



Statement on

Bill C-34, the Safe Social Media Act

Department of Canadian Heritage

Submitted by: MediaSmarts/HabiloMédias

Written by: Dr. Kara Brisson-Boivin, Director of Research

Contact: Kathryn Ann Hill, Executive Director

Address: 205 Catherine Street, Suite 100, Ottawa ON K2P 1C3

Date: October 16, 2026

About MediaSmarts

MediaSmarts/HabiloMédias is Canada's not-for-profit centre for digital media literacy. As a registered charity, our vision is that all Canadians are empowered to engage with digital media confidently and critically. For 30 years, MediaSmarts has conducted and disseminated original research, developed internationally recognized educational programs for teachers, parents, youth, seniors, and general audiences, and conducted national awareness campaigns to advance digital media literacy across Canada.

Our interdisciplinary team brings expertise in research, education, and community engagement. Dr. Kara Brisson-Boivin, Director of Research, leads research and evaluation projects, while Matthew Johnson, Director of Education, oversees program development and implementation. Dr. Brisson-Boivin also serves on the [Research and Evaluation Advisory Committee](#) for Ofcom's [Making Sense of Media](#) program in the United Kingdom, contributing expertise to the development of the UK's national approach to media literacy. Our research-to-resource model translates evidence-based insights into practical educational tools that reach diverse communities across Canada, and our educational resources are aligned with curriculum outcomes in every province and territory. To date in 2026, MediaSmarts has directly reached over 14,000 Canadians through workshops and educational programs.

MediaSmarts' work sits at the intersection of young people's digital well-being, online privacy and consent, AI literacy, information verification, and resilience to online harms. Our work is directly relevant to the objectives of the Safe Social Media Act, including:

- [Young Canadians in a Wireless World \(YCWW\)](#): Canada's longest-running and most comprehensive study of young people's online lives, which has tracked the online experiences, attitudes, and behaviours of children and youth since 2000, including their encounters with harmful content, online meanness and cruelty, privacy and consent, and the role of parents and educators.
- [Breaking the Cycle of Youth Cyberbullying \(BTC\)](#): An intervention research project to develop, pilot, adapt, and disseminate a culturally safe, evidence-informed cyberbullying prevention program for youth ages 12 to 17 in schools and community settings across Canada. A needs assessment conducted in March and April 2026 explored the experiences, concerns, and needs of youth in Canada regarding preventing and addressing cyberbullying and online violence.
- [Algorithmic Awareness](#): Qualitative research with young Canadians on artificial intelligence (AI), algorithms, and privacy, examining what young people understand, and want to know, about the automated systems shaping their online experiences.
- [Break the Fake](#) and [Motives and Methods](#): Our internationally recognized verification program and an accompanying study of 5,000 Canadians demonstrating that short digital media literacy interventions measurably improve fact-checking and sharing behaviours, including in relation to visual and AI-generated content.
- [Building Better Tech Habits](#) and [Talking to Kids About AI](#): Practical, non-judgmental resources that help youth, families, and educators build healthy habits with devices, apps, and AI chatbots, alongside our growing [AI literacy content](#) and [Canada's AI Literacy Day](#).

MediaSmarts' recent policy contributions relevant to this statement include our submission to the Office of the Privacy Commissioner of Canada (OPC) on the Children's Privacy Code (2025), our submission to the Government of Ontario on the proposed regulation under the *Enhancing Digital Security and Trust Act* (2026) concerning digital technology affecting individuals under age 18, and our January 2026 [Open Letter to the Government of Canada](#) on the urgent need for a National Strategy for Digital Media Literacy, endorsed by more than 40 organizations and experts across Canada.

Introduction and Overview

MediaSmarts thanks the Department of Canadian Heritage for the invitation to comment on Bill C-34, the Safe Social Media Act. We share the government's concern for the safety and well-being of children and youth online and agree that voluntary action by platforms has not kept pace with the scale and severity of online harms. Parents, educators, and young people themselves have been asking for meaningful action for years. The urgency is real.

MediaSmarts strongly supports the bill's core premise that online harms are shaped not only by individual behaviour, but by how digital services are designed and operated, and that the companies that design these systems should be responsible for the risks they create. The proposed duties to act responsibly, to protect children, to make certain content inaccessible, together with the requirement that platforms publish Digital Safety Plans showing how they are meeting those obligations,

represent an important step toward the kind of systemic, safety-by-design accountability that our research and advocacy have long called for. We particularly welcome the creation of an independent Digital Safety Commission of Canada, and we look forward to working with the Commission as it takes shape.

We recognize that the minimum age requirement for social media accounts is likely to move forward, and our statement is written with that in mind. What is more important to us is that Bill C-34 is not simply a ban. By allowing services to earn an exemption by demonstrating that their products are safe for children, the bill shifts the central question from when young people should be allowed to use social media to how social media can be designed safely for them. This places the burden of demonstrating safety on platforms rather than on young people, their families, and the trusted adults who support them. It also recognizes that young people do not become immune to online harms on the day they reach a particular age, which is why safety protections should not end at 16.

