



**LEAF
FAEJ**

WOMEN'S LEGAL
EDUCATION & ACTION FUND
FONDS D'ACTION ET D'ÉDUCATION
JURIDIQUE POUR LES FEMMES

Submission to the Department of Canadian Heritage on Bill C-34, *An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts*

29 September 2026

Prepared by:

Rosel Kim, Senior Staff Lawyer

Women's Legal Education and Action Fund (LEAF)¹

¹ Moira Aikenhead and Suzie Dunn contributed to the submission. Cassondra Barnaby, Ashna Hudani, Celeste Trianon, and Sophia Wedderburn provided research assistance.

I. Introduction

As an organization with a mandate to advance gender equality through the law, the Women's Legal Education and Action Fund (LEAF) supports the federal government's initiative to regulate harmful content online and imposing certain duties on providers of regulated social media services, regulated chatbot services, and other regulated online services through Bill C-34.

LEAF has long called for an expert regulator for technology-facilitated gender-based violence (TFGBV) to provide support to survivors and education to the general public on the issue.² For this reason, we welcome the establishment of the Digital Safety and Data Protection Commission in the Bill, which can receive and adjudicate on complaints regarding certain harmful online content including intimate content communicated without consent. The success of the Commission will depend on the government staffing it with adequate resources and relevant expertise, including expertise on human rights and substantive equality, so that it can provide real and meaningful support for survivors of TFGBV in a timely manner.

To ensure that Bill C-34 can address the needs of survivors of technology-facilitated gender-based violence, respect the fundamental rights of people using online services in Canada, and ensure users can access information online, we make the following suggestions in our submission:

1. Naming human rights and equality as a central guiding purpose of the Bill;
2. Ensuring the Commission has adequate resources and relevant staff expertise;
3. Having the Commission serve as the first place of contact for survivors experiencing harm, not the last resort;
4. Amending the definition of intimate content communicated without consent to remove references to deepfaked content needing to be "likely to be mistaken for a visual recording";
5. Pausing age-verification and age-estimation measures;
6. Having an education-forward approach to pornographic material; and
7. Ensuring consultations on regulations remain open and accessible.

² Cynthia Khoo, *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence* at 225 (2021), online: LEAF <<https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>> [*Deplatforming Misogyny*]; Moira Aikenhead, Suzie Dunn, and Rosel Kim, "Submission to Canadian Heritage on the Federal Government's Proposed Approaches to Address Harmful Content Online" (25 September 2021) at pp 13-17, online: LEAF <<https://www.leaf.ca/wp-content/uploads/2021/09/2021-09-25-LEAF-Submission-re-Harmful-Online-Content.pdf>> [LEAF 2021 Submission]; Pam Hrick, Cynthia Khoo, and Rosel Kim "Protecting against online gender-based violence and harassment", *Toronto Star* (28 April 2021) online <https://www.thestar.com/opinion/contributors/protecting-against-online-gender-based-violence-and-harassment/article_8cc61e41-43d8-5d32-8e31-a160e76712fd.html>

In addition, we share the concerns raised in the submission by Professor Jane Bailey, Dr. Jacquelyn Burkell, and Dr. Valerie Steeves and specifically endorse Recommendations 8, 9, and 10.³

We discuss the above-mentioned points in detail below.

1. Naming human rights and equality explicitly as a purpose of the Bill

It is critical that federal action in this area centre human rights, substantive equality, and intersectionality. TFGBV is an equality issue and a gendered issue. It can have devastating impacts on the equality rights of women, girls, trans and non-binary people who are targeted, including their physical and psychological safety, ability to participate in public life, and ability to benefit from equal protection of the law. We appreciate the explicit direction to the Commission to take equality rights into account when making regulations and issuing guidelines, codes of conduct, and other documents. Substantive equality and freedom from discrimination must be given due emphasis and prioritized alongside the right to freedom of expression.⁴

For this reason, we recommend adding “promote and uphold equality for all persons in Canada” as one of the purposes of *Digital Safety Act*, in section 14 of the Bill.

³ The recommendations are:

Recommendation 8: Digital safety plan obligations in Bill C-34 should be amended to include a requirement for providers to report on whether they have chosen not to include information on the basis of the trade secret and confidentiality exceptions set out in ss. 42(6), 58(6) and 59(6), and to describe the reasoning underlying those exclusions. In assessing the digital safety plan, the DSCC should consider whether reliance on the exception is justified and, if not satisfied, be empowered to request access to relevant information to independently assess its legitimacy.

