Mind*, a book that helped build the modern consensus that smartphones are harming children — nonetheless opposes age-verification mandates and vague harmful content duties on precisely this ground. Writing on June 15, 2026, Lukianoff noted that “if judges and lawyers have difficulty determining whether a particular statement counts as hatred, social media companies and AI companies concerned about facing fines will likely err on the side of censoring more expression.” The Canadian Constitution Foundation reaches the same conclusion from the bill’s text, warning that chatbots will “shy away from difficult truths or unpopular perspectives on topics ranging from immigration to gender identity.” Lukianoff’s position is significant precisely because he is not a social-media utopian: he is a child-safety advocate who still concludes that vague content duties create worse problems than they solve.

Bearing Institute Alert. The greatest threat to free expression in Bill C-34 may not be direct government censorship. It may be the regulatory incentive it creates for private platforms and AI systems to avoid entire categories of lawful, contested, but ordinary questions, rather than risk a multi-million-dollar penalty for guessing wrong about what a future Commission will consider “adequate.”

Source: Digital Safety Act, ss. 2(1), 2(3), 2(6), 49, 50, 88, 107 (Bill C-34, 45th Parliament, First Reading, parl.ca); Canadian Constitution Foundation, “Bill C-34, the Safe Social Media Act, Explained,” June 2026 (theccf.ca); Greg Lukianoff, “The online ‘safety’ trap,” Eternally Radical Idea, June 15, 2026 (eternallyradicalidea.com).

A Different, and More Defensible, Set of Chatbot Duties

It is important to be precise about what this critique does and does not cover. Bill C-34 also imposes a distinct set of chatbot duties under sections 51 to 54: a mandatory requirement to interrupt a conversation and direct users toward crisis intervention if they express suicidal ideation or an intention to harm themselves or others, and a duty to mitigate “harmful behaviour” including impersonating a human in a way likely to deceive, posing as a licensed professional, using manipulative engagement techniques to encourage harmful emotional dependency, and encouraging self-harm or suicide.

These duties respond to documented and growing harm. The parents of 16-year-old Adam Raine sued OpenAI in August 2025, alleging that ChatGPT acted as their son’s “suicide coach” in the months before his death by suicide. A separate wrongful-death suit against Character Technologies was permitted to proceed after a federal judge rejected the company’s argument that its chatbot outputs were protected speech. Closer to home, the February 2026 Tumbler Ridge Secondary School mass shooting in British Columbia, in which eight people were killed, prompted lawsuits alleging that OpenAI’s systems had flagged the shooter’s account for concerning activity months earlier, but that company leadership chose not to escalate the matter to authorities. Canada’s Minister of Artificial Intelligence subsequently summoned senior OpenAI staff to account for that decision.

Sections 51 through 54 are a reasonable legislative response to exactly this category of failure. The concern in this Part is narrower: the same chatbot framework that mandates crisis intervention also imports, without modification, two of those seven categories — “foments hatred” and “incites violence” — whose definitions turn on context, likelihood, and subjective assessments of detestation, making them unsuitable for a mandatory-removal and penalty regime applied to real-time AI outputs. Bearing Institute recommends striking both categories from section 2(1) entirely. The five remaining categories are sufficient, are legally precise, and should be retained.

Source: Digital Safety Act, ss. 2(1), 49, 51–54 (Bill C-34, 45th Parliament, First Reading, parl.ca); NBC News, “The family of teenager who died by suicide alleges OpenAI’s ChatGPT is to blame,” August 27, 2025; NPR, “Families sue OpenAI over Tumbler Ridge mass shooter’s use of ChatGPT,” April 29, 2026; BBC, “Canada summons OpenAI senior staff over Tumbler Ridge shooting,” 2026.

Part 2: The Delegate Now, Define Later Problem

This is the structural pattern at the heart of Bill C-34, and it is the genuinely new element in this brief. The Digital Safety Act establishes institutions, names a regulator, fixes penalty ceilings, and writes the number 16 into the statute. It then leaves almost every question about how the law will actually operate to be answered later, by regulations that do not exist yet, made either by the Governor in Council or by the Digital Safety Commission of Canada itself.

Michael Geist has tallied the scale of this delegation precisely: the Digital Safety Act contains 19 distinct decision points reserved for the Governor in Council, and a further 31 separate heads of regulation-making power are handed to the Commission under section 126(1) alone, a total of roughly 50 major issues left to be decided after the bill receives royal assent. That figure does not include the Commission's separate guideline-making powers, its case-by-case adequacy and exemption determinations, or the seven additional cabinet decisions required under the companion Digital Safety Commission of Canada Act simply to bring the Commission into existence, starting with appointing its members and chair. As Geist puts it, the Commission that will decide most of this "does not yet exist, has no members, no chair, no staff, and even no funding model," since the cost-recovery charges that will finance its operations are themselves left to future regulation under section 125.

This is not a criticism that every detail of a regulatory statute should be written into the bill itself; no legislature works that way, and some delegation is inevitable and appropriate. The concern is the proportion, and the centrality, of what has been delegated here. The table below sets out a representative sample of the questions Bill C-34 leaves open, drawn directly from the bill's text.

What the Bill Leaves Open	Statutory Provision	Who Decides, and When
Which social media services, chatbot services, and online services are "regulated" at all	ss. 6(2), 7(2), 8(2)	Governor in Council sets user-number thresholds and counting methodology by future regulation; until then, no service meets the definition
Which AI systems are exempt from being a "chatbot service"	ss. 2(7), 127(1)(a)	Governor in Council specifies exempt "purposes" by future regulation
Whether the under-16 minimum-age restriction applies to any given social media platform	ss. 27(1), 27(4)–(5)	Governor in Council designates specified services or classes of services by future regulation; the age of 16 is fixed in the Act, but its application is not
What counts as an "adequate" age-verification or age-estimation measure	ss. 22(2), 27(2)	Commission determines adequacy against criteria that include its own satisfaction that the measure is "effective," a term the Act does not define
What design features platforms must build to protect children	s. 21	Set out entirely in future regulations
Which online services beyond social media and chatbots are covered at all	s. 5	Governor in Council may establish "categories of online services" on the Commission's recommendation, following a Minister-directed analysis
What counts as an "adequate safeguard" enabling exemption from the under-16 ban	s. 29	Commission decides case by case, applying criteria the Governor in Council may, but need not yet, set by regulation
How the Commission itself will be funded	s. 125	Governor in Council sets cost-recovery charges by future regulation

Source: *Digital Safety Act*, ss. 2(7), 5–8, 21, 22, 27, 29, 125, 126–127 (Bill C-34, 45th Parliament, First Reading, [parl.ca](#)); 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,” [michaelgeist.ca](#), June 2026.