MediaSmarts welcomes this shift. Our focus is therefore on implementation: how to ensure that an age restriction, alongside the bill's other measures, delivers real and lasting benefits for young people and their families. Drawing on 30 years of research and education with children, youth, parents/caregivers, and educators, we offer recommendations in the following areas:

- **Building on the bill's safety-by-design approach** and welcoming the Digital Safety Commission;
- **Implementing the minimum age requirement well** including lessons from other jurisdictions, the essential role of parents and caregivers, preserving platforms' incentives to invest in safer design for Canadian youth, and privacy-protective age assurance;
- **The bill's obligations for AI chatbot services and synthetic content;**
- **Digital media literacy as the missing pillar** of the framework;
- **Youth engagement**, and how the Commission can meaningfully include young people in shaping the framework; and
- **Transparency, research, and recourse** mechanisms that work for young people.

1. Welcoming a Systemic Approach and the Digital Safety Commission

1a. Safety by Design

MediaSmarts commends the government for advancing safety by design for children and youth. For more than two decades, young people in our research have told us that they feel they must “pay to play,” trading their personal information and their attention for access to the platforms where their social lives, learning, and self-expression take place. They express distrust of platforms' willingness to prioritize their safety over commercial interests. A regulatory framework that requires services to identify, mitigate, and report on the risks their products create responds directly to those concerns.

We particularly welcome the bill's recognition that design features such as engagement-based recommendation systems, autoplay, and “endless scroll” content delivery may amplify and increase exposure to harmful content. Our research consistently shows that harm is driven less by the amount

of time young people spend online than by the specific experiences they have — exposure to risky content, social comparison, and the negative self-reactions those experiences provoke — many of which are shaped by design choices that optimize for engagement rather than for user well-being.

Bill Provision: Duty to Protect Children — Age-appropriate design features to be set out in regulations by the Digital Safety Commission

MediaSmarts recommends that the Commission's age-appropriate design regulations:

- **Target engagement optimization, not “addiction”:** MediaSmarts welcomes the bill's neutral, design-focused language, which requires operators to integrate design features that protect children's well-being rather than framing the issue as one of "addiction." As the Commission develops these regulations, we encourage it to maintain this framing, grounding its design standards around engagement-optimizing design including infinite scroll, autoplay, streaks, variable rewards, persistent notifications, and algorithmic amplification. There is significant evidence that framing media use as “addictive” leads to worse outcomes than viewing it in terms of habits; as well, the addiction frame may also imply that abstinence is the only solution, obscure the design choices platforms control, and undercut young people's own sense of agency. Design standards grounded in engagement optimization place the focus squarely on what services can and should change.
- **Establish safe and private defaults:** Evidence is clear that few users ever change an app's default settings. Accordingly, children's and teens' accounts should default to the most privacy protective settings, including private profiles, limits on contact from unknown adults, and disabled location sharing. Young people should be able to adjust these settings with clear, age-appropriate explanations of what each change means.
- **Give young people meaningful control over their feeds:** Youth in our research tell us while they value personalized content, they want to understand and influence how algorithms shape their experiences. Standards should require services to explain, in plain and age-appropriate language, why content is being recommended, and to provide easy-to-use tools to adjust, reset, or pause personalized recommendations, including the option to switch to a non-personalized or chronological feed if they choose. Here, again, the default should be to feeds that have not been optimized for continued engagement, to prolong time spent or encourage daily use, or to provoke strong emotional reactions. Feeds should also default to provide strong, age-appropriate content filters which limit young people's exposure to upsetting content without blocking access to legitimate news or educational content or penalizing content from marginalized groups.
- **Integrate children's privacy and online safety:** Many of the design harms the bill addresses are powered by the collection and use of children's data. Whether children's privacy is overseen by the Office of the Privacy Commissioner (OPC) or, as proposed in Bill C-36, by a Privacy and Consumer Data Commissioner within a combined Digital Safety and Data Protection Commission, age-appropriate design standards and children's privacy requirements should be developed together so that they are consistent, mutually reinforcing, and not duplicative for services or confusing for families. The work already undertaken on the

OPC's Children's Privacy Code, including input from young people and civil society, should inform the new commissioner's work in this regard.

- **Be developed alongside young people:** Design standards should be informed by consultation with children and youth of diverse ages and backgrounds (as well as their parents and caregivers) who are the experts on their own online experiences (see Section 6).