Recommendation 9: Augment obligations to assess risks and to report on and implement strategies to address risks currently set out in C-34 with explicit requirements to include risks arising from their own systems, including their business model, the design, features or functioning of their services, consideration of business recommender and ad systems, possibilities for user manipulation, data collection and use practices, terms of service, content moderation practices, technology tools and allocated resources.

Recommendation 10: Augment obligations to assess risks and to report on and implement strategies to address risks currently set out in C-34 to include actual or foreseeable negative effects on fundamental human rights and child rights, including equality, free expression, and privacy, as well as on identity-based violence, protection of public health and children, and “serious negative consequences to people’s physical and mental well-being” (see Art. 34(1)(d) DSA).

⁴ [Deplatforming Misogyny](#) at p 224; [LEAF 2021 Submission](#) at pp 6-8.

2. Setting up the Digital Safety and Data Protection Commission for success through adequate resources

With Bill C-34, the government has a pivotal opportunity to create a regulatory body that can meaningfully support survivors of technology-facilitated gender-based violence and hold technology platforms accountable. We are encouraged that the federal government has included research and education as part of the Commission's mandate, which will play an essential role in keeping up with the rapidly evolving landscape of TFGBV and online harms, monitoring the effectiveness of available recourse for survivors, and informing the public of their rights and available processes for online harms.

However, the Commission's success will only be possible by having adequate resources and prioritizing human rights and substantive expertise in staffing the Commission.

One of LEAF's chief recommendations to the federal government in our TFGBV work has been the creation of an independent regulator with expertise on TFGBV and a dual mandate to a) "provide legal remedies and support to individuals impacted by TFGBV on digital platforms, including regulatory and enforcement powers; and b) to develop research on TFGBV and provide training and education to the public, relevant stakeholders, and professionals."⁵ In the same research report containing this recommendation, we warned against the "bundling" of disparate harms⁶ and recommended "[l]egislative reforms that are genuinely intended to meaningfully address TFGBV must ensure they are sufficiently tailored to TFGBV and related systemic oppressions, in order to ensure a strong constitutional basis."⁷

The success of the Commission will depend on its accessibility to survivors and its ability to centre users' human rights and equality principles. The legal system is inaccessible to many survivors because of the high costs of retaining legal representation, lengthy timelines and delays, and high evidentiary thresholds in criminal proceedings that can retraumatize and revictimize survivors. In addition, many justice system actors often lack understanding of gender-based violence and its impact on survivors, which makes many survivors reluctant to engage with the legal system.⁸

With the introduction of Bill C-36, the Commission's mandate has expanded significantly to address both digital safety—which encompasses a wide range of harmful behaviours across multiple services—and privacy. Privacy experts have expressed concerns about having one Commission address many complex issues and harms, especially when the existing Office of

⁵ [Deplatforming Misogyny](#) at p 225 (Recommendation 4).

⁶ [LEAF 2021 Submission](#), p 6.

⁷ [Deplatforming Misogyny](#) at p 205.

⁸ [Deplatforming Misogyny](#) at p 52.

the Privacy Commissioner has developed a reputation and expertise on one of those issues.⁹ We urge the federal government to take these concerns seriously and sets up the Commission for success through proper resources and staffing, including hiring people with expertise on human rights and equality.

3. Easier access to the Commission for people experiencing harm

We support the targeted takedown requirement for content that sexually victimizes a child or revictimizes a survivor and intimate content communicated without consent. Unlike other types of harmful content that may require some deliberation and determination, content that sexually victimizes a child or revictimizes a survivor, and intimate content communicated without consent are easily identifiable and carry an increased risk of harm and re-traumatization through amplification if the content remains online.¹⁰

However, we have concerns about the takedown process and its potential difficulty for survivors. While the Commission does allow people to file complaints about intimate content posted without consent, the complaint mechanism is only available after a person has flagged the content for removal with the operator and is unsuccessful in appealing the operator's decision. While we understand the need to preserve the Commission's resources, the need for a survivor to exhaust internal mechanisms of content moderation of a regulated service provider would be a barrier for survivors whose priority is expedient removal of content without needing to go through multiple steps. Moreover, social media platforms have consistently shown their unwillingness to consider real harms users experience if moderating such harms would hurt their bottom line and also ignore their own rules and policies about harmful and abusive content.¹¹

We recommend having the Commission serve as the first point of contact and resource that survivors of intimate content shared without consent can access when they discover the content that must be flagged and removed. In the alternative, the Commission could establish

⁹ See Teresa Scassa, "Canada's new privacy reform bill (Bill C-36): renovation or demolition?" (18 June 2026) online: Substack <<https://teresascassa.substack.com/p/canadas-new-privacy-reform-bill-bill>>

¹⁰ [LEAF 2021 Submission](#) at p12.