The Age-16 Illustration

The minimum-age provision is the clearest illustration of how this works in practice, because it is the headline of the bill and the provision the government has most emphasized. Section 27(1) provides that an operator must implement adequate age-verification or age-estimation measures “designed to prevent a person under the age of 16” from holding an account, but only “with respect to every regulated social media service specified by regulations made by the Governor in Council under subsection (5).” Subsection 27(4) removes any ambiguity: the obligation “applies only in respect of regulated social media services... specified in regulations.”

The number 16 is therefore in the statute. Whether the restriction applies to Instagram, TikTok, Snapchat, YouTube, Roblox, Discord, or any other service Canadians under 16 currently use is not. That is a future cabinet decision, made service by service or class by class, and section 27(5) provides no criteria in the bill itself to guide how that decision will be made. Section 29 then layers a further discretionary step on top: even for a platform that is designated, an operator can apply to the Commission for an exemption by demonstrating “adequate safeguards,” a term the Commission itself will define through guidelines under section 30.

None of this means the under-16 restriction is illusory, or that it will never apply to anything. It means that a person reading Bill C-34 today, including the Members of Parliament being asked to vote on it, cannot answer the question “which platforms will my 14-year-old be barred from?” The honest answer: that depends on regulations that have not been drafted, made by a Commission that does not yet exist, possibly after consulting criteria that the Governor in Council has not yet decided whether to set.

Bearing Institute Alert. Bill C-34 fixes the number 16 in the Digital Safety Act. It does not fix, anywhere in the bill, which platforms that number applies to, what “adequate” verification looks like, what “adequate safeguards” for an exemption look like, or which AI chatbots count as “chatbot services” at all. Those are the questions that will determine, in practice, what this law does, and Parliament is being asked to approve the framework before any of them are answered.

Source: *Digital Safety Act*, ss. 27, 29–30 (Bill C-34, 45th Parliament, First Reading, [parl.ca](#)); Michael Geist, “Everything All At Once: Bill C-34 Combines Platform Duties, a Kids’ Social Media Ban, AI Chatbot Regulation, and a Powerful Digital Safety Commission Into a Risky ‘Trust Us’ Bet,” [michaelgeist.ca](#), June 2026.

Part 3: The Future Government Problem

It would be easy, and wrong, to frame the concerns in Part 2 as being about this government in particular. That framing is not only unfair, but also the weaker version of the argument, because it invites the response that the reader either trusts the current government or does not, and the debate ends there. The stronger and more durable point is institutional: whatever discretion Parliament hands to the Governor in Council and the Digital Safety Commission of Canada in 2026 does not expire when this government leaves office. It becomes a standing feature of the Canadian regulatory state, available in identical form to whichever party or coalition holds power when the Commission eventually gets around to writing the rules that section 126 and 127 leave open.

A future government of one stripe could use a broadly worded “content that incites violence” standard, applied to chatbots and social media alike, against content from climate activists, labour organizers, or Indigenous rights advocates whose rhetoric a complainant characterizes as encouraging disruption. A future government of another stripe could apply the same standard, with the same vagueness, against vaccine skeptics, critics of

gender-identity policy, or opponents of current immigration levels. The mechanism does not care which of these is the target. It was not built with either in mind, and it does not need to be, because the vagueness is the feature that makes it usable against whichever group a future Commission, advised by whichever government appointed its members, decides is the priority.

Bearing Institute Alert. The occupants of government change. Regulatory powers, once granted, remain. The question for Parliament is not whether the government currently in office can be trusted with 50 undefined decision points. It is whether any future government, of any party, should inherit that discretion without Parliament ever having defined its limits.

This Is Not the First Bill C-34 to Do This

Bill numbers reset with each new Parliament, and by coincidence, the immediately preceding bill to carry the number C-34 followed the same structural pattern, in a completely unrelated policy area. In the 44th Parliament, Bill C-34, the National Security Review of Investments Modernization Act, amended the Investment Canada Act to give the Minister of Innovation, Science and Industry significantly expanded powers to review and condition foreign investments on national security grounds. It received royal assent on March 22, 2024.

As with the current Bill C-34, the substance of the new powers was left to regulations made after the fact. The amended Act allows the Minister to require mandatory pre-implementation notice for investments in “prescribed business activities,” and to extend national security reviews for “prescribed periods,” but neither the business activities nor the periods were defined in the bill itself. Legal commentary at the time noted that the sections dealing with these prescribed sensitive sectors could not be implemented until the regulations defining them were enacted, and that this was not expected to happen until well into 2025, more than a year after the bill became law. Parliament voted on the framework in 2024; the substance of which sectors of the Canadian economy would be subject to the new mandatory-filing regime was decided afterward, by cabinet, through a process Parliament did not vote on.

Two different Parliaments. Two completely different policy domains, foreign investment security and online child safety. Two different governing priorities. The same structural move: establish the power, fix the penalties, and define the scope later. Naming this as an emerging habit of Canadian federal legislative drafting, rather than relitigating the merits of either individual bill, is the point of this Part. If the pattern recurs across governments and across subject matters, the fix must be procedural and apply generally, not a one-off amendment to a single bill that the next “Bill C-something” will simply repeat under a different heading.

Source: National Security Review of Investments Modernization Act, S.C. 2024, c. 4 (Bill C-34, 44th Parliament, Royal Assent, [parl.ca](https://www.parl.ca)); Fasken, “The National Security Review of Investments Modernization Act Receives Royal Assent,” March 28, 2024; BD&P, “Protecting Canada’s National and Economic Security Interests: Bill C-34 — The National Security Review of Investments Modernization Act.”

Part 4: The Age Verification Paradox — Why Protecting Children Shouldn't Mean Surveilling Adults

Bill C-34 is being presented to Canadians as a law that protects children under 16. What is rarely stated plainly is its structural precondition: a platform cannot prevent a 14-year-old from holding an account without first determining the age of every person who tries to open or keep one. There is no technical workaround. Age-restricting children requires age-verifying adults. A law sold as a child-safety measure is, in its operational reality, a population-wide adult identity verification mandate.