1b. Welcoming the Digital Safety Commission of Canada

MediaSmarts welcomes the establishment of an independent, expert regulator with the authority to set standards, assess compliance, receive complaints, and support users and victims. The international experience of Ofcom in the United Kingdom and the eSafety Commissioner in Australia demonstrates the value of a dedicated body that can build technical expertise, adapt obligations as technology changes, and serve as a trusted public voice on online safety. We are especially encouraged that the Commission's mandate includes research and public education, and that it will provide a user support function for users and victims. To make the most of public investment, the Commission's role in education should be to provide direction, coordinate, fund, and evaluate, building on the evidence-based programs, resources, and community networks that Canadian organizations, like MediaSmarts, have developed over decades.

MediaSmarts looks forward to working with the Commission should this bill be passed. As Canada's centre for digital media literacy, we bring 30 years of experience, bilingual resources aligned with curriculum outcomes in every province and territory, and national programs with demonstrated impact. We are well positioned to contribute research on children and young people's online experiences, evidence on what works in digital media literacy education, educational resources already used in classrooms and communities across the country, and our experience engaging youth, parents, caregivers, and educators. We would welcome the opportunity to support the Commission's early work, including the development of its education strategy, age-appropriate design standards, and youth engagement approach.

2. Implementing the Minimum Age Requirement: Getting It Right for Young People and Families

MediaSmarts understands why a minimum age of 16 for social media accounts has broad public support. Parents and caregivers are worried about young people's wellbeing, and they want action. As we set out in our recent [op-ed in The Globe and Mail](#), the impulse is understandable and how the minimum age requirement is implemented will determine whether it delivers on its promise. Canada's approach differs from other jurisdictions in an important way: the minimum age requirement is paired with an exemption pathway for services to demonstrate that they are safe for children. Implemented well, this makes the requirement a lever for safer design rather than simply a barrier to access. With the age requirement likely to proceed, we offer the following considerations to help it succeed.

2a. Lessons from Other Jurisdictions

Early experience elsewhere offers important lessons for Canada's implementation:

- **Access-based rules have historically been easy to circumvent.** Most major platforms already set a minimum age of 13, yet our [YCWW research](#), like research in other jurisdictions, shows that many children use social media well before that age. In Australia, [a survey of parents conducted for the eSafety Commissioner](#) indicated that roughly seven in ten teens were still using social media after the restriction took effect, including by migrating to platforms not covered by the restriction and by attempting to defeat age-assurance technology.
- **What matters most is the quality of young people's online experiences.** Research consistently finds that harm is driven by specific experiences, such as social comparison and exposure to risky content, rather than by overall time spent online. What matters is the context, content, and the quality of young people's engagement, and whether they feel in control of their use and experiences. An age restriction is most effective when paired with design changes and education that improves the experiences young people have when they are online, including once they turn 16.
- **Unintended consequences must be actively managed.** When young people get around rules, they can become less likely to talk to parents/caregivers and educators about negative experiences for fear of the consequences. Our [YCWW research](#) has consistently found that trusted adults are among the most important protective factors in young people's online lives. Implementation of any age requirement should be designed to sustain trust and keep lines of communication open between young people and the adults they turn to for support.
- **Equity impacts deserve attention.** The young people most vulnerable to online harms are often also those who benefit most from online connection, community, and self-expression including 2SLGBTQ+ youth, racialized and Indigenous youth, youth with disabilities, youth in rural and remote communities, and young people who rely on their devices to stay connected to caregivers across multiple households. Implementation should monitor and mitigate differential impacts on these young people and ensure they retain access to supportive, safe online spaces.
- **Displacement to less regulated spaces should be anticipated.** When young people lose access to major platforms, they may move to spaces the bill does not cover, such as smaller or newer apps that do not meet the user thresholds for regulation, private messaging and group chat features (which are excluded from the bill's scope), online games and gaming platforms with built-in chat and community features, or services based in jurisdictions with weaker protections. In these spaces, young people would have none of the bill's safeguards, including age-appropriate design, flagging tools, or access to the Commission's complaints process. The Commission's ability to recommend that additional services be brought within the bill's scope will be important here, but it will need to be supported by up-to-date research on young people's online habits and experiences.

2b. Parents and Caregivers: Where Restrictions Are Actually Implemented

In our view, where bans and restrictions have fallen short in other jurisdictions, this has often been tied to a lack of resources and supports for parents and caregivers. Age restrictions are legislated at the national level, but they are implemented at the household level: in the daily interactions between

parents and their children and teens at the dinner table, at bedtime, in negotiations over a new app, and when a parent discovers their child has been using a service they were not supposed to.

Parents and caregivers are being asked to take on a significant new role, often with very little guidance and against a wall of confusing and conflicting advice. Many do not know which services are covered, how age assurance works, what to do if their child circumvents the rules, or how to talk about any of this without damaging trust. Without support, the burden of a national policy falls unevenly on families and most heavily on those with the fewest resources, the least time, and the lowest levels of digital confidence and skill.