¹¹ See [Deplatforming Misogyny](#) at pp 90-92.

a helpline to explain options for recourse for survivors, similar to provincial initiatives like British Columbia’s Intimate Images Protection Service¹² or Nova Scotia’s CyberScan.¹³

4. Removing the “likely to be mistaken as a visual recording” threshold from the definition of deepfaked intimate content communicated without consent

The Bill’s definition of deepfaked intimate content communicated without consent¹⁴ is from the recently passed Bill C-16, which amends the *Criminal Code*’s offence of non-consensual distribution of intimate images provisions to include visual representations made by any electronic or mechanical means. While we understand the need to define criminal deepfakes more narrowly, legislation establishing regulatory regimes like the *Digital Safety Act* should capture deepfakes more broadly to recognize the harms of sexualizing someone’s image without their consent and ensure that many harmful deepfakes can be taken down.

We suggest revising the definition of “intimate content communicated without consent” in section (b) to “a visual representation that is made by any electronic or mechanical means, including by means of artificial intelligence software, and that shows an identifiable person **in a reasonably convincing manner**, who is depicted as nude, as nearly nude, as exposing their sexual organs or anal region or as engaged in explicit sexual activity.”

The wording “reasonably convincing” appears in the definition of “fake intimate image” in Manitoba’s *Non-Consensual Distribution of Intimate Images Act*¹⁵ This would allow for expedient takedown of deepfaked intimate content that may not meet the threshold of appearing like an authentic visual recording but can still cause harm—such as deepfakes of someone appearing to have sex with a celebrity.

¹² Government of British Columbia, “Intimate Images Protection Service” (Last updated 11 March 2026) online: Government of British Columbia <<https://www2.gov.bc.ca/gov/content/safety/public-safety/intimate-images/intimate-images-support>>

¹³ Province of Nova Scotia, “Intimate images and cyber-protection: support for victims” online: CyberScan <<https://novascotia.ca/cyberscan/>>

¹⁴ The Bill does not use the term “deepfake” but provides a separate definition of intimate content communicated without consent as a “a visual representation that is made by any electronic or mechanical means, including by means of artificial intelligence software, and that shows an identifiable person who is depicted as nude, as nearly nude, as exposing their sexual organs or anal region or as engaged in explicit sexual activity, if the depiction is likely to be mistaken for a visual recording of that person and if it is reasonable to suspect that the person does not consent to the representation being communicated.” See Bill C-34, *An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts*, 1st Sess, 45th Parl, 2026, cl 2(1) (definition of “intimate content communicated without consent” (b)) [Bill C-34].

¹⁵ *The Non-Consensual Distribution of Intimate Images Act*, CCSM c. N93 at s 1(1) (Definitions).

5. Concerns about age-estimation and age-verification

Neither age-verification nor age-estimation are defined in the Bill. Age-verification is widely understood to require government IDs or other forms of identification to verify a user's age, and age-estimation involves estimating a user's age through technology like facial recognition that guesses a user's age.¹⁶

Our concerns about the Bill's age-verification and age-estimation requirements for social media accounts and for pornographic content are based on three areas: effectiveness, privacy and equality implications of age verification requirements, and the impact on young people's access to information.