That is not a minor implementation detail. It is the central design feature of the bill's most prominent provision, and it is one the government has not squarely defended. Sections 22(2) and 27(2) include data-minimization requirements — verification data must not be used for other purposes and must be destroyed once verification is complete — but these are administrative safeguards on a system whose existence is itself the problem. Whether the data is deleted promptly or not, every adult Canadian who wants to use a designated social media platform will first have to prove their age to that platform, to a third-party verification vendor, or to both. That is a permanent, structural change to the relationship between Canadians and their online public life.

The Polling the Government Cites Does Not Support This Approach

The March 2026 Angus Reid Institute poll that has been cited throughout public debate found that 75 per cent of Canadians support a full ban on social media accounts for those under 16. The same poll found that 72 per cent of respondents believe the responsibility for enforcing such restrictions should rest with parents, not government policy. That finding has received almost no attention in commentary on the bill. It should receive considerably more because it describes a majority position that Bill C-34 ignores entirely: Canadians support the goal and believe parents, not the state, should be the mechanism for achieving it.

Bill C-34 takes the opposite approach. It substitutes a government-mandated identity verification infrastructure for parental responsibility, requiring platforms to enforce an age restriction that a clear majority of Canadians think should be enforced by families. The government has not explained why the parental-tools approach favoured by that majority is insufficient, or why population-wide identity verification is a proportionate response to a problem that most Canadians think belongs in the home rather than in a regulatory framework.

What Population-Wide Age Verification Looks Like in Practice

Canada is not the first jurisdiction to attempt this. Australia's under-16 ban came into force on December 10, 2025. By mid-December, the eSafety Commissioner reported that 4.7 million under-16 accounts had been removed. Within weeks, reporting described children bypassing the restriction using VPNs, migrating to non-designated platforms, and defeating facial age-estimation checks with masks or by having older siblings complete the scan. The list of covered platforms has been revised multiple times since the law took effect. The list of exempt platforms has been revised multiple times. Neither list has stabilized.

What has stabilized is the privacy cost to adults. Every adult Australian who uses a designated platform has been required to demonstrate their age — through document upload, facial scan, or third-party verification — as a condition of continued access to services they previously used without restriction. In October 2025, Discord disclosed a breach that exposed the government-issued identification documents of roughly 70,000 users who had submitted them for age-verification purposes. Whatever destruction requirements exist on paper, the breach window between submission and deletion is real, the vendor relationships created by verification infrastructure are permanent, and the data flows established at initial rollout are difficult to dismantle after the fact.

Greg Lukianoff, writing in June 2026, put the structural problem precisely: "To keep 15-year-olds out, platforms must find a way to check who is 15. And to do that at scale, the internet starts moving toward ID checks, face scans, and third-party verification systems." That is not a slippery slope argument. It is a description of what has already happened in Australia and what Bill C-34 would replicate in Canada — not as an unintended consequence, but as the mechanism the bill depends on.

How Canada, Australia, and the United Kingdom Compare on the Under-16 Model

Canada is not legislating into a settled consensus. The two jurisdictions furthest ahead, Australia and the United Kingdom, have both chosen the platform-enforced verification path that Bill C-34 also takes, rather than the parental-tools model most Canadians say they prefer. The early evidence from Australia, the only regime actually

in force, is that the mechanism is widely circumvented while the privacy cost to adults is permanent. The comparison below is drawn from the governing statutes and the responsible regulator in each jurisdiction.

Dimension	Canada: Bill C-34 (proposed)	Australia: in force Dec 10, 2025	United Kingdom: announced Jun 15, 2026
Status	First reading June 10, 2026; not yet law, with Royal Assent not expected before the end of 2026 and the core rules left to future regulation.	In force since December 10, 2025 under the Online Safety Amendment (Social Media Minimum Age) Act.	Announced June 15, 2026; legislation expected before the end of 2026 and in force around spring 2027, built on the Online Safety Act 2023.
Minimum age	16 for a social media account, fixed in the Act.	16.	16.
Who it applies to	"Regulated" social media, chatbot and online services above user thresholds not yet set; the platforms actually covered by the under-16 rule are designated later by the Governor in Council.	eSafety's list includes Facebook, Instagram, Snapchat, Threads, TikTok, Twitch, X, YouTube, Kick and Reddit; messaging and some services are excluded by rule, and the list has been revised repeatedly.	Selected platforms on the Australian model (Snapchat, TikTok, YouTube, Instagram, Facebook, X); messaging and YouTube Kids excluded, plus function limits on livestreaming and stranger contact across wider services including gaming.
Age-check mechanism	"Adequate" age-verification or age-estimation on designated services; what counts as "adequate" or "effective" is defined later by the Commission.	Platforms must take "reasonable steps," with layered age-assurance recommended; in practice mostly self-declaration with optional selfie estimation.	"Highly effective age assurance," with Ofcom to define feasible methods and report by October 2026.
Who bears the check	Every user of a designated platform, adults included.	Every user of a covered platform, adults included.	Every user of a covered platform, adults included.
Adult-data safeguards	Data-minimization in ss. 22(2) and 27(2); the Commission must consult the Privacy Commissioner (s.122), but the announced rollout may precede that consultation.	Rules may bar collection of specified data; privacy handling has been contested after breach concerns.	Vendor and data-protection concerns raised (Open Rights Group); detail pending Ofcom work.
Regulator	Digital Safety Commission of Canada, not yet created, with no members, chair or funding model.	eSafety Commissioner (established).	Ofcom (established).
Maximum penalty	Greater of \$10M or 3% of global revenue; greater of \$20M or 5% on indictment.	Up to about A\$49.5M, now being doubled to about A\$99M under June 2026 legislation.	Online Safety Act penalties: up to the greater of GBP 18M or 10% of global revenue.
AI chatbots	Distinct duties (ss. 49 to 54): harmful-content mitigation, crisis intervention, and a bar on posing as human.	Not the focus of the minimum-age law; addressed through separate online-content codes.	"Romantic companion" AI chatbots must enforce a minimum age of 18, with wider intimate functions restricted for under-18s.
Early real-world results	None yet, as the regime is not in force.	Government reports 5M+ accounts removed, deactivated or restricted; a	None yet, as the regime is not in force.