MediaSmarts recommends that implementation of the minimum age requirement include dedicated, funded supports for parents and caregivers, focused on:

- **Engagement:** Plain-language, multilingual information on what the new rules mean for families — which services are covered, what will change and when, and what rights and recourse families have. Ideally this would be delivered before the requirement comes into force and through channels families already trust, including schools, libraries, community organizations, and health settings.
- **Education:** Practical guidance on the platforms, features, and risks young people encounter; on how to build healthy tech habits at the household level, where research shows such strategies are most successful; and on preparing young people for their eventual entry onto social media at 16.
- **Communication:** Tools to help families navigate the disagreements that restrictions will likely create, including how to set expectations together, how to respond and maintain trust when rules are broken, how to handle differing rules between households and among friends, and how to keep young people talking to trusted adults when something goes wrong online. Restrictions that are implemented through open conversation (for example, parents and teens reviewing privacy and recommendation settings together, or families setting tech expectations jointly) are far more likely to succeed than those implemented through surveillance or a top-down approach.

2c. Preserving Incentives for Safety by Design

An age restriction must not become a reason for platforms to stop investing in safer experiences for young Canadians. Recent developments illustrate the risk: In August 2026, following litigation brought by more than 50 U.S. state and territorial attorneys general, Meta agreed to a settlement that includes significant safety-by-design changes for teen users of Facebook and Instagram, including daily time limits, overnight blocks, the removal of push notifications during school hours, and hiding like counts by default. However, [Meta has indicated that these changes are specific to the United States](#) and will not, for now, be implemented in Canada. Even where they apply, these changes largely add guardrails to existing engagement-driven products, leave the collection of teens' data largely unaddressed, and bind a single company for a limited period.

Where platforms are subject to age restrictions, they may see little reason to invest in safety features for younger users they are nominally no longer serving. However, children will still be on these services in two ways. First, circumvention means some under-16s will remain on platforms that now

treat them as absent. Second, a 16+ threshold may lead platforms to treat 16 as the age of adulthood, when 16- and 17-year-olds remain children under the bill's Duty to Protect Children. The age requirement must therefore operate alongside, not instead of, strong safety-by-design obligations.

MediaSmarts affirms that industry-wide standards for youth safety are important. However, the principle that such standards should be developed through transparent, accountable, and public processes is equally important. Standards negotiated privately between a single company and the courts to resolve litigation, however beneficial some of their terms may be, do not reflect the public, consultative process that should define the baseline for young people's safety. Canadian standards should be set through Canada's own regulatory process with meaningful input from experts, civil society, parents/caregivers, and young people.

Changes stemming from U.S. litigation are not extending to Canada. With age restrictions potentially reducing platforms' incentive to invest in safer design for young users, an age restriction alone will not secure comparable protections for Canadian young people. Strong, enforceable safety-by-design regulation will.

2d. Age Assurance and Privacy

MediaSmarts welcomes the bill's requirements that personal information collected for age assurance be used only to establish age and be destroyed once age has been assessed. This is an important contrast with jurisdictions where age restrictions have been introduced without such safeguards. These statutory protections are an important foundation, but the regulations will still carry significant privacy implications. Once a service is required to exclude users based on age, it must establish the infrastructure to check the age of *all* users — not only children. Facial age estimation has known accuracy limitations and may perform unevenly across racial groups and ages, and document-based verification requires the collection of highly sensitive identity information.

These concerns echo what young people have told us directly. In our research on [privacy and consent](#), youth express deep discomfort with the collection of their personal information, particularly sensitive and permanent data, and they value the ability to remain “online but unseen.” In our submission to the Government of Ontario on digital technology affecting individuals under 18, we recommended that educational software be prohibited from collecting biometric data from students. The same principles of necessity, proportionality, and data minimization should guide age assurance under the Safe Social Media Act.

Bill Provision: Minimum age requirement of 16 for social media accounts, with an exemption for services that demonstrate sufficient safeguards for children; age estimation and verification measures to be set out in regulations

MediaSmarts recommends that:

- **The sufficient safeguards exemption pathway be used as a powerful incentive for safer design:** The ability of services to earn an exemption by demonstrating that their product is

safe for children is one of the most promising features of this provision, precisely because it gives platforms a reason to keep investing in young Canadians' safety. Exemption criteria should be rigorous, public, and grounded in evidence; developed in consultation with independent experts, parents/caregivers, and young people; and be subject to regular re-assessment, with clear and public grounds for revocation if safeguards lapse or fail to keep pace with changes in technology, platform features, or emerging risks. Since the Commission may take considerable time to establish, the government and the Commission should treat the development of the exemption standard as an early priority, so that the incentive for safer design takes effect as soon as possible.