Effectiveness

Evidence from countries that have already implemented age-verification and age estimation reveals mixed results about their ability to keep young people away from social media platforms and pornographic content:

- A study published this summer measuring the effect of Australia's *Social Media Minimum Age Act* on teenagers' social media use found that "implementation of age assurance measures by social media platforms is suboptimal, and evidence suggests that these are being circumvented by adolescents."¹⁷
- A recent report by Australia's eSafety Commissioner on technology companies' compliance with social media minimum age requirements found that facial age estimation is "known to have higher error rates for children near the age threshold of 16 years."¹⁸
- A report from the United Kingdom's Ofcom, the country's national communications services regulator, found that "nearly half of [pornography] services visited by 8 to 14-year-olds had no age assurance in place."¹⁹

¹⁶ See Emily Laidlaw, "Online Age Verification is Crucial and Bill S-210 Gets It Wrong" (5 February 2024) online: ABLawg.ca < <https://ablawg.ca/2024/02/05/online-age-verification-is-crucial-and-bill-s-210-gets-it-wrong/> >

¹⁷ Courtney Barnes et al., "Assessing early effects of Australia's *Social Media Minimum Age Act* on adolescents' social media use: observational study" (24 June 2026) British Medical Journal 2026; 393 < <https://doi.org/10.1136/bmj-2026-363695> >

¹⁸ eSafety Commissioner, *Social Media Minimum Age: March 2026 Compliance Update* (March 2026) at p 21, online: < <https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806> >

¹⁹ Office of Communications, *Report on the Use of Age Assurance* (27 July 2026) at 4.37, online: < <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162> >

- In a submission to the Australian Parliament’s inquiry about social media bans and age verification and estimation, the Australian Human Rights Commission noted that facial age estimation is less reliable for “individuals with darker skin tones and for those aged 16-20, raising serious concerns about equality and discrimination.”²⁰ From early on, experts flagged the racial and gender bias of facial recognition technology,²¹ which is now being used widely as a gatekeeper of the internet.

Privacy concerns

Age-estimation and age-verification require gathering more personal information about users of services. This raises serious privacy concerns, as hacking incidents targeting companies that are holding such personal information become more commonplace. In October 2025, government ID photos of about 70,000 users of Discord, a messaging platform, were leaked due to hacking. It was suspected that some users had additional personal information exposed, including names, email addresses and contact details, IP addresses, and messages with Discord’s service agents.²² Just a few days ago, the Privacy Commissioner of Canada announced it will be investigating the data breach at IDScan.net, a third-party company that verifies government identification for businesses.²³ An independent journalist estimated that the breach included about 153 million stolen identity documents from the US and Canada.²⁴

The Bill specifies that age-estimation and age-verification measures must minimize collection of personal information and provide for the protection of personal information;²⁵ however, the personal information required to enable age-verification necessarily increases risks of people’s privacy rights being violated.

²⁰ *Internet Search Engine Services Online Safety Code and under 16 social media ban*, Report of the Senate Environment and Communications References Committee at 2.58, Parliament of Australia, November 2025, online: Parliament of Australia.

<https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OnlineSafetyCode48P/Report>

²¹ Joy Buolamwini & Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification” (2018) 81:1 *Proceedings of Machine Learning Research* 15, online: <<https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>>

²² Robert Booth, “Hacks of age verification firm may have exposed 70,000 Discord users’ ID photos” (9 October 2025) *The Guardian*: <https://www.theguardian.com/media/2025/oct/09/hack-age-verification-firm-discord-users-id-photos>

²³ Office of the Privacy Commissioner of Canada (OPC), “Privacy Commissioner of Canada launches investigation into a data breach involving stolen identification details” (21 September 2026) online: OPC <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260921/>

²⁴ Ariel Rabinovitch, “Canada’s privacy czar launches investigation of major driver’s licence hack”, *Global News* (22 September 2026) online <<https://globalnews.ca/news/12068230/privacy-commissioner-investigation-drivers-licence-hack/>>

²⁵ [Bill C-34](#) at cl 22(2).

Equality concerns

The focus on government-issued identification to verify someone's age has negative implications from a substantive equality perspective for people who are precariously housed or unhoused, for trans people whose IDs may not correspond with their lived identity, and for sex workers who may want to shield their legal identity due to the criminalization of sex work.

The use of age verification or estimation has a disproportionate impact on trans and non-binary adults who often do not have government-issued identification or banking information consistent with their gender and/or name, and who often face misgendering and exclusion by facial recognition algorithms.²⁶ As a result, strict age-verification requirements may lead to trans and non-binary people being unable to access important parts of the internet.²⁷ In addition, age-verification requirements may lead to discrimination against trans and non-binary people if companies that conduct age-verification and collect personal information are required to share such information with another country if people enter that country.