Dimension	Canada: Bill C-34 (proposed)	Australia: in force Dec 10, 2025	United Kingdom: announced Jun 15, 2026
		BMJ / University of Newcastle study found more than 85% of under-16s still using social media three months in; testers opened self-declared "16" accounts on 9 of 10 platforms without being asked for proof; circumvention via VPNs, false birthdates and selfie tricks is widely reported.	

Source: Bill C-34 (45th Parliament, first reading, [parl.ca](#)) and Government of Canada, *The Safe Social Media Act* ([canada.ca](#)); Australia: *Online Safety Amendment (Social Media Minimum Age) Act* and *eSafety Commissioner, Social Media Age Restrictions* ([esafety.gov.au](#)), with results reported by Reuters, NBC News and The BMJ, 2026; United Kingdom: DSIT / Rt Hon Liz Kendall statement, 15 June 2026 ([gov.uk](#)) and Ofcom implementation letter, 16 June 2026. Compiled by Bearing Institute from primary government and regulator sources, July 2026.

Bearing Institute Alert. Every jurisdiction that has adopted the under-16 model has adopted platform-enforced age verification, and none has solved its central problem: confirming that a user is under 16 requires checking the age of everyone. Australia, six months in, reports millions of removed accounts alongside survey evidence that most under-16s are still on the platforms, while every adult now proves their age to keep access. Canada would inherit that trade-off by regulation, before its Commission, its standards, or its privacy review exist.

The Sequencing Problem: The Bill's Own Safeguards Don't Apply When They're Needed Most

There is a further problem that compounds the mechanism concern. Section 122 of the Digital Safety Act requires the Commission to consult the Privacy Commissioner of Canada before issuing any age-verification guideline or regulation — an acknowledgment, written into the bill itself, that mandatory population-wide verification carries serious privacy risks requiring independent review. The government's own announced implementation timeline would bring the under-16 restriction into force for at least some platforms before the Commission exists, before any verification standard has been published, and before that consultation has occurred. The safeguard and the deadline are on different tracks. This is not a hypothetical risk about what might go wrong later. It is a sequencing failure the government has already built into its rollout plan.

A Better Mechanism: Verify the Device, Not the Adult

There is a way to keep under-16s off social media without verifying the identity of a single adult, and it does not come from a civil-liberties group. It comes from Jonathan Haidt, the social psychologist whose bestseller *The Anxious Generation* did more than any other single work to build the public case for an under-16 social media age. In Chapter 12 of that book, developed with his collaborator Ravi Iyer, a former Meta product manager now at the University of Southern California, Haidt sets out the mechanism he calls device-based age verification, or age check.

The design is simple. The operating-system providers, Apple, Google and Microsoft, would build a single age signal into the device, switched on by default whenever a parent sets up a device for a child under 18. The device passes that signal to any app or site, which can then restrict age-sensitive features such as uploading video or being contacted by strangers. Age is established once, by the parent, at the device level, rather than by each platform checking every user who arrives. The feature Haidt emphasizes is the one at the centre of this Part: adults are never checked at all. A grown Canadian who visits a site that uses age check provides nothing and proves nothing, so their experience of the internet is unchanged and no adult identity data is collected anywhere.

Haidt does not treat that as a lucky side effect. He is unusually attentive to adult privacy for a child-safety advocate, and device-based verification is precisely his answer to the objection that protecting children should not require surveilling adults. The approach is already moving from proposal into law. Utah enacted the first app-store-level age-verification law in the United States, the App Store Accountability Act, in 2025, placing the age check on the app-store gatekeeper rather than on each platform, and Apple has since built a Declared Age Range API that passes a parent-set age range to apps without exposing a birthdate. Minnesota had introduced an equivalent operating-system-level age check provision a year earlier, in its 2024 Prohibiting Social Media Manipulation Act. These two models differ in one respect Parliament should hold onto. Utah's app-store approach still verifies every user once, adults included, at the store rather than at each platform; it removes the per-platform checking but not the initial check. The device-signal model Haidt favours goes further: a parent sets the age on a child's device, that signal travels to apps, and an adult who never sets up a managed child account is never asked to prove anything. It is that second form, verification at the device rather than of the adult, that this brief recommends, because it alone preserves the under-16 restriction while leaving every adult's access to the internet untouched.

Source: Jonathan Haidt, The Anxious Generation (2024), ch. 12, on device-based age verification (age check); Ravi Iyer, How Apple, Google and Microsoft Can Help Parents Protect Children, After Babel, May 2024 (afterbabel.com); Utah App Store Accountability Act, S.B. 142 (2025); Apple, Declared Age Range API (2025); Minnesota Prohibiting Social Media Manipulation Act, H.F. 4400 (2024).

Parental Tools Complement Device-Based Verification, Not State Identity Checks

The objective of keeping younger children off social media platforms is legitimate. The mechanism Bill C-34 chooses to achieve it — requiring platforms to verify the identity of every adult Canadian — is not proportionate to that objective, and it is not the mechanism most Canadians say they want.

Device-based verification should be paired with a duty on platforms to provide effective, accessible, and genuinely functional parental control tools: account-linking features that give parents visibility into their child's account, time-limit and content-filter settings that parents can configure, age-appropriate default settings for accounts that self-report as belonging to minors, and meaningful penalties for platforms that make parental controls difficult to find or use. This approach puts enforcement responsibility where 72 per cent of Canadians say it belongs — with parents — without building a government-mandated identity verification infrastructure that treats every adult as a suspect until proven otherwise.

It also addresses the real failure the bill is responding to. The documented harms to children from social media — algorithmic amplification of self-harm content, manipulative engagement design, lack of parental visibility — are not primarily the result of children lying about their age on sign-up forms. They are the result of platforms designing their services to maximize engagement regardless of user wellbeing. Effective parental tools, combined with the design-safety obligations already in Bill C-34's section 21 and the harmful-behaviour duties in sections 51 to 54, address that failure directly. A population-wide age verification mandate does not.

Bearing Institute Alert. Bill C-34 requires every adult Canadian to prove their identity to access designated social media platforms in order to enforce a restriction that 72 per cent of Canadians say should be enforced by parents. That is a disproportionate invasion of privacy in service of a mechanism most Canadians did not ask for. The right policy is effective parental tools, not state-mandated identity infrastructure.