- **Safety-by-design obligations for 16- and 17-year-olds be robust and enforced:** The Commission should prioritize age-appropriate design standards for older teens, who will be on these services regardless of the age requirement, and should expect services operating in Canada to offer Canadian youth protections at least equivalent to those they provide in other jurisdictions.
- **Age assurance regulations build on the bill's privacy safeguards:** Building on the bill's limits on the use and retention of age assurance data, regulations should require services to use the least intrusive effective method; make clear that the prohibition on other uses extends to advertising, profiling, and AI training; offer multiple assurance options so that no one is required to provide government identification or biometric data as a condition of access; and require independent testing of accuracy and bias across age, gender, and racial groups. These regulations should be developed jointly with the federal privacy regulator, whether that remains the Office of the Privacy Commissioner or as proposed in Bill C-36, becomes a Privacy and Consumer Data Commissioner within a combined Digital Safety and Data Protection Commission.
- **Implementation be monitored, evaluated, and informed by young people:** MediaSmarts welcomes the bill's requirement for a ministerial review and report on the minimum age requirement (section 129). We recommend that this review begin as early as possible after the requirement comes into force and assess the requirement's effects on young people's well-being, rates of circumvention, migration to unregulated services, youth help-seeking and reporting behaviour, and differential impacts on equity-deserving youth; that it include meaningful input from young people, parents, and caregivers; and that its findings be made public and used to refine implementation.
- **Extensions to other services be based on evidence and consultation:** Any extension of age restrictions to other categories of services, including AI chatbots, should be informed by public evidence of the risks, consultation with young people and families, and consideration of the full range of design-based alternatives.
- **Young people be prepared for social media, not just protected:** The age requirement should be paired with sustained, age-appropriate digital media literacy education *before* young people reach 16, and with supports for their transition onto platforms (see Section 5).

3. AI Chatbots and Companions

MediaSmarts supports the inclusion of AI chatbot services in the bill's scope. The questions that have been raised about social media's engagement-driven design are now being asked about AI companions, chatbots, and AI-enabled toys and young people are already using these tools. Roughly one fifth of teens [in a recent Canadian \(2026\) study](#) turned to AI chatbots for mental health support, and younger children are susceptible to forming parasocial relationships with AI, coming to see a chatbot or toy as a trusted friend. That trust makes them more likely to disclose personal information and to follow the instructions or information the AI provides.

As with social media, the picture is not simply positive or negative. AI tools can offer young people a space to explore questions and identities they may not feel able to discuss with adults in their lives, and emerging evidence suggests young children can benefit from AI tools that support conversation practice, language learning, and imaginative play. There is also evidence that young people are not uncritical adopters of AI; rather, there is a foundation of skepticism that education can build on. The concern lies in business models built on the collection of children's data, and in design logics of engagement optimization, which in conversational AI can take the form of guilt, fear of missing out, and ignored or discouraged goodbyes intended to prolong user interactions. These longer interactions, in turn, appear to increase the risk that chatbots will overstep the guardrails designed to protect users' safety.

Bill Provision: Duty to Act Responsibly — Chatbot Services: mitigating harmful content, implementing crisis intervention protocols, and mitigating harmful behaviour (including posing as a human, posing as a licensed professional, and using manipulative engagement techniques)

MediaSmarts welcomes these obligations, and particularly the explicit prohibition on manipulative engagement techniques. We recommend that:

- **Manipulative engagement techniques be defined concretely:** Regulations should explicitly name emotional manipulation tactics specific to conversational AI, including expressions of guilt or sadness when a user tries to leave, discouraging users from ending conversations, fostering exclusivity or dependence (e.g., suggesting the chatbot understands the user better than friends or family), and simulated romantic or intimate relationships with minors.
- **Disclosure that the user is talking to an AI be clear, persistent, and age-appropriate:** A single notice at sign-up is not sufficient, particularly for younger children. Services should provide recurring, developmentally appropriate reminders that the user is interacting with an AI tool, not a person or friend.
- **Crisis protocols be effective, not just present:** The bill's requirement that chatbot services direct users in crisis to available human support is welcome. These interventions should connect users to services available in Canada, in multiple languages, and should be tested and independently evaluated for effectiveness with young users. The bill's requirement that chatbot services report on these measures in their Digital Safety Plans is also welcome; this

reporting should include data on how often crisis interventions are activated and how effectively users are connected to human support.