Access to information

Imposing age verification and age assurance can also have negative impacts on young people's ability to access sex education online. With age verification requirements, platforms may opt to ban content about sexuality altogether, which would impact young people's ability to access vital information. In addition, requiring identification to create accounts may result in barriers for women, trans, and non-binary people who are poor, precariously housed or unhoused, sex workers, migrants, and face other systemic barriers.²⁸

For many 2SLGBTQIA+ youth whose gender identity and/or sexuality are not accepted by their parents or guardians, the internet and social media remain important spaces for them to learn about and connect with members of their community, as well as express themselves. Age verification measures may suppress legitimate expression and educational materials about one's sexuality that could be lifesaving for some young people, especially those whose identities are not accepted by their parents, their communities, and/or their peers.

²⁶ Os Keyes, "[The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition](#)" (2018) 2: CSCW *Proceedings of the ACM on Human-Computer Interaction* 88; Morgan Klaus Scheuerman, Jacob M Paul & Jed R Brubaker, "How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services" (2019) 3: CSCW *Proceedings of the ACM on Human-Computer Interaction* 144, online: <<https://dl.acm.org/doi/10.1145/3359246>>

²⁷ Janus Rose, "'Age Verification' could force trans people to out themselves to use the Internet", *The Verge* (10 March 2026), online: <<https://www.theverge.com/policy/892075/age-verification-kansas-id-trans>>

²⁸ LEAF, "Measures to facilitate online safety for youth must uphold human rights (Letter sent to the Chair of the Parliamentary Committee on Public Safety and National Security re: Bill S-210)" (29 May 2024) at p 3, online: <<https://www.leaf.ca/submission/bill-s-210-concerns-age-verification/>>

Recommendation re: age-estimation and age verification

We understand the need to tackle children’s exposure to harmful content and to hold social media companies accountable for profiting from harmful content. However, the concerns regarding equal access, freedom of expression, and privacy, in combination with the known efficacy issues of age verification and estimation technology at this time, should lead to pause. In addition, age-verification and age-estimation do not tackle the systemic roots of harms that people experience online. As Daniel Angus and Christine Parker point out, “[k]eeping [teenagers] out of a handful of social media platforms won’t address the deeper problems of platform design, recommendation systems and business models that can make these environments harmful in the first place.”²⁹

For the reasons outlined above, we urge caution on implementing age verification and age estimation.

If the government decides to implement these measures, we recommend:

- a) narrowly defining the types of content that will be subject to age verification and age estimation to avoid over-censoring of content, including important information about sexuality for young people; and
- b) ensuring that personal information collected for age-verification and age-estimation purposes are held by companies based in Canada, to avoid having personal information shared without the person’s consent or knowledge with another country, which could lead to discriminatory and harmful impact for marginalized community members who may want to shield their identity and/or whose identity does not match their government-issued IDs.

6. An education-forward approach to pornographic content

The Bill would ban access to pornographic content for people under 18 years old. The definition of pornographic content in the Bill is both under-and over-inclusive, due to its focus on a person’s genital and anal regions depicted for a sexual purpose. The anatomical focus could result in sexual education materials being wrongfully flagged as pornographic and becoming censored for young people, especially if platforms are using automated content moderation mechanisms.

²⁹ Daniel Angus and Christine Parker, “Australia’s social media ban has an enforcement problem. These new laws aim to fix it”, *The Conversation* (7 September 2026) online: <<https://theconversation.com/australias-social-media-ban-has-an-enforcement-problem-these-new-laws-aim-to-fix-it-291356>>

While we have concerns about young children accessing violent and harmful porn, we believe older teens having access to consensually made, nude sexual content does not rise to the same level of concern. As we have stated in the past, “implementing age-appropriate, inclusive education on online pornography to build media literacy amongst young people, parents, and educators”³⁰ may strike a better balance than the current approach in the Bill.

7. Need for accessible consultation and meaningful participation

Many details have been left to the regulations. We urge the federal government to hold open and accessible consultations with stakeholders including survivors and experts in TFGBV before enacting the regulations. Accessible consultations also require material support—including funding—for the consultees to ensure equitable and meaningful participation from civil society organizations representing systemically marginalized groups, especially in the context of regulating powerful technology companies and platforms.

We would welcome an opportunity to discuss our submission further.

³⁰ LEAF, “Measures to facilitate online safety for youth must uphold human rights (Letter sent to the Chair of the Parliamentary Committee on Public Safety and National Security re: Bill S-210)” (29 May 2024) at p 3, online: <<https://www.leaf.ca/submission/bill-s-210-concerns-age-verification/>>