Source: Digital Safety Act, ss. 21, 22, 27, 51–54, 122 (Bill C-34, 45th Parliament, First Reading, parl.ca); Angus Reid Institute, "Banning children under 16 from social media platforms widely supported by parents and most Canadians," March 30, 2026; eSafety Commissioner, Social Media Age Restrictions, esafety.gov.au; Greg Lukianoff, "The online 'safety' trap," Eternally Radical Idea, June 15, 2026; Michael Geist, "The Exemption Illusion," michaelgeist.ca, June 2026; IAPP, "OPC's Dufresne touts new age assurance guides," May 2026.

Part 5: The Competition and Innovation Problem

One dimension of Bill C-34 that has received comparatively little attention is its effect on competitive dynamics for digital services in Canada. The bill's penalty regime scales by gross global revenue: the maximum administrative monetary penalty is the greater of \$10 million or 3 per cent of global revenue, while the maximum criminal fine on indictment reaches the greater of \$20 million or 5 per cent of global revenue. These figures were chosen because only amounts calculated as a fraction of global revenue create meaningful compliance pressure on the world's largest platforms — companies like Meta, Alphabet, and ByteDance whose revenues run to hundreds of billions annually.

The structural consequence is that the marginal cost of compliance — legal staff, technical infrastructure for age verification and content moderation, Commission registrations, digital safety plans, the dedicated resource person required under sections 40 and 57 — falls proportionally far more heavily on smaller operators. A Canadian social media startup with 500,000 users and revenues of \$5 million faces a compliance infrastructure requirement, in kind if not in dollar amount, substantially similar to what the bill demands of Facebook, but without the economies of scale and in-house legal capacity that make that infrastructure manageable for large incumbents. Torys LLP has noted the long runway to implementation may give large platforms time to prepare, while also giving their legal and engineering teams a head start that smaller entrants cannot match.

Regulatory bodies whose substantive rules are made in collaboration with dominant incumbents have a well-documented tendency in network industries to entrench those incumbents. The Digital Safety Commission of Canada Act contains no structural safeguard against that outcome: the same 31 heads of regulatory power that give the Commission authority to set the rules also give the platforms with the most resources the greatest influence over what those rules say.

Bearing Institute Alert. Penalty regimes calibrated to global revenue are appropriate for global incumbents. Their side effect is that compliance infrastructure requirements fall disproportionately on smaller Canadian platforms and startups. A bill intended to discipline large foreign platforms may disproportionately burden Canadian innovators.

Source: Digital Safety Act, ss. 40, 57, 88, 100, 107 (Bill C-34, 45th Parliament, First Reading, parl.ca); Digital Safety Commission of Canada Act, s. 9; Torys LLP, "Bill C-34: Canada proposes legislation to regulate social media, AI chatbot, and online services," June 2026; Canadian Constitution Foundation, "Bill C-34, the Safe Social Media Act, Explained," June 2026.

Part 6: What Bill C-34 Gets Right

Bearing Institute's analysis is not a rejection of digital safety legislation. Several provisions of Bill C-34 represent legitimate, proportionate, and defensible responses to real problems.

Removal of the Criminal Code and Human Rights Act Provisions

Bill C-63 died in part because it combined platform safety regulation with Criminal Code and Canadian Human Rights Act amendments that would have expanded hate speech liability and permitted civil complaints to a human rights tribunal with power to award damages. Civil liberties organizations across the political spectrum opposed those provisions. Bill C-34 does not resurrect them. Minister of Canadian Identity and Culture Marc Miller has confirmed they will not be reintroduced as part of this bill. That decision should be acknowledged as a genuine response to earlier criticism.

The Explicit Expression-Protection Clause

Sections 22(3), 27(3), and 32(3) each provide that the relevant duty does not require an operator to implement measures that “unreasonably or disproportionately limit users’ expression.” This is a textual proportionality hook that reflects a legislative attempt — unusual in online safety legislation globally — to write limits on over-compliance directly into the bill’s operative provisions. Its limitation is that the Commission decides what is unreasonable or disproportionate, but its presence provides a meaningful ground for judicial review if the Commission adopts an unreasonable standard.

Targeted Mandatory Takedown for Abuse Material and Non-Consensual Images

Sections 43 through 47 require regulated social media services to make inaccessible, within 24 hours, content that sexually victimizes a child and intimate content communicated without consent. The definitions in section 2(1) are carefully drafted, with detailed carve-outs in section 2(4) for legitimate purposes related to justice, science, medicine, education, or art. These carve-outs reduce the risk that mandatory removal obligations will be weaponized against legitimate documentary or educational content.

The AI Chatbot Crisis-Intervention Duty

Section 51 is, in Bearing Institute’s view, the most clearly justified chatbot provision in the bill. It requires regulated chatbot operators to implement measures that, if a user expresses suicidal ideation or intention to self-harm, cause the service to immediately interrupt and direct the user toward available, human-staffed crisis intervention services. Section 53 adds duties against impersonating a human in a way likely to deceive, posing as a licensed professional, using manipulative engagement techniques to encourage harmful emotional dependency, and encouraging self-harm or suicide. These provisions respond directly to documented harm — including the Raine litigation and the Tumbler Ridge events — with specific duties that give operators a clear standard to meet.

Data-Minimization Requirements for Age Verification

Sections 22(2) and 27(2) specify that adequate age-verification measures must not collect or use personal information for any purpose other than the verification itself, must provide for the destruction of that information once verification is complete, and must protect it until destroyed. These data-minimization principles are consistent with the Privacy Commissioner’s age-assurance guidance and distinguish Bill C-34 from age-verification regimes that contain no equivalent protection.

Transparency Requirements and Research Access

Sections 42, 58, and 59 require operators of all three categories of regulated services to submit public digital safety plans disclosing how they assess risk, what measures they have implemented, how they evaluate those measures, and what resources they allocate to compliance. The plans must be publicly available on the service itself. Section 60 creates an accreditation pathway for researchers to access the data inventories platforms must include in their plans — a genuine innovation relative to the opaque data arrangements that have characterized platform research access to date.

Source: Digital Safety Act, ss. 22(2)–(3), 27(2)–(3), 32(3), 42, 43–47, 51, 53, 58–60 (Bill C-34, 45th Parliament, First Reading, parl.ca); CCLA, “CCLA warns against risks to freedom of expression and privacy posed by Bill C-34,” June 2026; IAPP, “OPC’s Dufresne touts new age assurance guides,” May 2026.