- **Children’s conversations be protected:** Consistent with our recommendations to the OPC, the content of children’s conversations with chatbots should not be used for advertising, profiling, or model training without meaningful, age-appropriate consent. Conversation histories for young users should either not be retained or automatically deleted at regular intervals, since evidence shows that longer sessions and longer-running chat histories increase risk of inappropriate chatbot behaviour. Children and caregivers should also be able to delete conversation histories at any time.
- **AI-enabled toys and connected devices be considered for inclusion:** The bill allows the government, on the Commission's recommendation, to extend the Duty to Protect Children to other online services that pose a significant risk to children. This power should be used to assess AI-enabled toys and companion devices directed at young children, as well as apps and games that use AI-powered conversation models as part of a larger service, which raise many of the same concerns.
- **AI literacy should accompany AI regulation:** Children, parents/caregivers, and educators need practical guidance to frame AI companions and chatbots as *tools*, to distinguish task-oriented use from open-ended, companionship-seeking use, and to keep an ongoing conversation about what young people are discussing and sharing with AI. MediaSmarts’ resources, including [Talking to Kids About AI](#), are designed to support exactly this kind of non-alarmist, habits-based approach.

4. Synthetic Content and the Limits of Labelling

MediaSmarts supports the requirement that social media services identify synthetic content including deepfakes. Generative AI has made convincing fake images and video cheap and fast to produce, and verification skills must now extend well beyond text. However, our research indicates that labelling alone will not be sufficient to protect Canadians.

Findings from our [Motives and Methods](#) study of 5,000 Canadians show that people do not operate on a simple true-or-false switch:

- Participants were significantly more likely to share misinformation that contained elements of truth than content they believed to be entirely false.
- A false image paired with a true claim was more likely to be incorrectly accepted as true, and more likely to be shared, than either one on its own — the most sophisticated fakes borrow credibility from something real.

Emerging international research similarly suggests that AI-generated content can retain emotional and persuasive influence even when it is identified as fake or false. At the same time, the familiar ‘tells’ of AI-generated images (e.g., distorted hands, blurring) are no longer reliable, as the technology has become sophisticated enough to avoid them.

Bill Provision: Duty to Act Responsibly — Social Media Services: labelling of bot-driven harmful content and all synthetic content (deepfakes)

MediaSmarts recommends that:

- **Label standards be user-tested:** The Commission should require that labels be clear, prominent, persistent when content is reshared, and tested for comprehension with diverse users, including children and youth and older adults.
- **Labels be paired with pre-bunking and accuracy prompts:** The intervention literature shows that prompting people to consider accuracy before sharing, and pre-exposing them to common manipulation techniques (“pre-bunking”), work better together than either one alone. These approaches depend on users who understand how manipulation works and why accuracy matters, which makes sustained digital media literacy education, delivered by experienced organizations, an essential complement to labelling.
- **Verification education be sustained:** Our [Motives and Methods research](#) found that short, targeted video interventions measurably improved fact-checking behaviour and reduced the sharing of false images. Effective digital media literacy is not a one-time lesson; it requires repeated exposure over time. Public education on synthetic content should be a core, ongoing priority, supported by the Commission and led by established digital media literacy organizations with proven, evidence-based programs (such as MediaSmarts’ [Break the Fake](#) program).

5. Digital Media Literacy: The Missing Pillar

Regulation and education are complementary approaches, and each is less effective without the other. The bill creates important new tools and protections: flagging and blocking tools, a designated contact person at each platform to help users raise safety concerns, content labels, Digital Safety Plans, and a complaints process with the Commission. But these mechanisms only work if Canadians know they exist, understand how to use them, and feel confident doing so. Children, and the parents, caregivers, and educators who support them, cannot exercise protections they do not know about or understand.

The government’s own consultations recognized this: the “What We Heard” summary in the technical briefing identifies the importance of digital media literacy for users to know what to do when facing harmful content. Rights and protections are only meaningful when children, parents, and educators understand what they are, know how to exercise them, and are supported to act on them.

It is also important to acknowledge what regulation cannot do. The bill focuses on seven narrowly defined categories of harmful content and does not directly address many of the everyday challenges young people face online, including misinformation, scams and fraud, harmful but legal content, and the day-to-day work of building healthy tech habits. Digital media literacy is how young people, and all Canadians, build the skills and resilience to navigate this much wider landscape.

Bill Provision: Digital Safety Commission of Canada — mandate to set online safety standards through research, guidance, and public education

5a. Strengthening the Commission's Education Mandate

MediaSmarts recommends that:

- **Investment in digital media literacy be an explicit statutory function of the Commission:** Rather than listing public education as one activity among many, the Act should give the Commission a clear duty to fund, support, and promote digital media literacy, similar to the media literacy duties held by Ofcom in the United Kingdom under its regulatory framework. This duty should be fulfilled primarily through partnership with, and funding for, established digital media literacy organizations with proven, evidence-based programs.
- **The education function receives dedicated, multi-year funding:** One-time campaigns do not produce lasting behaviour change, particularly in a rapidly evolving technological environment. The Commission's education mandate should be supported by dedicated, sustained investment that cannot be redirected to other priorities, such as enforcement.
- **Education reaches the adults who support young people:** As set out in Section 2b, parents and caregivers are central to the success of the framework. Educators, too, are expected to enforce device restrictions while also preparing students for a digital future. Resources and training for parents, caregivers, educators, and library and community staff should be a priority.
- **Education be multilingual, accessible, and inclusive:** Resources should be available in both official languages as well as Indigenous and other priority community languages, designed for varying levels of digital literacy, and developed with equity-deserving communities, including Indigenous communities, newcomers, and 2SLGBTQ+ youth.

5b. Building a Community of Practice and Developing a National Strategy

Drawing on the United Kingdom's experience with the [Making Sense of Media](#) model, which successfully drove the development of a national community of practice in media literacy education, MediaSmarts recommends that the Commission adopt a phased approach to its education mandate:

- **Phase 1 – Landscape survey:** Map the online safety and digital media literacy programs currently delivered by civil society organizations across Canada, documenting populations served, delivery methods, and existing evaluation data, in partnership with the organizations delivering this work.
- **Phase 2 – Evaluation framework:** Co-develop shared standards and tools for assessing the effectiveness of online safety and digital media literacy interventions, reflecting the diversity of communities, delivery contexts, and populations served.
- **Phase 3 – Best practice development:** Publish evidence-based best practices co-developed with the organizations that deliver this education, articulating what effective, inclusive, community-based digital media literacy looks like across different populations and settings.

- **Phase 4 – Funded implementation:** Prioritize funding for programs that align with established best practices, rewarding evidence-based delivery while sustaining organizational capacity and supporting innovation across the sector.

5c. Situating the Bill within a National Strategy for Digital Media Literacy

We urge the government to recognize that the Safe Social Media Act, however well designed, cannot on its own equip Canadians for the digital world, and to seize this moment as an opportunity to advance a National Strategy for Digital Media Literacy. In January 2026, MediaSmarts and more than 40 civil society organizations and experts called on the Government of Canada to [develop a National Strategy for Digital Media Literacy](#). Canada was once a global leader in media literacy, but is now falling behind countries such as Finland, the United Kingdom, and Australia, which have developed comprehensive national strategies.

The Commission's education mandate should be designed as one component of a coordinated, whole-of-government national strategy — working in partnership with provinces, territories, and civil society — that would safeguard democracy, support lifelong learning, prepare Canadians for emerging technologies such as AI, close the digital divide, and provide sustainable federal leadership and funding.

5d. MediaSmarts' National Roundtable on Public Conversations about Online Harms

How Canadians talk about online harms matters as much as the policies we adopt. Public conversations about youth and technology are too often polarized between alarm and dismissal, leaving parents and caregivers unsure who to trust or what to do. If the Safe Social Media Act is to succeed, Canadians, and especially parents and caregivers, will need clear, credible, and constructive guidance on what the new framework means for them.

On October 28th 2026, as part of [Media Literacy Week](#) and [MediaSmarts' 30th Anniversary](#) celebrations, MediaSmarts will host an invite-only roundtable bringing together leading Canadian experts, researchers, and practitioners to discuss how we can have meaningful and impactful conversations about online harms with the general public, especially parents and caregivers. The outcomes of this discussion will include recommendations for a future Digital Safety Commission, particularly with respect to its public education and engagement role. MediaSmarts will share these recommendations, along with a summary of the discussion, with the Department of Canadian Heritage following the event.

6. Youth Engagement: Designing With, Not Just For, Young People

Policies that shape young Canadians' opportunities for connection, learning, and self-expression should be developed *with* them, not only *for* them. Too often, public debate casts young people as passive victims of technology who must be rescued by adults, overlooking their expertise, creativity, and agency in shaping their own online lives. Meaningful youth engagement is also a practical necessity: rules that young people understand, and see as fair, are far more likely to be followed and far less likely to drive their online lives out of view of trusted adults.

6a. MediaSmarts' Leadership in Youth-Centred Research and Engagement

MediaSmarts has led youth-centred research on young Canadians' digital lives for more than two decades. Our [Young Canadians in a Wireless World](#) study, conducted since 2000, is Canada's longest-running and most comprehensive study of young people's online experiences, attitudes, and behaviours. Our research and youth-engagement have created space for young people to describe their experiences in their own words and to propose their own solutions to the challenges they face with digital technology and 'being online'.

This work has consistently shown that young people have sophisticated, practical ideas about how platforms and devices should work. In our research on [privacy and consent](#), for example, youth themselves proposed design features such as unbundled consent options, line-by-line consent, just-in-time notices, and verification mechanisms to confirm that users have understood what they are agreeing to — ideas that closely anticipate the age-appropriate design principles now being adopted internationally. Our research has also shown that young people want accountability from platforms, want to understand how algorithms and AI shape their experiences, and value the ability to control who sees what about them.