Part 7: Five Structural Problems That Require Amendment

7.1 The Scope Problem: Parliament Does Not Know What It Is Regulating

Bill C-34 asks Parliament to approve duties and penalties for operators of “regulated” services, but sections 6(2), 7(2), and 8(2) make clear that no service currently meets any of those definitions, because the definitions require meeting user-number thresholds that have not been specified. The types of services, the thresholds for each type, and the methodology for counting users are all to be set by the Governor in Council after royal assent. Section 2(7) adds that an AI system “exclusively serving a purpose specified in the regulations” is excluded from the chatbot-service definition — but section 127(1)(a) does not require those purposes to be specified at all, it only permits the Governor in Council to specify them. Parliament therefore does not know which services will be regulated, which AI systems will be exempt, or how the thresholds will be measured.

Bearing Institute Alert. Parliament is voting to create duties and penalties for operators of regulated services without knowing which services will be regulated, how the regulatory threshold will be measured, or which AI systems are exempt. These are not implementation details. They are the questions that determine what the law does.

Source: Digital Safety Act, ss. 2(7), 6(2), 7(2), 8(2), 127(1)(a) (Bill C-34, 45th Parliament, First Reading, [parl.ca](#)); Osler, “Bill C-34 at a glance,” June 2026; Michael Geist, “The Law to Be Named Later,” [michaelgeist.ca](#), June 2026.

7.2 The Vague Content Problem: No Legitimate-Purpose Protection for Contested Expression

The definitions of “content that foments hatred” and “content that incites violence” in section 2(1) each turn on context and likelihood, and their application to AI chatbot operators under sections 49 and 50 creates a compliance environment where the safest course is to refuse to engage with any topic that could conceivably satisfy the definitions in the most generous interpretation a complainant might apply. The bill does not include the explicit legitimate-purpose exclusion for journalism, education, and art that it provides for terrorism content under section 2(6). As both the CCLA and the Canadian Constitution Foundation have documented, when the standard is unclear and the penalties are severe, over-compliance is the rational response — producing a sanitized information environment that serves no one. Those two definitions should be struck from the Bill.

Source: Digital Safety Act, ss. 2(1), 2(3), 2(6), 49, 50 (Bill C-34, 45th Parliament, First Reading, [parl.ca](#)); CCLA, “CCLA warns,” June 2026; Canadian Constitution Foundation, “Bill C-34, the Safe Social Media Act, Explained,” June 2026.

7.3 The Sequencing Problem: Age Verification Without Standards, Review, or Enforcement

The government’s announced implementation timeline would bring the under-16 restriction into force for at least some platforms before the Digital Safety Commission of Canada exists, before any age-verification standard has been published, and before the mandatory consultation with the Privacy Commissioner required by section 122 has occurred. The legal basis for age verification on that accelerated timeline is platform self-assessment against adequacy criteria that the Commission has not yet operationalized. Parliament should not enact a bill whose own implementation plan bypasses the privacy safeguard the bill itself was designed to provide.

Source: Digital Safety Act, ss. 22, 27, 122 (Bill C-34, 45th Parliament, First Reading, [parl.ca](#)); Michael Geist, “The Exemption Illusion,” [michaelgeist.ca](#), June 2026; BetaKit, “Ottawa introduces bill to ban social media for kids under 16,” June 2026.

7.4 The Commission Structure Problem: A Regulator with No Structural Limits

The Digital Safety Commission of Canada is simultaneously assigned responsibility for writing the implementing regulations, assessing platform compliance with those regulations, adjudicating complaints, auditing operators, issuing penalties, and granting exemptions from the bill’s most significant obligation. This concentration of

regulatory, enforcement, and adjudicative functions in a single body has a well-documented historical precedent. The Federal Communications Commission in the United States was created in 1934 to solve a practical problem — allocating the electromagnetic spectrum — and has repeatedly become a tool for jawboning media companies, threatening licences, and pressuring perceived political opponents, under administrations of both parties. Under the current FCC Chair Brendan Carr, that pattern has become starkly visible again. A communications-adjacent regulator with broad discretion over what services may say, how they must be designed, and what content they must suppress is a tool that whoever holds power will be tempted to use. The Digital Safety Commission of Canada Act contains no structural safeguard — no separation between the rule-writing and adjudicative functions, no independent review of the Commission’s own compliance decisions — against the same dynamic.

Bearing Institute Alert. The Digital Safety Commission of Canada is assigned rulemaking, enforcement, adjudication, and exemption functions with no structural separation between those roles. The FCC’s history illustrates what happens when a communications-adjacent regulator with broad discretionary powers outlasts the government that created it.

Source: Digital Safety Commission of Canada Act, ss. 6–9; Digital Safety Act, ss. 15–19, 122, 126; Greg Lukianoff, “The online ‘safety’ trap,” Eternally Radical Idea, June 15, 2026; Michael Geist, “The Commission: How Bill C-34 Creates an Internet Super-Regulator,” michaelgeist.ca, June 2026.

7.5 The Parliamentary Oversight Gap

The Digital Safety Act requires, under sections 128 and 129, that the Minister review the Act and the minimum-age provisions within five years of the relevant provisions coming into force, and report the results to Parliament. This is a welcome mechanism. Its limitation is that the most consequential decisions — the designation of which platforms face the age restriction, what counts as adequate age verification, what design features platforms must implement, and the scope of chatbot-service exemptions — will all be made through Commission or Governor in Council regulations, not through the Act itself. The parliamentary review is a review of the framework. It does not reach the regulations that will constitute, in practice, most of what the law does.

Source: Digital Safety Act, ss. 128–129 (Bill C-34, 45th Parliament, First Reading, parl.ca); Torys LLP, “Bill C-34: Canada proposes legislation to regulate social media, AI chatbot, and online services,” June 2026.

Part 8: Legislative Recommendations — Amendments You Can Table

Each of the five recommendations below is designed to preserve the legitimate safety goals of Bill C-34 while addressing its most significant structural flaws. The first three address the delegation and vagueness problems. The fourth addresses the sequencing and privacy problem. The fifth addresses parliamentary oversight.