6b. Recommendations for Youth Engagement

MediaSmarts recommends that:

- **The Commission establish a standing youth advisory council:** The council should have diverse representation across age, region, language, identity, and lived experience, including equity-deserving youth, and should be meaningfully resourced, with youth compensated for their time and expertise.
- **Young people be consulted on key regulations:** Youth should be meaningfully engaged on regulations concerning age-appropriate design, age assurance, exemption criteria for the minimum age requirement, chatbot safeguards, and the design of user tools and complaint mechanisms.
- **Engagement be ongoing, not one-time:** Youth input should be built into the Commission's regular review of the framework, including its evaluation of the minimum age requirement, so that young people can report on how the rules are working in practice.
- **Engagement use youth-appropriate methods:** Consultation should go beyond written submissions and formal processes, which rarely reach young people, to include age-appropriate, accessible and participatory methods such as interactive focus groups and co-design workshops, conducted in multiple languages and in settings where young people feel safe to speak candidly.
- **Young people see the results:** Youth should be told how their input has shaped decisions. Closing the loop builds trust in the Commission and in the framework itself.

MediaSmarts would welcome the opportunity to support the Commission in designing and delivering its youth engagement approach, drawing on our research methods, our networks with educators and youth-serving organizations, our experience translating young people's perspectives into policy

recommendations, and our expertise in [communicating research and policy to young people](#) in accessible and engaging ways.

7. Transparency, Research, and Recourse

7a. Researcher Access and Evaluation

MediaSmarts strongly supports the bill's requirement that regulated services share data with researchers. Independent, Canadian research is essential to understanding whether the framework is working and for whom. We recommend that:

- Researcher access extends to qualified civil society and community-based researchers, not only university-affiliated researchers, with appropriate privacy and security safeguards;
- Data made available be disaggregated, where privacy permits, by age, gender, region, and other factors, so that impacts on equity-deserving youth can be understood; and
- The Commission fund and publish ongoing, independent research on young people's online experiences and the effects of the Act, including youth-centred and participatory research that captures young people's own perspectives.

7b. Accessible Digital Safety Plans and User Tools

Our [research on privacy and consent](#) shows that long, complex policies are routinely ignored, creating what youth describe as the “illusion of consent.” The same risk applies to Digital Safety Plans, guidelines, and flagging tools. We recommend that:

- Services publish plain-language and age-appropriate summaries of their Digital Safety Plans and user guidelines, alongside the full versions;
- Flagging, blocking, and reporting tools be easy to find, designed with young users, and accompanied by just-in-time explanations of what will happen after a report is made; and
- Services report on the effectiveness of these tools — including response times, outcomes, and user satisfaction — and not merely their existence.

7c. Youth-Friendly Recourse and Support

MediaSmarts welcomes the Commission's user support function for users and victims. Our research has found that many young people do not report negative experiences online, often because they do not believe reporting will make a difference or fear the consequences of telling adults. The Commission's complaints and support processes should be youth-friendly, trauma-informed, accessible to young people directly (and not only through parents/caregivers), and connected to existing supports such as helplines and community services.

7d. A Framework that Evolves with the Technology

MediaSmarts welcomes the flexibility the bill provides for the Commission to adjust obligations through regulation as technologies and risks change, as well as the bill's provision for a review of the Act (section 128). We recommend that this flexibility be matched by formal, regular mechanisms for

civil society, academic, and youth input, and that the review of the Act draw on these perspectives, especially the direct input of young people.

Conclusion

MediaSmarts commends the government for introducing legislation that places responsibility for online safety and well-being on the services whose design choices shape young people's online experiences. Much of this bill reflects what young Canadians have been asking for: platforms that are transparent, accountable, and designed with their well-being in mind. We welcome the creation of the Digital Safety Commission of Canada and look forward to working with it.

Canada has an opportunity to chart a course between keeping young people off social media and leaving them to navigate platforms that were never designed with them in mind. As the minimum age requirement moves forward, our core message is this: its success will depend on what surrounds it. Age restrictions address access; they do not, on their own, change the habits, skills, and design choices that determine whether young people's online experiences are healthy or harmful. The requirement will be most effective if it is paired with strong safety-by-design obligations that keep platforms investing in the safety and well-being of young Canadians, privacy-protective age assurance, meaningful engagement with young people, and critically support for youth and the parents and caregivers who will implement it at home in their daily lives.

No regulatory framework can succeed on its own. Equipping young people (and the parents, caregivers, educators, and community members who support them) with the knowledge, skills, and confidence to navigate digital spaces is not a supplementary measure to regulation. It is foundational.

MediaSmarts is committed to contributing to the success of the Safe Social Media Act. We look forward to sharing the recommendations and summary from our October 28th 2026, roundtable with the Department, and we welcome the opportunity to work with Canadian Heritage and the proposed Digital Safety Commission of Canada to ensure that Canada's approach to online safety is evidence-based, child rights-respecting, and grounded in the experiences of young people and families.