Recommendation 1: Define Core Scope in the Statute Before the Bill Proceeds

The Action: Amend sections 6, 7, and 8 to include, in the statute itself, either (a) a default minimum user threshold triggering “regulated” status for social media and chatbot services, subject to adjustment by the Governor in Council within a defined range, or (b) an explicit list of service types initially subject to the bill’s major duties, with a defined process for expansion. Similarly, amend section 2(7) to specify, in the statute, at least the principal categories of AI systems excluded from the “chatbot service” definition.

The Goal: Parliament should not vote to create penalties of up to 5 per cent of global revenue for operators of “regulated” services without knowing which services will be regulated. Writing a default threshold into the statute ensures that the core coverage decision is made by Parliament, not by a future Governor in Council acting without parliamentary vote. The Investment Canada Act analogue in Part 3 illustrates exactly what happens when

the regulated-sector designation is left entirely to post-assent regulations: years of uncertainty for the public, affected businesses, and affected individuals.

Legislative Anchor: Bill C-34, Digital Safety Act, ss. 2(7), 6, 7, 8.

Recommendation 2: Strike "Foments Hatred" and "Incites Violence" from the Harmful Content Definition

The Action: Amend section 2(1) of the Digital Safety Act to remove "content that foments hatred" and "content that incites violence" from the definition of harmful content entirely. The five remaining categories — content that sexually victimizes a child or revictimizes a survivor, intimate content communicated without consent, content that sexually exploits a child, terrorist and violent extremist content, and content that incites genocide — should be retained without modification.

The Goal: The five categories Bearing Institute recommends retaining share three characteristics: they have precise statutory or common law definitions, they have been tested in courts and tribunals over decades, and they command near-universal public consensus. "Content that foments hatred" and "content that incites violence" share none of those characteristics. They are context-dependent, turn on subjective assessments of likelihood and intent, and have been the subject of unresolved litigation in human rights tribunals staffed by lawyers for decades. There is no principled case for including them in a mandatory-removal and penalty regime whose consequences reach 5 per cent of global revenue when the bill already captures the most serious platform harms without them.

The over-compliance argument is not theoretical. As the CCLA, the Canadian Constitution Foundation, and FIRE's Greg Lukianoff have each documented, when the standard is undefined and the penalties are severe, platforms and AI chatbot operators will decline to engage with entire categories of lawful but contested public discourse — on history, demographics, foreign policy, gender, and immigration — rather than risk guessing wrong about what a future Commission will consider adequate. That chilling effect does not require bad intent from the government that drafted the bill. It is a mechanical consequence of vague standards and asymmetric penalties, and it will operate identically under every future government that inherits this Commission.

Bearing Institute notes that removing these two categories does not leave hatred and violence unaddressed in Canadian law. The Criminal Code already prohibits public incitement of hatred likely to lead to a breach of the peace under section 319(1), wilful promotion of hatred against an identifiable group under section 319(2), and counselling the commission of an indictable offence under section 464. Those provisions carry the procedural protections — judicial authorization, the requirement of criminal intent, the right to full answer and defence — that a mandatory-removal regime administered by a Commission does not. Parliament should not create a parallel enforcement track for speech offences that bypasses those protections under the guise of platform regulation.

Legislative Anchor: Bill C-34, Digital Safety Act, s. 2(1): delete the definitions of "content that foments hatred" and "content that incites violence," and remove all cross-references to those categories in ss. 32, 43, 49, and 50. The remaining five categories of harmful content are sufficient.

Recommendation 3: Replace Population-Wide Identity Verification with Device-Based Age Verification and Parental Control Tools

The Action: Amend sections 22 and 27 of the Digital Safety Act to remove the platform-by-platform age-verification and age-estimation requirement as the mechanism for the under-16 restriction, because that mechanism cannot operate without verifying the age of every adult who uses a designated service. Replace it with two duties. First, a duty on regulated social media services to recognize and honour a device-level age signal

(device-based age verification, or age check) as the primary means of identifying users under 16, so that age is established once at the operating-system level rather than by each platform checking every user. Second, a complementary duty on those services to provide effective parental control tools, specifically: (a) account-linking features that allow a parent or guardian to connect their account to a minor's account and receive meaningful visibility into account activity; (b) configurable time-limit, content-filter, and privacy settings that parents can apply to linked accounts; (c) age-appropriate default settings automatically applied to any account whose user self-reports as being under 18; and (d) a duty to make parental control features accessible, prominent, and no more difficult to use than the platform's core features. Retain the section 21 design-safety obligations and sections 51 to 54 crisis-intervention and harmful-behaviour duties in full.

The Goal: A March 2026 Angus Reid Institute poll found that 72 per cent of Canadians believe enforcement of under-16 social media restrictions should rest with parents, not government policy. Bill C-34 as drafted ignores that majority view and substitutes state-mandated identity verification infrastructure for parental responsibility. Every adult Canadian who wants to use a designated platform will be required to prove their age to that platform or to a government-approved third-party vendor — not as a byproduct of the policy, but as its central operating mechanism. That is a disproportionate invasion of the privacy of adults who are not the policy's intended subject, in service of a mechanism that Australia's implementation experience demonstrates is easily circumvented by the children it is designed to protect.

The mechanism that satisfies that majority without surveilling adults already exists in the child-safety literature. Jonathan Haidt, whose book *The Anxious Generation* built much of the public case for an under-16 age, proposes device-based age verification: the operating system carries a single age signal, set once by the parent, that every app honours, so that no adult is ever asked to prove anything to any platform. That is the design this recommendation adopts as its primary mechanism. It enforces the under-16 restriction the government wants while removing the population-wide adult identity verification that makes the current draft so constitutionally exposed.

Parental control tools are not a weaker alternative to device-based verification. They are its complement. The documented harms to children from social media — algorithmic amplification of harmful content, manipulative engagement design, inadequate crisis intervention — are addressed directly by Bill C-34's existing section 21 design-safety obligations and sections 51 to 54 harmful-behaviour duties. What parental tools add is the enforcement mechanism that most Canadians actually want: visibility and control at the family level, without building a national identity verification infrastructure whose privacy costs fall on every adult in Canada.

Legislative Anchor: Bill C-34, Digital Safety Act, ss. 22 and 27: replace the platform-level age-verification and age-estimation duty with a device-based age-verification (age check) duty as the primary mechanism, plus a complementary mandatory parental control tools requirement. Retain ss. 21, 51–54 without modification.

Recommendation 4: Require Parliamentary Approval for Major Regulations

The Action: Amend the Digital Safety Act and the Digital Safety Commission of Canada Act to subject the following categories of Commission and Governor in Council regulations to a tabling and affirmative-resolution requirement before taking effect: (a) regulations designating which social media services and chatbot services are “regulated” under sections 6 and 7; (b) regulations specifying design features platforms must implement for children under section 21; (c) regulations defining what constitutes adequate safeguards for an under-16 exemption under section 29; and (d) cost-recovery charges under section 125.

The Goal: The approximately 50 regulatory decisions that constitute the operative content of Bill C-34 will collectively determine, far more than the Act itself, what this law actually does, who it covers, what compliance costs, and who is exempt. The parliamentary review provisions in sections 128 and 129 review the Act after five

years. This Recommendation ensures that the regulations making the Act substantive are reviewed by Parliament before they are in force. A 30-sitting-day affirmative-resolution requirement in both Houses is a proportionate mechanism for regulations of this scope.

Legislative Anchor: Bill C-34, Digital Safety Act, ss. 6, 7, 21, 29, 125–126; Digital Safety Commission of Canada Act: add tabling and affirmative-resolution requirement for designated major regulations.

Recommendation 5: Add an Independent Adjudicative Function Separate from the Commission’s Regulatory and Enforcement Roles

The Action: Amend the Digital Safety Commission of Canada Act to require that the Commission’s adjudicative functions — complaints under section 68, penalty proceedings under sections 83 to 106, and compliance orders under section 81 — be performed by a structurally distinct Adjudicative Panel whose members are not the same individuals exercising the Commission’s regulatory and enforcement functions. The Chairperson of the Adjudicative Panel should be designated separately and hold law-society or judicial qualifications.

The Goal: Under the bill as drafted, the Commission that writes the rules, investigates non-compliance, and brings penalty proceedings is the same body that decides whether a violation occurred and at what penalty level. This is a well-recognized structural due process concern that courts applying *Baker v. Canada* (Minister of Citizenship and Immigration) have consistently held requires, at minimum, the reasonable appearance of independence in the adjudicative function. A bill with penalties up to 5 per cent of global revenue for expression-adjacent conduct should not be administered by a regulator with no structural separation between the roles of investigator, rule-writer, and judge.

Legislative Anchor: Digital Safety Commission of Canada Act, ss. 8–14: amend to establish a structurally distinct Adjudicative Panel.

Summary: What Bearing Institute Recommends

Recommendation	Provision	What It Preserves
1. Define core scope in the statute	DSA ss. 2(7), 6, 7, 8	Platform and chatbot duties with a known scope, reducing regulatory uncertainty for compliant operators
2. Strike "foments hatred" and "incites violence" from the harmful content definition	DSA s. 2(1); consequential amendments to ss. 32, 43, 49, 50	Five remaining harmful content categories retained in full; Criminal Code provisions remain the appropriate mechanism for hate speech and incitement
3. Replace population-wide identity verification with device-based age verification and parental control tools	DSA ss. 22, 27; retain ss. 21, 51–54	The under-16 child-safety objective, achieved through the mechanism 72 per cent of Canadians say they prefer
4. Parliamentary approval for major regulations	DSA ss. 6, 7, 21, 29, 125–126; DSCCA	Full Commission regulation-making authority, with democratic scrutiny of its most consequential exercises
5. Structurally distinct adjudicative function	DSCCA ss. 8–14	Commission enforcement capacity, with the structural independence necessary for fair proceedings involving major penalties

Source: Bearing Institute analysis of Bill C-34 (45th Parliament, First Reading, June 10, 2026, [parl.ca](#)).

Conclusion

Canada needs a digital safety framework. The harms Bill C-34 responds to — child sexual exploitation facilitated by algorithmic amplification, non-consensual intimate image distribution, AI chatbots that have failed to interrupt conversations moving toward real-world violence — are documented, serious, and growing. Voluntary action by platforms has been insufficient. The government is right that Parliament has a role to play, and the public support for the bill's stated goals is genuine and broad.

The question before Parliament is not whether digital harms are real. They are. The question is whether Canadians should grant broad regulatory powers today and trust future governments, future regulators, and future Commissions — whichever parties appoint them — to decide their limits afterward. Good legislation does not depend on who occupies office when the regulations are eventually written.

Bill C-34, as tabled, is built on the assumption that it does. The Digital Safety Commission of Canada does not yet exist. Its members have not been appointed. Its funding model has not been set. Which services it will regulate, what “adequate” means for age verification, and what categories of AI systems are exempt have not been decided. None of the roughly 50 decisions that will constitute the operative content of this law have been made, and Parliament is being asked to approve the framework in which they will be made without knowing what they will say.

Canada is joining a rapidly moving global experiment. The United Kingdom announced its own under-16 ban on June 15, 2026 — five days after Bill C-34 was tabled. Australia's ban has been in effect for six months, and the compliance picture there is already more complicated than the headline figure of 4.7 million removed accounts suggests. There is no settled consensus to catch up to. There is an emerging approach whose real-world performance is still being assessed, and whose central unresolved problem — that verifying who is under 16 requires checking everyone — no jurisdiction has yet solved.

Justice Robert Jackson wrote in *West Virginia State Board of Education v. Barnette* that the First Amendment was designed “to avoid these ends by avoiding these beginnings.” That principle applies, with equal force, to the parliamentary discipline of defining power before granting it. The five amendments recommended in this brief would preserve Bill C-34's legitimate child-safety objectives, remove its most structurally dangerous provisions, and require the government to produce the regulatory definitions Parliament is owed before voting. That is not an anti-reform position. It is the minimum standard of legislative accountability that a bill of this constitutional and societal significance demands.

Matthew Trenholm, MSc, is a co-founder of the Bearing Institute and a published researcher in the Journal of International Health Sciences and Management. He has worked in Canada's busiest emergency room for twenty years.

Bearing Institute is a Canadian public-policy institute focused on legislative research and ready-to-table amendments. Bearing Institute would welcome the opportunity to present this analysis during committee hearings or Senate consideration of Bill C-34, and is available to provide further analysis on request.

[BearingInstitute.ca](https://bearinginstitute.ca)